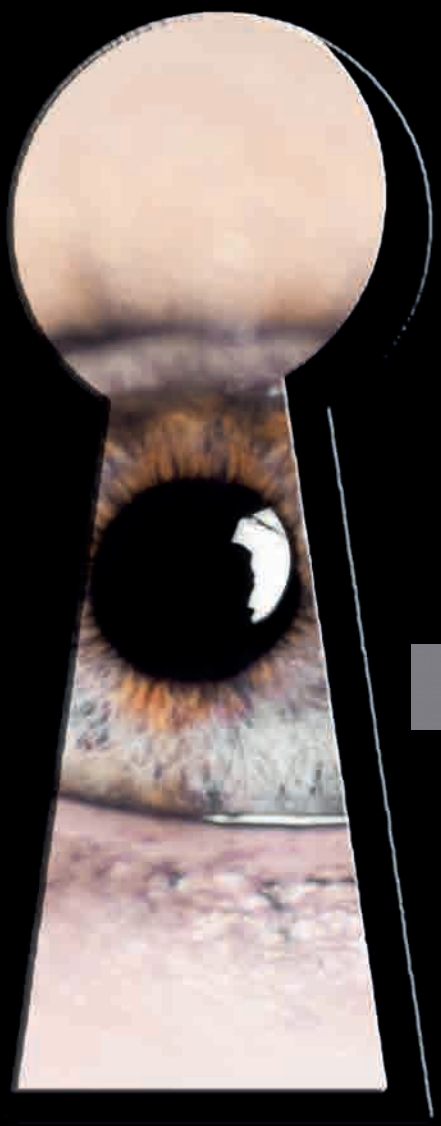
VADEMECUM
5 lat

VAR-ÓW i INTEGRATORÓW

CRN
WYDANIE SPECJALNE
maj 2018
ISSN 1640-9183



Ochrona sieci

Antymalware

Uwierzytelnianie

Zasilanie i monitoring

Prawo

Bezpieczeństwo
infrastruktury IT

NAKIVO®

BACKUP MASZYN WIRTUALNYCH VMWARE, HYPER-V ORAZ INSTANCJI AMAZON EC2

Backup bezagentowy — oparty na obrazie maszyny wirtualnej

Screenshot Verification — weryfikacja backupu i migawek

Flash VM Boot — natychmiastowe odzyskiwanie maszyn wirtualnych

Oszczędzisz nawet 50%

na backupie maszyn wirtualnych

Sprawdź

nakivo.fen.pl

Vademecum 2/2018

Ilustracje AdobeStock

Inteligentna wojna

Odwieczna wojna z cyberprzestępcami doprowadziła do tego, że obie strony wytoczyły najcięższe działa. Dostawcy rozwiązań ochronnych zaangażowali już do walki sztuczną inteligencję, hakerzy pójdą w ich ślady lada moment. Może to oznaczać, że my, ludzie, w pewnym momencie stracimy kontrolę nad procesem wykrywania i zwalczania cyberzagrożeń. Ale nie musi do tego dojść, o czym zapewniają eksperci z branży.

Historia sztucznej inteligencji sięga lat 50. ubiegłego wieku, ale z namacalnymi i wyrazistymi przykładami jej zastosowania w codziennym życiu mamy do czynienia dopiero teraz. Jest obecna na przykład w asystentach głosowych w smartfonach. Wszystko wskazuje na to, że będzie miała ogromny wpływ także na proces zabezpieczania zasobów IT. Firmy produkujące rozwiązania ochronne po prostu przestały sobie dawać radę zarówno ze skalą ataków, jak i z poziomem ich skomplikowania. Mimo że po drugiej stronie barykady także działają ludzie, nadążenie za ich – celowo zakamuflowanymi – informatycznymi sztuczkami wymaga nie tylko wiedzy i energii, ale przede wszystkim czasu. Wygrywa ten, kto potrafi wykorzystywać go bardziej efektywnie.

Sztuczna inteligencja nie pojawi się jednak jako zupełnie nowa kategoria produktów. Będzie raczej stosowana tam, gdzie to możliwe, w znanych już rozwiązaniach: firewallach nowej generacji, systemach IDS/IPS, nawet w zwykłych antywirusach. Naturalnie analiza maszynowa nie będzie prowadzona na urządzeniach użytkowników, bo potrzeba do niej ogromnego centrum danych z setkami serwerów. A to może znacząco opóźnić osiągnięcie pełnej skuteczności rozwiązań wykorzystujących sztuczną inteligencję. Na urządzenia użytkowników trafi oprogramowanie wyposażone w efekt analizy uczenia maszynowego. Stworzone w ten sposób mechanizmy poradzą sobie z najbardziej skomplikowanymi, ale już znanymi rodzajami zagrożeń. Zawsze jednak będzie to działanie reaktywne – w pierwszej kolejności będzie miał miejsce atak na urządzenia użytkowników indywidualnych, a dopiero później dowiedzą się o tym systemy ochronne i będą miały szansę go odeprzeć. Mleko się jednak rozleje...

Eksperci ds. bezpieczeństwa wciąż mają zbyt mało wiedzy na temat zastosowania nauczania maszynowego w rozwiązaniach ochronnych.

Dostawcy systemów zabezpieczeń dwoją się i troją, aby pokazać się z najbardziej innowacyjnej strony. Oczekują tego użytkownicy: według badań przeprowadzonych przez organizację ESG 12 proc. korporacji na świecie już teraz w dużym stopniu uzależnia swoją strategię bezpieczeństwa od rozwiązań bazujących na sztucznej inteligencji, a kolejnych 27 proc. prowadzi testy. Ten wzrostowy trend zdecydowanie nabierze tempa w 2018 r. Forrester Research przewiduje, że tegoroczne inwestycje w tej dziedzinie będą trzykrotnie większe niż ubiegłoroczne.

Ale jest też problem. Pytani przez ESG eksperci ds. bezpieczeństwa zgodnie stwierdzili, że wciąż mają zbyt mało wiedzy na temat zastosowania nauczania maszynowego w rozwiązaniach ochronnych. Tylko 30 proc. z nich ma wrażenie, że dysponują wiedzą na satysfakcjonującym poziomie. Możemy też być pewni, że ze sztucznej inteligencji wkrótce zaczną korzystać także cyberprzestępcy. Na ile będą skuteczni w walce z inteligentnymi maszynami wykorzystywanymi przez organizacje tworzące systemy zabezpieczeń? Nie wiadomo, ale z pewnością będzie to fascynująca walka.

Krzysztof Jakubik
redaktor prowadzący

Fot. Marek Zawadzki

Ustawa o krajowym systemie cyberbezpieczeństwa

26 kwietnia 2018 r. Rada Ministrów przyjęła projekt ustawy o krajowym systemie cyberbezpieczeństwa. Równolegle dobiega końca proces legislacyjny dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej (tzw. dyrektywa NIS). Projektowana ustawa o krajowym systemie cyberbezpieczeństwa wpisuje się w cel 5. Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 (tworzenie warunków do rozwoju zintegrowanego systemu bezpieczeństwa narodowego). Efektem wprowadzonych regulacji ma być podniesienie odporności kluczowych usług świadczonych z wykorzystaniem technik IT na ataki pochodzące z cyberprzestrzeni.

GŁÓWNE CELE USTAWY

1. Ustanowienie na szczeblu krajowym architektury ochrony systemów teleinformatycznych z uwzględnieniem regulacji międzynarodowych oraz wskazanie organów władzy publicznej odpowiedzialnych za zarządzanie bezpieczeństwem informacji.
2. Ustanowienie krajowego systemu reagowania na zagrożenia dla bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych, pochodzące z cyberprzestrzeni.
3. Ustalenie zasad współpracy podmiotów zobowiązanych do wykrywania incydentów spowodowanych zagrożeniami z cyberprzestrzeni i sposobów postępowania w okresie trwania tych incydentów.
4. Prawne umocowanie dokumentu ustanawiającego krajową strategię bezpieczeństwa sieci i informacji mającą na celu osiągnięcie akceptowalnego poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej.
5. Wskazanie sektorów gospodarki narodowej, w których zastosowanie będą miały przepisy ustawy, oraz określenie kryteriów kwalifikowania podmiotów objętych regulacją.
6. Ustalenie poziomu istotności incydentu z zakresu bezpieczeństwa oraz wprowadzenie obowiązku notyfikowania incydentów wskazanemu organowi władzy publicznej.

OPERATORZY USŁUG KLUCZOWYCH

Krajowy system cyberbezpieczeństwa będzie obejmował: operatorów usług kluczowych (m.in. z sektorów energetycznego, transportowego, bankowości i infrastruktury rynków finansowych, zaopatrzenia w wodę, zdrowotnego), dostawców usług cyfrowych, zespoły CSIRT poziomu krajowego (Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego), sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa (odpowiedzialne za nadzór nad operatorami usług kluczowych) oraz Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa (służący do komunikacji w ramach współpracy w Unii Europejskiej w tej dziedzinie).

JEDEN LOGIN DLA KAŻDEGO OBYWATELA

Rada Ministrów RP przyjęła tzw. ustawę węzłową (projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw). Przewiduje ona wprowadzenie jednego loginu/identyfikatora, który docelowo umożliwi korzystanie ze wszystkich cyfrowych usług administracji rządowej. Wprowadzono również regulacje będące podstawą prawną funkcjonowania publicznej aplikacji mobilnej mDokumenty.

SYSTEM REAGOWANIA NA INCYDENTY

W projektowanej ustawie zaproponowano stworzenie systemu reagowania na incydenty, którego założeniem jest kompletność (obecność we wszystkich kluczowych sektorach), transparentność i kompleksowość. Ustawa określa zadania zespołów CSIRT (Computer Security Incident Response Team), które będą odpowiedzialne za przeciwdziałanie zagrożeniom o charakterze ponadsektorowym i transgranicznym, a także koordynację obsługi poważnych incydentów. Przewiduje też włączenie aspektów cyberbezpieczeństwa do sfery zarządzania państwem.

Projekt ustawy wprowadza kilka kategorii incydentów, które są zróżnicowane w zależności od rodzaju podmiotu, który je zgłasza, i stopnia ich oddziaływania (progów):

- incydent poważny, zgłaszany przez operatora usług kluczowych, związany jest z poważnym obniżeniem jakości lub przerwaniem ciągłości świadczenia usługi kluczowej,
- incydent istotny – ma istotny wpływ na świadczenie usługi cyfrowej,
- incydenty krytyczne skutkują znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów gospodarczych i działania instytucji publicznych.

Złożoność jest wrogiem bezpieczeństwa

– Producenci rozwiązań ochronnych powinni wziąć na siebie odpowiedzialność za uczynienie życia partnerów i klientów łatwiejszym. Produkty te powinny być proste nie tylko w obsłudze, ale też we wdrażaniu – mówi **Kris Hagerman**, **Chief Executive Officer w Sophosie**.

CRN Odbiorcy rozwiązań IT w ostatnich latach mają problem z wyborem systemów zabezpieczeń infrastruktury teleinformatycznej. Z jednej strony są producenci, którzy działają od 20–30 lat i wielu kojarzą się z „dinozaurami" branży, a z drugiej „rozpychające się" kilkuletnie startupy uzurpujące sobie wyłączne prawo do bycia innowacyjnymi. Jakich argumentów powinni używać resellerzy i integratorzy, aby skłonić klientów do współpracy z przedstawicielami jednej z tych dwóch grup?

Kris Hagerman Rzeczywiście, dość popularna opinia, że to głównie startupy są innowacyjne, jest moim zdaniem zupełnie błędna. Dla przykładu podam nazwy trzech firm: Apple, Google i Amazon. Pierwsza ma ponad 40 lat, a pozostałe ponad 20. Żadnej nie można zarzucić, że nie jest innowacyjna. Oczywiście także wiele startupów ma świetne pomysły, ale w branży rozwiązań ochronnych IT to nie wystarczy, bo przedmiotem sprzedaży jest w niej bardzo specyficzny rodzaj produktów. Oprócz funkcji i jakości oferowanych rozwiązań bardzo ważne są też kreatywność, innowacyjność, doświadczenie i wiarygodność producenta oraz gotowość klienta do obdarzenia go zaufaniem. My jesteśmy tego najlepszym przykładem – mamy ponad 30 lat i zdobyte przez ten czas zaufanie tysięcy klientów, ale nie zwalnia to nas z pracy nad ciągłym rozbudowywaniem funkcji kolejnych produktów. W bezpieczeństwie nie ma mowy o sukcesie bez bycia liderem innowacyjności.

CRN Czy naprawdę tworząc nowe rozwiązania, korzystacie ze swojego doświadczenia z lat 80. i 90.?

Kris Hagerman Oczywiście! I to na wielu poziomach. Naturalnie zmieniło się otoczenie techniczne, inne są systemy operacyjne, aplikacje i – niestety – przyczyny podejmowania działań przez atakujących. Ale znajomość procesu tych zmian, ewolucji rynku oraz świadomość tempa poszerzania się wiedzy użytkowników pomaga nam w utrzymaniu profesjonalnych relacji z klientami oraz resellerami i integratorami. Wiemy, jakie są ich potrzeby i staramy się je zaspokoić, tworząc innowacyjne rozwiązania w taki sposób, aby nie doprowadzać za każdym razem do rewolucji. Dzięki temu możemy cieszyć się najcenniejszą w branży zdobyczą – zaufaniem.

CRN Jak zatem startupom udaje się utrzymać na rynku, skoro – jako nowe podmioty – nie miały jeszcze szansy zyskać zaufania?

Kris Hagerman Widzimy jak to dla nich trudne. Efektem zresztą jest duża liczba startupów, które znikły z rynku, bo nie odniosły sukcesu. W tej chwili istnieje ponad tysiąc niezależnych firm oferujących rozwiązania ochronne i codziennie powstają nowe. Wiemy, że większość z nich nie przetrwa, więc z punktu widzenia partnerów i klientów inwestowanie czasu i pieniędzy w rozwiązania nowopowstałych producentów to loteria. Gdy firma jest na rynku tylko parę lat, nie sposób ocenić, jak będzie reagowała w przypadku kryzysów, na jak solidne wsparcie mogą liczyć klienci i czy będzie starała się zostać rynkowym liderem. Doświadczenie pokazuje, że z czasem większość nowych firm przejmują bardziej zadomowione w branży przedsiębiorstwa, co jest swego rodzaju ratunkiem dla ich klientów, którzy zdecydowali się podjąć ryzyko.

Sztuczna inteligencja to kolejny etap wyścigu między dobrem i złem w kontekście IT.

CRN Obserwacja rynku dostawców rozwiązań ochronnych prowadzi do bardzo ciekawej konkluzji. Przykładowo w dwóch magicznych kwadrantach Gartnera, obejmujących producentów UTM-ów oraz oprogramowania zabezpieczającego urządzenia końcowe, powtarzają się tylko dwie firmy: Sophos i Cisco. Czy fakt skupienia się prawie wszystkich dostawców na jednym obszarze powinien skłaniać do wniosku, że klienci mogą skupić się na ochronie też tylko jednego – infrastruktury sieciowej lub urządzeń końcowych?

Kris Hagerman To pytanie w rodzaju, co dla człowieka jest ważniejsze: woda czy jedzenie. Niezbędna jest ochrona w każdym punkcie infrastruktury IT! Ale faktem jest, że nasza branża od czasu do czasu poddaje się modzie na ochronę albo sieci, albo urządzeń końcowych. Wówczas dostawcy rozwiązań dla jednego obszaru przekonują klientów, że zabezpieczanie tych z drugiego jest mniej istotne. Bywa, że producenci oprogramowania antywirusowego twierdzą, iż ochrona sieci nie jest tak ważna, bo złośliwy kod będzie próbował uruchomić się na stacji roboczej. Tego typu tłumaczenie jest absurdalne. My uważamy, że jeśli klient chce efektywnego i wszechstronnego rozwiązania, musi zabezpieczyć swoją infrastrukturę w każdym punkcie. I najważniejsze: wszystkie rozwiązania ochronne powinny komunikować się ze sobą, bo dwie z pozoru niewiele znaczące informacje skorelowane ze sobą mogą już na coś konkretnego wskazywać. To tak jakby strażnikom wewnątrz i na zewnątrz budynku dać krótkofalówki do komunikacji – oczywistym efektem będzie większe bezpieczeństwo.

CRN W takim modelu konieczne jest jednak stosowanie wszystkich rozwiązań od jednego dostawcy. Czy nie obawiacie się, że zostaniecie oskarżeni o monopolistyczne praktyki typu vendor lock-in?

Kris Hagerman Nie, ponieważ leży to w interesie klienta. Dzięki takiemu ograniczeniu zdobywa on gwarancję, że korzysta z przetestowanych w zakresie współdziałania rozwiązań, które mają unikalne możliwości, jakich nie posiadają pojedyncze produkty.

CRN Czy kiedyś powstanie otwarty standard w tej dziedzinie, a urządzenia do ochrony sieci i pakiety antywirusowe różnych dostawców zyskają interfejs API, dzięki któremu będą komunikować się ze sobą?

Kris Hagerman Nie sądzę. I znów, nie dlatego, że próbujemy na siłę utrzymać model vendor lock-in. Z zasady wspieramy otwarte standardy, ale one nie zawsze się sprawdzają, szczególnie jeśli nie obejmują głębokich struktur danego rozwiązania. W przypadku systemów ochronnych czasami zachodzi konieczność wymiany bardzo dużej ilości informacji, a w otwartych standardach często spotyka się limity w tym zakresie. Poza tym, chyba największym problemem jest fakt, że wszelkie standardy nie są rozwijane w takim tempie, w jakim rośnie rynek zagrożeń IT. Nie ma więc szans, by dogonić cyberprzestępców, nie mówiąc już o ich przegonieniu. Dlatego czasami po prostu trzeba pójść swoją drogą, nie zważając na innych, gdyż tylko w ten sposób można zapewnić wydajność rozwiązania ochronnego i bardzo krótki czas reakcji w przypadku problemów.

CRN Do całej olbrzymiej grupy zagrożeń związanych z IT dołączył ostatnio cryptojacking, czyli kopanie kryptowalut bez wiedzy i zgody użytkownika komputera...

Kris Hagerman Potwierdzam, że liczba nielegalnie uruchamianych skryptów kopiących kryptowaluty ogromnie wzrosła w ostatnim czasie, ale nie jest to najpoważniejsze zagrożenie, z jakim przyszło nam walczyć. Oprócz tego, że cryptojacking może znacznie wpłynąć na rachunek za energię zaatakowanego użytkownika, nie wyrządza żadnej innej szkody. Poza tym dość łatwo go wykryć – zdradza go bardzo wysokie wykorzystanie mocy obliczeniowej komputera.

CRN Co zatem pozostaje najtrudniejszym do rozwiązania problemem?

Kris Hagerman Zdecydowanie ransomware. Ostatnio w jednej z ankiet zapytaliśmy o ransomware 2700 menedżerów IT z różnych krajów i wyniki były porażające. Ponad połowa firm została zaatakowana przez ransomware w ciągu ostatniego roku. Co więcej, na każdą z nich przypadały średnio dwa ataki. O tym ›

rodzaju zagrożenia wiele mówiło się już w mediach, ale nadal w olbrzymiej liczbie przedsiębiorstw nie ma nawet podstawowej wiedzy na ten temat, a administratorzy nie podejmują żadnych działań, aby wprowadzić skuteczne rozwiązania ochronne. Udało się nam już nauczyć zwalczać wiele rodzajów ataków doprowadzających do zaszyfrowania danych użytkownika, ale cyberprzestępcy nie ustają w próbach wykrycia nowych luk w systemach operacyjnych i rozwiązaniach ochronnych. Na pewno w tej dziedzinie będą bardzo aktywni w najbliższych latach.

CRN Kradzież legalnie zdobytych kryptowalut jest kolejnym przykładem cyberprzestępstw. Czy macie pomysł na skuteczną ochronę przed ich utratą?

Kris Hagerman W tym przypadku najlepsze praktyki nie różnią się specjalnie od tych związanych z ochroną innych zasobów, np. w szpitalu, banku, przedsiębiorstwie handlowym czy sklepie internetowym. Konieczne jest zachowanie zdrowego rozsądku oraz zabezpieczenie prawne w postaci umowy z firmą przechowującą cyfrowe pieniądze. Nie widzę nic charakterystycznego dla kryptowalut, co mogłoby pomóc w ich ochronie.

CRN Czy podobnie można podejść do zabezpieczania rozwiązań Internetu rzeczy?

Kris Hagerman Tu sytuacja jest bardziej skomplikowana. W przypadku kryptowalut mówimy o wartości wirtualnej, tymczasem wiele rozwiązań Internetu rzeczy ma wpływ na nasze fizyczne bezpieczeństwo. Liczba rodzajów urządzeń podłączonych do Internetu rośnie wykładniczo – lodówki, dzwonki do drzwi, doniczki, termostaty itd. Pozytywne zjawisko, które dostrzegliśmy, polega na tym, że wreszcie dostawcy wspomnianego sprzętu zaczęli poczuwać się do odpowiedzialności za jego zabezpieczenie, więc przynajmniej na podstawowym poziomie jest chroniony. Ale dużo zależy od użytkowników. Powinni przede wszystkim zmieniać domyślne hasła, a tu ignorancja jest przerażająca.

CRN Czy zatem można spodziewać się rozwiązań ochronnych dla urządzeń Internetu rzeczy, stworzonych przez niezależne firmy?

Kris Hagerman Byłoby to trudne do zrealizowania, chociaż nie niemożliwe. Niektóre rozwiązania bazują na otwartych, powszechnie znanych systemach operacyjnych, chociażby na Androidzie, w których można bez problemu zainstalować antywirus. Większość jednak jest zupełnie zamknięta. Wówczas pełna odpowiedzialność za bezpieczeństwo spoczywa na producencie, ale też na wdrożeniowcu, który musi wiedzieć, co podłącza i jak wyeliminować oczywiste luki w ochronie, np. wspomniane domyślne hasła administratora i użytkownika. Niektóre firmy użytkujące rozwiązania IoT przyjmują strategię, zgodnie z którą na początku żadne z podłączanych do sieci urządzeń nie jest traktowane jako godne zaufania, a następnie powoli i uważnie przydzielane są uprawnienia do korzystania z poszczególnych zasobów. Dobrą praktyką jest też stosowanie rozwiązań analizujących dane przesyłane w sieci w celu wykrycia prowadzonego ataku.

W tej chwili istnieje ponad tysiąc niezależnych firm oferujących rozwiązania ochronne. Większość z nich nie przetrwa.

CRN W systemach IoT często wykorzystywana jest sztuczna inteligencja, także w narzędziach ochronnych. Do czego służy i czy generalnie stanowi ona przyszłość diagnostyki w zakresie bezpieczeństwa IT?

Kris Hagerman Sztuczna inteligencja jest stosowana do tzw. głębokiego maszynowego uczenia bazującego na sieci neuronowej, podobnej do struktury szarych komórek w mózgu. Jest przykładem bardzo dużego postępu w dziedzinie walki ze stale rosnącą ilością złośliwego oprogramowania. Codziennie trafia do nas 300–400 tys. unikalnych próbek malware'u. Dawniej, zanim zaczęliśmy korzystać z uczenia maszynowego, musieliśmy stosować narzędzia automatyzujące analitykę i wspierające inżynierów w zrozumieniu technik stosowanych przez cyberprzestępców. Ta metoda jednak nie wystarcza przy tak dużej liczbie próbek jak notowana obecnie i konieczne jest stosowanie bardziej zaawansowanych rozwiązań. Uczenie maszynowe i sieci neuronowe są szczególnie przydatne, bo nie tylko gwarantują ochronę przed już występującymi zagrożeniami, ale także służą do symulowania zachowania złośliwego kodu, który jeszcze nie został stworzony.

CRN Czy nie boicie się, że cyberprzestępcy pokonają was waszą własną bronią? Przecież mogą spróbować zaatakować samouczący się mechanizm odpowiednim kodem, który nauczy go, że dany malware nie stanowi żadnego zagrożenia i można pozwolić mu działać...

Kris Hagerman To ciekawa koncepcja. Teoretycznie ryzyko podjęcia takiej próby istnieje, chociaż będzie bardzo trudna do przeprowadzenia. Oczywiście uczenie maszynowe i sieci neuronowe to nadal tylko urządzenia i algorytmy, więc mogą zawierać błędy. Technologie są neutralne, mogą być użyte do dobrego i złego. Ale uczenie maszynowe jest ogromnie skomplikowane, trudne w obsłudze, wymaga bardzo zaawansowanych umiejętności i kwalifikacji. Zatem wykrycie luk w danym mechanizmie, do którego przecież cyberprzestępcy nie mają dostępu, i późniejsze wykorzystanie ich praktycznie wydaje się niemożliwe. Z drugiej strony wiemy, że cyberprzestępcy też są zainteresowani uczeniem maszynowym, aby uczynić swoje ataki skuteczniejszymi i trudniejszymi do wykrycia. Nie wszyscy będą sobie mogli na to pozwolić, więc spadnie liczba skutecznych ataków i to jest dobra wiadomość. Jednak ogólnie uważamy, że mamy przewagę – jako firma produkująca rozwiązania ochronne, stosowane w setkach milionów urządzeń końcowych na świecie, otrzymujemy z powrotem ogrom informacji. Indywidualni cyberprzestępcy nie mają szansy na zdobycie wiedzy, którą my mamy, a nawet gdyby ją uzyskali, to bez odpowiednich kwalifikacji nie umieliby jej przetworzyć. Pewne jest natomiast, że sztuczna inteligencja to kolejny etap wyścigu między dobrem i złem w kontekście IT.

KRIS HAGERMAN jest Chief Executive Officerem w Sophos od 2012 r. Odpowiada za wszystkie aspekty związane z planowaniem strategicznym i działalnością operacyjną producenta. Wcześniej był CEO w Corel Corporation oraz pełnił funkcje menedżerskie m.in. w Symantecu i Veritas Software. Był także założycielem kilku startupów.

CRN Wielu administratorów w firmach wypowiada się o inteligencji, ale... użytkowników, których zachowanie potrafi zaskakiwać. Bardzo łatwo ich zmanipulować metodami socjotechnicznymi. Czy jakikolwiek producent jest gotowy do dostarczenia rozwiązania technicznego, które będzie przeciwdziałać wpływaniu na ludzkie emocje?

Kris Hagerman W jakimś stopniu to już się dzieje, potrafimy np. z dość dużą skutecznością wyszukiwać e-maile i strony phishingowe. Ale nie uda się uniknąć odpowiedzialności człowieka, on ma ogromny i z reguły negatywny wpływ na bezpieczeństwo. Niezmiennie stoimy na stanowisku, że wykształceni użytkownicy powinni stanowić jedną z linii obrony przed cyberprzestępcami. Dlatego proponujemy partnerom i klientom różnego typu narzędzia edukacyjne, m.in. symulator ataków phishing, który umożliwia wykrycie nieostrożnych lub nieświadomych zagrożenia użytkowników oraz poinformowanie o tym zespołu ds. bezpieczeństwa oraz IT, aby przeprowadził szkolenia doskonalące.

CRN Tego typu edukacja musi być zatem procesem ciągłym.

Kris Hagerman Tak, przedsiębiorcy muszą zaakceptować fakt, że konieczne jest nieustanne szkolenie zarówno nowych, jak i zatrudnionych wcześniej pracowników. W świecie fizycznym tysiące pokoleń miało czas, aby nauczyć się zachowań, które zapewniają bezpieczeństwo. Z Internetu korzystamy mniej niż 30 lat, a rozwija się on znacznie szybciej niż świat fizyczny – powstają nowe standardy, aplikacje itp. W świecie online robimy rzeczy, których nigdy nie robiliśmy w świecie fizycznym. Gdy ktoś podejdzie do nas na ulicy i powie: „co prawda nigdy się nie spotkaliśmy, ale czy mogę spojrzeć na twoją kartę kredytową w zamian za pokazanie fajnego wideo", nigdy się na to nie zgodzimy. A w świecie online ludzie się godzą, nie wiedzą komu i czemu można zaufać. Z czasem wszyscy będą mądrzejsi, będą wiedzieć, jak kierować swoją osobowością online i swoim wirtualnym życiem. Ale to wymaga wieloletniej edukacji i praktyki.

CRN Taka postawa napotyka jednak opór odbiorców rozwiązań IT. Twierdzą, że mają prawo oczekiwać od dostawców Internetu wyeliminowania wszelkich zagrożeń, tak jak mogą oczekiwać od elektrowni prądu bez zakłóceń, a od filtrów czystej wody w kranie...

Kris Hagerman W naszej branży, szczególnie w kontekście chmury, często stosuje się porównania z instytucjami użyteczności publicznej. Są jednak niewłaściwe, przede wszystkim dlatego, że w świecie online komunikacja jest dwustronna – nie tylko konsumujemy treści, jak w przypadku telewizji, ale także tworzymy je i udostępniamy. Ludzie chcą mieć nieskrępowany dostęp do wszystkiego. Dostawca usługi mógłby powiedzieć, że zagwarantuje bezpieczeństwo, ale to będzie oznaczać, że odbiorca straci dostęp do ulubionej strony lub e-maili od danej osoby, ponieważ jej komputer nie jest zabezpieczony. Na to nie zgodzi się większość użytkowników. Faktem jest, że dostawcy usług internetowych i tak blokują wiele ataków, np. DDoS, ale moim zdaniem nie powinni integrować w przesyłane treści.

CRN Na rynku rozwiązań ochronnych IT to resellerzy i integratorzy są najbliżej klientów i dzięki zdobytemu zaufaniu stanowią bardzo ważne ogniwo w łańcuchu sprzedaży. Jednocześnie często narzekają, że ta dziedzina jest wyjątkowo skomplikowana, a zmiany na rynku następują tak szybko, że bardzo trudno za nimi nadążyć. Jaką radą możecie służyć partnerom, aby ich proces edukacyjny przebiegał szybciej oraz by stawali się coraz lepsi w świadczeniu usług związanych z bezpieczeństwem IT?

Kris Hagerman Jak ważna jest współpraca z partnerami, świadczy fakt, że to jeden z najważniejszych punktów wpisanych w naszą misję i strategię. Tylko dzięki niej można odnieść sukces. Jesteśmy jednak świadomi wyzwań z tym związanych. Niestety, liczba rodzajów zagrożeń i poziom ich skomplikowania cały czas rośnie. Wartość sprzedaży rozwiązań cyberochronnych na świecie przekroczyła już 40 mld dol. w skali roku i jest najszybciej – o 7 proc. rocznie – rosnącym segmentem branży IT. Dlatego uważamy, że to producenci tych rozwiązań powinni wziąć na siebie odpowiedzialność za uczynienie życia partnerów i klientów łatwiejszym. Produkty powinny być proste nie tylko w obsłudze, ale też we wdrażaniu. Złożoność jest wrogiem bezpieczeństwa.

Rozmawiał Krzysztof Jakubik

Od podstaw
do sztucznej inteligencji

Klientom trzeba uświadamiać, że o właściwej ochronie sieci powinni myśleć przed szkodą, a nie dopiero po niej. To stwierdzenie nabiera jeszcze większej mocy w obliczu konsekwencji przewidzianych w RODO.

Tomasz Janoś

Ilustracje AdobeStock

Zdaniem integratora

Grzegorz Kędziora, kierownik ds. kluczowych klientów, IMNS

Niezmiennie podstawą ochrony sieci są wszelkiego rodzaju firewalle nowej generacji, bo oferując wiele funkcji, zastąpiły urządzenia brzegowe realizujące pojedyncze zadania. Klientom zależy zwłaszcza, by chroniły przed atakami z wykorzystaniem ruchu szyfrowanego, których jest coraz więcej. Wcześniej szyfrowana komunikacja była poza kontrolą firewalli, ale teraz standardem stało się już rozszyfrowanie sesji SSL. Ważnym elementem nowoczesnego firewalla jest sandboxing. Klienci chcą też kontroli dostępu do sieci, uzyskiwanego za pomocą urządzeń mobilnych. Ci, którzy korzystają z usług zewnętrznych, potrzebują rozwiązania do zarządzania dostępem uprzywilejowanym. Ze swojej strony dostarczamy klientom kompleksową ochronę w formie sprzętowej lub programowej, przy czym bardzo istotna jest wartość dodana, wynikająca z naszych kompetencji. Najwięcej zarabia się bowiem na sprzedaży usług, czyli dokładaniu swojej wiedzy i doświadczenia do oferowanych produktów. Sprzedajemy swój pomysł na bezpieczeństwo, pokazując klientom, jak można sieć podzielić i skonfigurować, czy też jak kontrolować użytkowników, czyli optymalnie wykorzystać kupione narzędzia.

Gdy rośnie złożoność i skala zagrożeń, coraz liczniejsza grupa klientów przekonuje się o konieczności posiadania zabezpieczeń chroniących przed atakami nowego typu. Najczęściej w firmach stosuje są wydajne UTM-y lub zapory sieciowe. Ważnym elementem stał się sandboxing umożliwiający neutralizowanie niezidentyfikowanego złośliwego kodu i zapobieganie atakom typu zero-day. Rośnie też rola kontroli dostępu uprzywilejowanego, zwłaszcza w kontekście RODO. Statystyki nie pozostawiają wątpliwości – wśród naruszeń bezpieczeństwa określanych jako wewnętrzne, większość jest związana z wykorzystaniem kont z prawami administratora.

W walce z cyberzagrożeniami wciąż problem stanowi zbyt późne identyfikowanie ataków. W szybkim wykrywaniu incydentów i reagowaniu na nie pomóc mają rozwiązania w rodzaju SIEM (Security Information and Event Management), zapewniające szeroki wgląd w system IT oraz funkcje monitorowania i analizy zdarzeń w czasie rzeczywistym. Problem w tym, że często wgląd ten bywa zbyt szeroki, dostarczana jest masa danych i trudno wyłowić te, które mają jakieś znaczenie. Dlatego z jednej strony rośnie rola zewnętrznych usług, a z drugiej automatyzacji – usprawniającej wykrywanie zagrożeń i bazującej na algorytmach maszynowych.

Dobry firewall to wciąż podstawa

Gdy zaobserwowano jak duże szkody wyrządził ransomware WannaCry zmieniło się podejście do bezpieczeństwa sieci. Gdy coraz częściej mają miejsce ataki dnia zerowego, w których wykorzystywane są nieujawnione wcześniej luki w zabezpieczeniach systemów i aplikacji, UTM oparty na zabezpieczeniach sygnaturowych przestaje wystarczać.

– *Tradycyjne narzędzia nie zapobiegną już atakowi, w wyniku którego dojdzie do zaszyfrowania dysków lub innych szkód* – tłumaczy Mariusz Bajgrowicz, Security Product Manager w Ingram Micro.

Podstawą aktywnej ochrony sieci pozostaje zatem UTM, ale już nie tylko z typowymi licencjami obejmującymi: antywirus, antyspam, IDS/IPS i podstawowy filtr sieciowy. Nowe platformy zapewniają detekcję i zapobieganie zaawansowanym atakom, a także działania naprawcze. W tym celu mogą wykorzystywać heurystykę i analizę zachowań, sandboxing, sieci reputacyjne, zarządzanie informacją o zagrożeniach (Threat Intelligence) i inne mechanizmy.

Rosnącą popularnością cieszy się zwłaszcza sandboxing, który jest realizowany w chmurze albo lokalnie, w ramach platformy sprzętowej. Są klienci, którzy wybierają sandboxing jako uzupełnienie posiadanych rozwiązań UTM. W ostatnich latach nastąpił znaczny spadek cen sprzętu, po części spowodowany agresywną polityką producentów, którzy chcą w ten sposób zwiększać swoje udziały rynkowe. Firmy używające kilkuletnich urządzeń często decydują się zatem na ich wymianę na zupełnie nowe, oferujące więcej funkcji, w tym właśnie „piaskownicę".

Nawet, gdy firma już dysponuje tak wyrafinowanymi mechanizmami, jak sandboxing, administrator nie może zapominać o podstawowych regułach zapewnienia bezpieczeństwa. Dlatego bardzo ważną funkcją platformy ›

W opinii branży

Krzysztof Hałgas, dyrektor, Bakotech

Sławomir Karpiński, prezes, Connect Distribution

Mariusz Bajgrowicz, Security Product Manager, Ingram Micro

Paweł Rybczyk, Business Developer CEE&Russia, Wallix

Grzegorz Krzątała, Channel Leader, Juniper Networks

Dawid Królica, Area Sales Manager, Extreme Networks

KRZYSZTOF HAŁGAS Działanie w modelu usługowym to dziedzina, która w ostatnim czasie najszybciej się rozwija. Gdy zatrudnienie dobrego administratora stało się problemem, decydujący się na zewnętrzną usługę klient nie musi martwić się o wykwalifikowanych specjalistów. Dzięki niej ma dostęp do fachowców o potrzebnych kompetencjach. Taki model działania sprawia także, że klient ma szersze pole manewru – może łatwo zrezygnować z niepotrzebnej już usługi lub zmienić ją na inną. Dlatego obserwujemy systematyczny wzrost znaczenia oferty usługowej. To już nie są tylko najprostsze rozwiązania, w tej formie klient może już kupić praktycznie większość narzędzi zapewniających bezpieczeństwo IT.

SŁAWOMIR KARPIŃSKI Sytuacja na rynku UTM-ów dynamicznie się zmienia. Rozwiązania i marki, które jeszcze parę lat temu były poza zasięgiem finansowym polskich klientów, dziś są dla nich dostępne. Poza ceną, na którą klienci nadal zwracają baczną uwagę, ważna jest wydajność. I to nie tylko opisana w specyfikacji urządzenia, lecz potwierdzona przez praktyczne testy. A są produkty, w których po włączeniu wszystkich funkcji ochrony wydajność spada dramatycznie. Dlatego nawet w małych projektach ważny jest etap Proof of Concept, podczas którego weryfikuje się rzeczywiste możliwości rozwiązania.

MARIUSZ BAJGROWICZ Rozwiązania typu UTM/NGFW są oferowane w cenach na tyle atrakcyjnych, że przedsiębiorcy często wolą kupić nowe urządzenie, niż przedłużać umowę wsparcia dla starszego sprzętu. W ten sposób, praktycznie za cenę odnowienia posiadanych licencji i wsparcia, otrzymują lepszą ochronę, lepiej przystosowaną do aktualnych, a także przyszłych zagrożeń. Nowe urządzenia są znacznie wydajniejsze i wyposażone w bogatsze funkcjonalnie oprogramowanie, zapewniające lepsze zarządzanie. Najczęściej umożliwiają też wykorzystanie wielu mechanizmów obrony przed zaawansowanymi atakami dnia zerowego, w tym sandboxing.

PAWEŁ RYBCZYK W obszarze bezpieczeństwa sieci mamy dwie warstwy kontroli. Pierwsza obejmuje przepływ danych przez sieć, który w ramach ochrony jest analizowany przez rozmaite narzędzia pod kątem incydentów. Druga to zarządzanie dostępem w odniesieniu nie tylko do punktów końcowych – baz danych, serwerów, urządzeń użytkowników – ale także elementów tworzących firmową sieć, przełączników, routerów oraz firewalli. W drugim przypadku bardzo ważne jest zarządzanie kontami uprzywilejowanymi oraz kontrola zautomatyzowanej komunikacji między urządzeniami a aplikacjami.

GRZEGORZ KRZĄTAŁA W zapewnianiu bezpieczeństwa sieci ważne są trzy elementy. Po pierwsze, rozciągnięcie funkcjonalności NGFW na wszystkie elementy infrastruktury sieciowej. Już nie tylko firewall, ale i przełączniki oraz routery muszą pełnić rolę elementów, które służą do egzekwowania reguł polityki bezpieczeństwa. Po drugie, kluczowa staje się pełna automatyzacja reagowania na incydenty bezpieczeństwa. Obecnie administratorzy nie poradzą sobie sami, to sieć musi wykryć atak i podjąć właściwe działania, aby wyizolować zagrożenie i nie dopuścić do jego rozprzestrzeniania się. I wreszcie trzeci element: ochrona środowisk fizycznych oraz wirtualnych i to nie tylko we własnej infrastrukturze, ale także w zasobach chmurowych.

DAWID KRÓLICA Wiele przedsiębiorstw doświadczyło strat finansowych i wizerunkowych z powodu ataków wykorzystujących niezabezpieczone punkty końcowe połączone z firmową siecią. Rozwiązaniem nie może być tylko odcięcie portów albo zwiększenie fizycznej ochrony w budynku. Efektywna kontrola dostępu wymaga proaktywnego podejścia i zagwarantowania, by wszystkie urządzenia końcowe były właściwie zabezpieczone i wolne od niebezpiecznych plików, zanim zostanie im przyznany dostęp do wewnętrznych zasobów sieciowych danej firmy.

ochronnej jest wymuszanie instalowania aktualizacji systemowych na urządzeniach końcowych, jak tylko się pojawią. Warto zwracać zatem uwagę klientów na fakt, że pozostawienie niezałatanej luki jest jak otwarcie drzwi do systemu informatycznego z zaproszeniem do ataku. Można przy tym demonstrować, jak proces dostarczania łatek jest realizowany przez poszczególnych producentów platform bezpieczeństwa sieciowego.

Istotnym elementem UTM powinna być także ochrona sieci bezprzewodowych. O ile LAN bywa dobrze zabezpieczony, o tyle o firmy zwykle zapominają o WiFi. Punkty dostępowe, przez które łączy się wiele osób, są bardzo często pozbawione ochrony realizowanej przez UTM, a zatem rozwiązanie, które integruje bezpieczeństwo obu rodzajów sieci, bardzo się przydaje.

Szyfrowanie to broń obosieczna

Wzrost ilości przesyłanych zaszyfrowanych danych, które w październiku ubiegłego roku stanowiły aż połowę globalnego transferu (generowanego zarówno przez zwykłych użytkowników, jak i cyberprzestępców), postawił przed specjalistami ds. cyberbezpieczeństwa nowe wyzwania związane z monitorowaniem zagrożeń. Z jednej strony stosowane obecnie na dużą skalę szyfrowanie połączeń i danych w spoczynku wyraźnie zwiększa poziom ich bezpieczeństwa, z drugiej także cyberprzestępcy wykorzystują ruch szyfrowany, np. w celu ukrycia zapytań wysyłanych do serwerów Command and Control. W ciągu ostatniego roku eksperci Cisco zaobserwowali trzykrotny wzrost częstości wykorzystywania szyfrowanej komunikacji sieciowej w sprawdzanym ruchu związanym z plikami malware. Konieczne staje się więc użycie właściwych mechanizmów ochrony.

W efekcie niezbędnym elementem zabezpieczenia firmowych sieci są wszelkiego rodzaju bramy VPN. Rozwiązania przeciwdziałające atakom, bazujące na ruchu zaszyfrowanym, wchodzące w skład nowoczesnych platform UTM/NGFW lub oferowane jako oddzielne produkty, przeprowadzają analizę źródeł komunikacji i certyfikatów bezpieczeństwa oraz wykorzystują proxy SSL. Ten ostatni mechanizm zapobiega nawiązaniu bezpośredniej komunikacji z urządzeniem końcowym i – działając zgodnie ze schematem legalnego „man in the middle" – rozdziela jedno połączenie na dwa: ze źródłem ruchu i z chronionym użytkownikiem.

Wzrośnie popularność rozwiązań automatycznie analizujących ruch sieciowy z wykorzystaniem sztucznej inteligencji.

Czasy, gdy na zakup NGFW mogli sobie pozwolić tylko najwięksi i najbogatsi klienci, to już przeszłość. Producenci coraz częściej oferują rozwiązania, które mogą chronić zarówno małe firmy, jak i korporacje. Zapewniają, jeśli nie taki sam, to bardzo zbliżony poziom zabezpieczeń. Ceny można zatem dostosować do finansowych możliwości klienta.

– *Inna jest tylko wielkość „pudełka", skalowalność i wydajność rozwiązania. Natomiast wykorzystywane są te same silniki antywirusowe, tak samo działa obsługa SSL i sandboxing* – wyjaśnia Mariusz Bajgrowicz.

Kontrola dostępu, zwłaszcza uprzywilejowanego

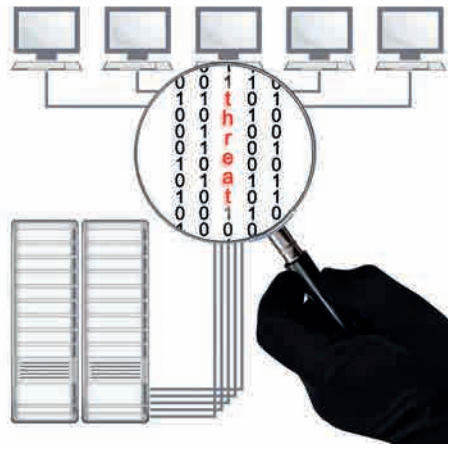
Kontrola dostępu do sieci to jeden z najistotniejszych aspektów bezpieczeństwa sieciowego. Decyduje o tym, kto ma dostęp, do jakiego zasobu i przy użyciu jakiego urządzenia. Może zapobiec łączeniu się z siecią z nieautoryzowanych urządzeń, ograniczyć dostęp do określonych plików i zasobów sieciowych, określić jakie uprawnienia powinny być przydzielone poszczególnym osobom w firmie. Uwzględnione w procesie projektowania sieci mechanizmy kontroli dostępu ułatwiają wprowadzanie zawartej w przepisach RODO zasady Privacy by Design i zapobiegają kradzieży informacji.

Obecnie stosowanie całościowych rozwiązań typu Network Access Control w przedsiębiorstwach jest utrudnione. Kontrolą dostępu muszą być bowiem objęte nie tylko zestandaryzowane korporacyjne komputery PC, ale i mnóstwo rozmaitego sprzętu mobilnego (często będącego własnością użytkowników). Do tego dochodzą urządzenia tworzące Internet rzeczy, zwirtualizowane serwery itp. W dodatku do sieci podłączają się nie są tylko pracownicy firmy, ale także usługodawcy, serwisanci, partnerzy, dostawcy lub goście. Dlatego producenci zaczęli się skupiać na określonych rodzajach dostępu, tworząc prostsze w użyciu, a dzięki temu skuteczniejsze narzędzia ochronne.

Ze względu na nowe przepisy o ochronie danych osobowych dostawcy zwracają uwagę klientów na to, jak ważne staje się zarządzanie dostępem uprzywilejowanym. Rośnie potrzeba stosowania rozwiązań Privileged Access Management, zwłaszcza wykorzystania ich podstawowych funkcji, czyli nagrywania sesji i zarządzania hasłami. Wynika to przede wszystkim z coraz powszechniejszego wykorzystania w firmach outsourcingu, który sprawia, że użytkownikom spoza firmy przydziela się dostęp do najważniejszych jej zasobów (w tym wrażliwych danych), często właśnie na poziomie uprzywilejowanym, a przy tym bardzo słabo kontrolowanym. Standardowa funkcja PAM, czyli nagrywanie sesji, po pierwsze zapewnia bezpieczeństwo (zniechęcając zarejestrowanego użytkownika do nadużyć i prowadząc dokumentację wszelkich działań potrzebną do audytu i ewentualnych dochodzeń śledczych), po drugie – umożliwia dokładne rozliczanie z wykonanej pracy.

Jednak rozwiązania PAM to dużo więcej niż nagrywanie sesji. Dzięki nim można ułatwić klientom ochronę zasobów i przestrzeganie regulacji prawnych bądź branżowych przez zabezpieczanie, zarządzanie oraz monitorowanie uprzywilejowanych kont i uzyskiwanego za ich pomocą dostępu. Taka ochrona obejmuje różne elementy systemowe i infrastrukturalne – od systemów operacyjnych, baz danych i aplikacji po urządzenia sieciowe, wirtualizatory i chmurowe aplikacje SaaS.

Nic nie zastąpi własnych testów



W wyborze platform bezpieczeństwa sieciowego klienci mogą zwracać uwagę na wyniki testów przeprowadzanych przez niezależne organizacje. Przykładowo, pokazują one jak spada wydajność wielofunkcyjnego firewalla po włączeniu kolejnych mechanizmów ochrony. Dostawcy i ich partnerzy twierdzą, że w sprzedaży tego typu urządzeń (i wszelkich rozwiązań ochrony sieciowej) wyraźnie pomaga pozycja zajmowana przez producenta w magicznym kwadrancie Gartnera. W ocenie producentów ważne są też raporty przedstawiające ich zaangażowanie w wykrywanie dotychczasowych zagrożeń oraz przygotowanie do przyszłych zadań.

Skuteczniej niż zewnętrzne testy i raporty przekona jednak potencjalnego nabywcę okazja sprawdzenia możliwości systemów UTM/NGF w środowisku funkcjonującym w jego firmie. Warto zatem przedsiębiorstwu poszukującemu nowego rozwiązania zapewnić do testów kilka rozwiązań z tej samej półki cenowej i ułatwić porównanie ich możliwości. Wpięcie urządzenia do sieci i uzyskanie po dwóch tygodniach jego używania raportów mówiących, ile jest luk w systemie, ile szkodliwego oprogramowania przepuściły obecnie wykorzystywane zabezpieczenia, a także sprawdzenie, jak przyjazny i funkcjonalny jest interfejs zarządzania, to najlepszy sposób na dobranie właściwej dla danego środowiska platformy UTM.

Za dużo alertów, za mało specjalistów

Rozwiązania typu UTM/NGFW to bardzo pożyteczne, wręcz niezbędne narzędzia do ochrony sieci – pokazują, co się dzieje w systemie. Informacje są zapisywane w logach, które następnie gromadzi rozwiązanie SIEM. Ma to pomóc w szybkim wykrywaniu incydentów i reagowaniu na nie, zapewniając szczegółowy wgląd w system IT oraz funkcje monitorowania i analizy zdarzeń w czasie rzeczywistym. To kolejny element, na którym powinno bazować zabezpieczanie sieci w każdym przedsiębiorstwie, tym bardziej że platformy SIEM „trafiły pod strzechy".

– *Jeszcze kilka lat temu tego typu rozwiązania, oferowane przez zaledwie kilku dostawców, były drogie i przeznaczone wyłącznie dla bardzo dużych firm. Nawet średnie przedsiębiorstwa nie brały pod uwagę zakupu tego produktu* – zauważa Krzysztof Hałgas, dyrektor Bakotechu.

Obecnie w sprzedaży znajduje się ogromna liczba narzędzi zapewniających agregowanie i korelowanie logów systemowych. A SIEM stał się podstawowym elementem ochrony sieci, szczególnie że jako rozwiązanie gromadzące informacje o tym, to co się w niej zdarzyło, zyskuje na znaczeniu w kontekście RODO.

Administratorzy muszą się obecnie mierzyć z wielką masą informacji generowanych przez platformy UTM/NGFW/IDS/IPS, agregowanych i korelowanych przez rozwiązania typu SIEM. Problemem jest jednak trudna do prześledzenia liczba ujawnianych zdarzeń, z których zdecydowana większość jest odchyleniem od normy, ale w rzeczywistości nie ma związku z żadnym atakiem. Przykładowo, skanowanie portów serwera może być wstępem do ataku, ale najczęściej nie jest.

– *Jeśli administratorzy mają pod opieką środowisko złożone z wielu setek czy tysięcy urządzeń, z których SIEM agreguje logi i wysyła alerty o każdym podejrzanym zdarzeniu, w krótkim czasie przestają w ogóle reagować na te ostrzeżenia* – twierdzi Paweł Rybczyk, Business Developer CEE&Russia w firmie Wallix.

W dodatku na rynku brakuje specjalistów ds. bezpieczeństwa, którzy mogliby logi sprawdzać i interpretować. To szansa dla integratorów, którzy w charakterze dostawców zewnętrznych usług zarządzanych mogą rozbudować ofertę dla klientów o Security Operations Center as a Service. Oczywiście musi być to usługa z prawdziwego zdarzenia, bo oferowanie klientowi sprawdzania logów raz na tydzień mija się z celem.

Automatyzacja, a nawet sztuczna inteligencja

Równolegle do rozwoju usług zewnętrznych będzie rosło znaczenie rozwiązań, które – wykorzystując sztuczną inteligencję oraz uczenie maszynowe – mogą automatycznie analizować ruch sieciowy. Mechanizm ich działania polega na uczeniu się wzorców w działającej sieci i na tej podstawie identyfikowaniu odchyleń od normy. Obserwujemy obecnie pierwsze zastosowania sztucznej inteligencji w zakresie bezpieczeństwa sieciowego.

– *Celem jest użycie algorytmów zamiast sygnatur w analizie ruchu sieciowego po to, by liczba alertów zmniejszyła się z tysięcy do kilku tygodniowo, za to rzeczywiście istotnych dla bezpieczeństwa* – wyjaśnia Paweł Rybczyk.

Według autorów raportu Cisco 2018 Annual Cybersecurity Report wdrażanie rozwiązań z zakresu uczenia maszynowego zwiększy bezpieczeństwo sieci, ponieważ w dalszej perspektywie mogą one „nauczyć się" wykrywać wzorce w szyfrowanych połączeniach, chmurze oraz środowisku Internetu rzeczy. Część z 3,6 tys. profesjonalistów, którzy wzięli udział w ankiecie Cisco, przyznaje, że chętnie uzupełniłoby portfolio posiadanych narzędzi o rozwiązania z zakresu uczenia maszynowego oraz sztucznej inteligencji, ale zniechęca ich duża liczba błędnych alertów (false positives) generowanych przez te systemy. Dalszy rozwój wspomnianych, wciąż nowatorskich, technik zapewne znacząco zwiększy liczbę prawidłowych wskazań w monitorowanym środowisku sieciowym.

SonicWall – dużo więcej niż firewalle

Rozbudowana oferta produktowa sprawia, że partnerom amerykańskiego producenta dużo łatwiej będzie zdobyć nowych klientów, a dotychczasowym zaproponować kolejne rozwiązania tworzące zunifikowaną platformę ochrony sieci oraz urządzeń końcowych.

W kwietniu br. do oferty firmy SonicWall trafiła nowa grupa produktów ochronnych – Capture Cloud Platform. Składa się na nią kilka rodzajów firewalli oraz oprogramowanie do zabezpieczania punktów końcowych.

Do ochrony najważniejszych firmowych komponentów w wirtualnych środowiskach prywatnych klientów i chmurach publicznych partnerzy mogą wykorzystać nowe firewalle z rodziny **Network Security virtual**. Modele te mają wszystkie zalety fizycznego rozwiązania, a dodatkowo zapewniają operacyjne i ekonomiczne korzyści wynikające z wirtualizacji. NSv daje wgląd w komunikację między maszynami wirtualnymi i automatycznie zapobiega włamaniom oraz rozprzestrzenianiu się malware'u. Zapewnia egzekwowanie reguł polityki bezpieczeństwa dotyczących aplikacji w środowisku wirtualnym.

Nowy w ofercie SonicWall **Web Application Firewall** oferuje zaawansowane funkcje ochrony aplikacji webowych uruchamianych w środowiskach chmury prywatnej, publicznej bądź hybrydowej. Jest to kompletne, łatwe w użyciu i gotowe do pracy „wprost z pudełka" rozwiązanie, którym powinny zainteresować się przede wszystkim podmioty ze ściśle regulowanych sektorów gospodarki. Ułatwia im utrzymanie zgodności z przepisami, dzięki temu, że zapewnia ochronę wrażliwych danych i niezakłócone działanie aplikacji webowych.

WAF, podobnie jak wirtualne firewalle z serii NSv, może być stosowany jako wirtualne urządzenie w chmurach prywatnych, bazujących na VMware lub Microsoft Hyper-V, a także w środowiskach tworzonych w chmurach publicznych, takich jak Amazon Web Services czy Microsoft Azure.

Z kolei rozwiązanie **Capture Client Endpoint Protection** to zunifikowana platforma wyposażona w wiele mechanizmów ochrony punktów końcowych. Znacząco upraszcza analizę DPI-SSL zaszyfrowanego ruchu i rozwiązuje wielki problem z dostarczaniem certyfikatów do wszystkich punktów końcowych. Zapewnia instalowanie i zarządzanie zaufanymi certyfikatami na wszystkich urządzeniach zainstalowanych za firewallem. Ponieważ obecnie szyfruje się 68 proc. całego ruchu, wykorzystanie mechanizmu DPI-SSL jest kluczowe dla ochrony przed atakami omijającymi tradycyjne zabezpieczenia.

Na odświeżoną serię sprzętowych firewalli nowej generacji **Network Security appliance** składają się z modele 3650, 4650 oraz 5650 (wcześniej zostało zaprezentowane urządzenie 2650). Nowe urządzenia w porównaniu z poprzednikami oferują dwa razy więcej połączeń SPI (do 4 mln) oraz cztery razy więcej DPI-SSL. Bazują na wielordzeniowej architekturze sprzętowej i udostępniają wydajne interfejsy 10 GbE i 2,5 GbE. Na tle konkurencji wyróżnia je zwłaszcza dostępność portów 2,5 GbE – dzięki nim można w pełni korzystać z gigabitowej wydajności bezprzewodowych punktów dostępowych w standardzie 802.11ac Wave 2.

Nowością jest także kolejna wersja (SonicOS 6.5.1) przedstawionego w 2017 r. i przełomowego w rozwoju SonicWall systemu operacyjnego SonicOS 6.5.0 (wprowadzono ponad 60 nowych funkcji). Aktualizacja zapewnia dwukierunkowe API i nawet 18-krotnie większą liczbę połączeń DPI-SSL.

SEBASTIAN CYGAN
Security Sales Manager Poland and Baltic States, SonicWall

Misją firmy SonicWall jest zapewnienie firmom każdej wielkości skutecznej ochrony przed narastającą falą cyberataków. A skala i zaawansowanie zagrożeń rosną bardzo szybko – tylko w pierwszym kwartale 2018 r. klienci chronieni przez rozwiązania SonicWall doświadczyli średnio 7739 prób ataków malware (wzrost o 151 proc. rok do roku). Co ważne, 335 było przeprowadzanych z użyciem szyfrowania SSL/TSL. W tym samym czasie producent zidentyfikował niemal 50 tys. nowych wariantów ataków, a dzięki mechanizmowi Real-Time Deep Memory Inspection odkryto 3,5 tys. zagrożeń zupełnie nowego typu. Reakcją SonicWalla na ten „stan wyjątkowy" jest platforma bezpieczeństwa Capture Cloud Platform.

Dodatkowe informacje: **SEBASTIAN CYGAN**, SECURITY SALES MANAGER POLAND AND BALTIC STATES, SONICWALL, TEL. 513 099 200, SCYGAN@SONICWALL.COM
MARIUSZ BAJGROWICZ, SECURITY PRODUCT MANAGER, INGRAM MICRO, TEL. 785 403 220, MARIUSZ.BAJGROWICZ@INGRAMMICRO.COM

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI SONICWALL I INGRAM MICRO.

Bezpieczne sieci z Juniper Networks

W ostatnich latach stale rośnie skala oraz złożoność cyberzagrożeń. Każdego dnia pojawiają się informacje o spektakularnych atakach lub wyciekach danych, które są ich konsekwencją. Ataki te stają się coraz bardziej medialne, co często jest dodatkową zachętą dla przestępców.

W obliczu coraz bardziej wyrafinowanych ataków klasyczne podejście do cyberbezpieczeństwa i stosowanie brzegowych systemów ochrony (firewalli lub next generation firewalli) wraz z zabezpieczeniami stacji końcowych przestało być wystarczające. Konieczne jest stosowanie kompleksowych oraz nowocześniejszych zabezpieczeń, które poza podstawową ochroną oferują rozbudowaną warstwę automatyzacji procesów oraz możliwość szybkiego reagowania na incydenty.

W odpowiedzi na te wyzwania firma Juniper Networks opracowała koncepcję Software Defined Secure Network (SDSN). Uwzględnia ona wiele rozwiązań, które zapewniają zautomatyzowane zabezpieczanie infrastruktury IT i wymuszanie (enforcement) ochrony wszystkich elementów architektury sieciowej. Rozwiązanie to znajduje się w ofercie firmy Nuvias – dystrybutora Juniper Networks w Polsce.

Ochrona w każdym punkcie

Kluczowym elementem rozwiązania SDSN jest oprogramowanie Security Director umożliwiające scentralizowane zarządzanie regułami firmowej polityki bezpieczeństwa, szczegółową analizę środowiska sieciowego oraz automatyzację procesów zapewniających reakcję na incydenty. Security Director jest integrowany z firewallami Juniper Networks SRX oraz usługą sandbox JuniperNetworks Sky ATP dostępną w chmurze. Pobierane przez użytkowników pliki na bieżąco dostarczane są przez firewalle SRX do usługi Sky ATP w celu wielostopniowej analizy zawartości, która ma służyć wykryciu oraz identyfikacji złośliwego oprogramowania. Urządzenia SRX, działając jako SSL Proxy, przekazują do inspekcji dane, przesyłane protokołami HTTP, SMTP i IMAP, w postaci zarówno nieszyfrowanej, jak i zaszyfrowanej (SSL).

W przypadku, gdy pobierany plik jest znanym zagrożeniem, jego transfer zostaje zablokowany w firewallu SRX w czasie rzeczywistym. W przeciwnym przypadku, jego analiza w sandboksie może potrwać kilka minut. W takiej sytuacji ze względu na komfort użytkowników plik musi zostać dostarczony do odbiorcy wraz z potencjalnie szkodliwą zawartością. Ale nie są oni w tej sytuacji całkowicie pozbawieni ochrony. Natychmiast po zakończonej analizie w usłudze Sky ATP i rozpoznaniu nowego zagrożenia Security Director zmienia reguły polityki bezpieczeństwa stosowane w firewallach serii SRX oraz filtry ruchu w przełącznikach Juniper Networks serii EX lub QFX, co uniemożliwia rozprzestrzenianie się malware'u w sieci klienta. Wszystkie te działania podejmowane są automatycznie – zgodnie ze zdefiniowaną polityką – i nie ma potrzeby ręcznego blokowania stacji.

Taka metoda działania daje użytkownikom skuteczne narzędzie do walki z nowoczesnym złośliwym oprogramowaniem, wykorzystującym równolegle wiele wektorów ataków, takich jak WannaCry. Tym ransomware'em, należącym do najbardziej szkodliwych oraz inwazyjnych w historii, zainfekowanych zostało ponad 200 tys. firm w 150 krajach. WannaCry dostawał się pierwotnie do komputerów użytkowników w klasyczny sposób (phishing, watering hole) – najczęściej był pobierany z Internetu lub załączony do phishingowych e-maili. Po uruchomieniu ransomware WannaCry szyfrował pliki na komputerach ofiar oraz zaczynał rozprzestrzeniać się w sieci lokalnej w sposób typowy dla robaków internetowych. Wykorzystywał podat-

ność dnia zerowego w protokole Samba (szeroko stosowanym w systemach Windows), która umożliwiała niekontrolowane rozprzestrzenianie się malware'u na komputery innych osób w przedsiębiorstwie. Straty poniesione globalnie w wyniku braku odpowiednich zabezpieczeń oraz braku kopii zapasowych w firmach liczone były w miliardach dolarów.

Zastosowanie rozwiązania SDSN może pomóc w powstrzymaniu tego rodzaju ataku co najmniej na kilka sposobów. Zainfekowany plik podczas pobierania zostałby poddany analizie w sandboksie Sky ATP i zablokowany na firewallu Juniper Networks SRX w czasie rzeczywistym. W przypadku gdyby malware był nieznany, a dostałby się na stację roboczą, po przeprowadzeniu analizy w sandboxie i rozpoznaniu złośliwej aktywności stacja robocza zostałaby odizolowana na przełączniku, dzięki czemu powstrzymanoby rozprzestrzenianie malware'u. Poniesione straty zostałyby ograniczone do minimum lub w ogóle by do nich nie doszło.

Rozwiązanie uniwersalne

SDSN współpracuje z większością produktów w portfolio Juniper Networks, ale można go też integrować z rozwiązaniami innych producentów w celu odbierania informacji o incydentach oraz wymuszania ochrony. Reguły polityki w oprogramowaniu Security Director mogą być automatycznie zmieniane na podstawie zdarzeń z systemów zabezpieczeń innych dostawców, a także przełączników innych producentów (np. Cisco, HPE), mogą automatycznie izolować zainfekowane stacje robocze zgodnie z regułami zdefiniowanymi w Security Director. Jednym z kluczowych warunków zrealizowania takiej integracji jest zastosowanie uwierzytelnienia stacji roboczych protokołem 802.1X oraz wykorzystanie serwera RADIUS wymienionego na liście kompatybilnych urządzeń (m.in. Cisco ISE, HPE Aruba Clearpass).

Juniper Networks SDSN jest systemem otwartym i elastycznym. Może z powodzeniem być wdrożony w istniejących już środowiskach sieciowych i nie wymaga wprowadzania rewolucyjnych zmian. Dzięki zastosowaniu SDSN zróżnicowana infrastruktura sieciowa może zostać objęta spójną polityką ochrony i zmienić się w aktywny element, znacznie podnoszący poziom bezpieczeństwa w sieci. Architekturę SDSN uzupełniają rozwiązania do zarządzania incydentami w infrastrukturze klienta (SIEM). Producent oferuje platformę Juniper Networks Security Analytics (JSA), która m.in. umożliwia zbieranie logów z wielu rodzajów urządzeń sieciowych, ochronnych i serwerów, efektywną ich korelację, dzięki czemu pozwala na identyfikację podejrzanych incydentów.

Juniper Networks stale pracuje nad poszerzeniem portfolio rozwiązań cyberbezpieczeństwa, co gwarantuje coraz bardziej zaawansowane metody ochrony zasobów, skuteczniejsze rozwiązywanie problemów i spełnianie wymagań klientów każdej wielkości. Przykładem dojrzałego, kompleksowego podejścia do zagadnień cyberbezpieczeństwa jest transakcja z ostatnich miesięcy, gdy producent kupił firmę Cyphort, jednego z liderów rynku rozwiązań typu sandbox w środowisku lokalnym.

>>> Trzy pytania do...

Pawła Marciniaka, dyrektora polskiego oddziału Nuvias

CRN Jakiego typu klienci mogą być zainteresowani rozwiązaniem SDSN?

Paweł Marciniak Są to raczej firmy średnie, duże i bardzo duże, głównie ze względu na wysoki koszt tych rozwiązań. W naturalny sposób najczęściej systemami SDSN są zainteresowane przedsiębiorstwa z branży finansowej i przemysłowej, a także placówki użyteczności publicznej. Ważne jest, aby pracownicy ich działów IT mieli podstawową wiedzę na temat bezpieczeństwa oraz zarządzania zdarzeniami w sieci, bo to podstawa pracy z oprogramowaniem typu SIEM. Ale oczywiście mogą korzystać z eksperckiej wiedzy zewnętrznych podmiotów, np. integratorów, którzy dokonują danego wdrożenia.

CRN Jakimi cechami rozwiązania SDSN najbardziej interesują się klienci?

Paweł Marciniak Przede wszystkim doceniają kompleksowość podejścia do polityki bezpieczeństwa. Ważna dla nich jest możliwość integracji różnych elementów w ramach koncepcji SDSN – firewalli, przełączników, routerów i sandboksów. Dla wielu z nich kluczowa jest możliwość monitorowania środowiska sieciowego. Natomiast warto podkreślić, że jeszcze przed rozpoczęciem czynności sprzedażowych trzeba poświęcić wiele czasu klientom, aby pokazać im korzyści płynące ze stosowania tego typu rozwiązań.

CRN Na jakiego typu wsparcie mogą liczyć współpracujący z Nuvias integratorzy?

Paweł Marciniak Muszą zacząć od samodzielnego zarejestrowania się w programie partnerskim prowadzonym przez Juniper Networks. Kolejnym etapem jest przejście przez ścieżkę edukacyjną i zdobycie odpowiednich certyfikatów. W tym zakresie jesteśmy pomocni my, jako dystrybutor – organizujemy webinaria oraz warsztaty techniczne, na których demonstrujemy zasady budowania bezpiecznego środowiska. Podczas realizacji pierwszych projektów partnerzy mogą liczyć na pełną pomoc naszego inżyniera w projektowaniu danego rozwiązania i jego budowie. Czasami robimy spotkania dla kilku partnerów, ma wówczas miejsce wymiana doświadczeń na temat problemów technicznych, z którymi spotkaliśmy się ostatnio u klientów.

Dodatkowe informacje: Paweł Marciniak, dyrektor polskiego oddziału Nuvias, pawel.marciniak@nuvias.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI JUNIPER NETWORKS I NUVIAS.

ABC Data
– bezpieczeństwo sieci bez tajemnic

W ofercie dystrybutora znajdują się rozwiązania ochronne dla firm dowolnej wielkości. Inżynierowie ABC Data pomagają partnerom w doborze właściwego sprzętu i oprogramowania oraz udzielają porad dotyczących argumentacji sprzedażowej, a także późniejszego wdrożenia wybranych rozwiązań.

Resellerzy z wartością dodaną i mniejsi integratorzy, którzy zaczynają swoją przygodę z rozwiązaniami ochronnymi, powinni zainteresować się systemami typu Unified Threat Management. Mogą one zostać zaimplementowane w firmowym środowisku IT jako fizyczne urządzenie lub maszyna wirtualna.

Kontrola zagrożeń

Podstawowymi funkcjami każdego UTM-a są moduły firewalla, bazującego na sygnaturach antywirusa oraz systemy wykrywania i zapobiegania włamaniom (IDS/IPS). Niektórzy producenci tych urządzeń zapewniają ponadto heurystyczną analizę danych przesyłanych w sieci oraz pobieranych z Internetu. Z reguły UTM-y są wyposażone także w moduł filtrowania treści i adresów URL. To bardzo ważna funkcja, która nie obciąża sprzętu, lecz zapewnia możliwość ograniczenia użytkownikom dostępu do określonych stron internetowych lub całych witryn – na przykład znajdujących się na serwerach hostujących złośliwe oprogramowanie. Ważne jest, że administrator zarządzający UTM-em zyskuje możliwość wdrożenia dodatkowych reguł polityki bezpieczeństwa, które są przyjęte w danej firmie. Może blokować określone strony internetowe lub całe ich grupy (według kategorii), albo tworzyć białe listy stron dozwolonych, blokując wszystkie pozostałe.

Na tym jednak funkcjonalność UTM-ów wcale się nie kończy. Wiele modeli umożliwia bowiem kontrolę aplikacji webowych lub znajdujących się fizycznie na komputerach użytkowników. Niektórzy producenci wzbogacają swoje rozwiązania o dodatkowych agentów ochrony, instalowanych bezpośrednio na stacjach roboczych lub serwerach w danej sieci. Zdecydowanie zwiększa to poziom bezpieczeństwa, ponieważ ochrona z wykorzystaniem UTM-a nie jest wówczas ograniczona wyłącznie do brzegu sieci. To na agentach spoczywa część zadań systemu UTM również wtedy, gdy użytkownik „wyjdzie" z jego zasięgu i na przykład podłączy swój komputer do niezabezpieczonej sieci publicznej.

Jako router lub sonda

Większość modeli UTM-ów może być wdrażanych na dwa sposoby. W najczęściej spotykanym, stosowanym głównie w mniejszych przedsiębiorstwach, rozwią-

UTM-y w ofercie ABC Data

- **Cisco Meraki MX** – rozwiązanie do kompleksowej ochrony sieci z wykorzystaniem modułów: firewall, antywirus, IPS (Snort), filtr treści, kontrola aplikacji, MDM. Umożliwia zarządzanie poprzez hostowaną centralną konsolę, co pozwala na wprowadzanie zmian konfiguracyjnych z dowolnego miejsca.
- **SonicWall TZ, NSA, SuperMassive** – szerokie portfolio produktów (również w wersji wirtualnej) do środowisk dowolnej wielkości. Zawierają takie moduły jak: firewall, IPS, antywirus, antyspam, filtr treści, kontrola aplikacji, ochrona agentowa.
- **ZyXEL USG** – urządzenia do ochrony sieci z wykorzystaniem modułów: firewall, IDP, antywirus, antyspam, filtr treści.

zanie pełni jednocześnie funkcję routera podłączonego do WAN-u oraz umożliwia stworzenie podstawowej sieci, bowiem wybrane modele mają wbudowany także punkt dostępowy Wi-Fi. Takie rozwiązania często stosowane są w oddziałach firm, gdzie nie jest wymagana duża segmentacja sieci, a konieczne jest jej zabezpieczenie przed atakami z zewnątrz i zapewnienie połączenia szyfrowanego (VPN) z centralą.

UTM może być wdrożony również w trybie inline. Wówczas w infrastrukturze sieciowej musi być zastosowany oddzielny router oraz wszystkie pozostałe urządzenia aktywne, przełączniki, kontrolery WLAN czy punkty dostępowe. W takiej sytuacji UTM jest podłączany pomiędzy modemem od operatora, a routerem i przełącznikiem sieciowym. Nie jest już jednostką budującą sieć, zaczyna natomiast pełnić rolę sondy zapewniającej prowadzenie analizy ruchu sieciowego pod kątem obecności złośliwego kodu, kontrolę aplikacji oraz filtrowanie stron internetowych.

Wychodząc naprzeciw potrzebom klientów, wielu producentów UTM-ów udostępniło ich wersje, które mogą być wdrożone jako wirtualne maszyny w środowisku VMware vSphere, Microsoft Hyper-V lub Citrix XenServer.

Bezpieczeństwo dla każdego

Rozwiązania UTM wybierane są bardzo często przez małe firmy. Traktowane są jako ochronne „kombajny", zapewniające funkcje typu AIO. Decyzja ta ma podłoże ekonomiczne, jednak nie tylko.

– *UTM-y oferują bardzo wiele funkcji, dzięki którym klienci nie muszą dokupować bram do serwerów poczty elektronicznej czy ruchu generowanego przez przeglądarki stron internetowych* – przekonuje Wojciech Kotkiewicz, menedżer działu wsparcia technicznego w ABC Data. – *Oczywiście oddzielne produkty mogłyby zapewnić bardziej skuteczną ochronę. Jednak istnieje obawa, że firmy, w których nie ma rozbudowanego działu IT, mogą nie zapanować nad ich konfiguracją i obsługą w momencie wykrycia zagrożenia. Dlatego podejmują decyzję o pewnym kompromisie i wybierają UTM jako rozwiązanie zapewniające wystarczający poziom ochrony.*

W większych firmach – bankach, instytucjach energetycznych, placówkach administracji publicznej – tam gdzie w działach IT istnieje podział odpowiedzialności, a często zatrudnieni są też specjaliści ds. bezpieczeństwa, zdecydowanie warto rozważyć wdrożenie rozwiązań takich jak firewalle nowej generacji czy osobne bramy pocztowe. Pozwalają one definiować reguły polityki bezpieczeństwa na bardzo szczegółowym poziomie. Co więcej, jeżeli taka firma ma oddziały, nie ma potrzeby stosowania także w nich zaawansowanych rozwiązań, wskazane jest jedynie, aby korzystać np. z UTM-ów tego samego producenta. Zagwarantowana zostanie wówczas kompatybilność między nimi, a administratorzy będą mogli zdalnie wprowadzać nowe reguły firmowej polityki bezpieczeństwa.

– *Nie można też zapominać o antywirusach instalowanych na stacjach roboczych i serwerach. Zapewniają ochronę przede wszystkim wtedy, gdy użytkownicy korzystają z Internetu poza siecią lokalną* – przypomina Wojciech Kotkiewicz.

>>> Trzy pytania do...

Damiana Przygodzkiego, inżyniera systemowego w ABC Data

CRN Jak duże znaczenie w procesie sprzedaży rozwiązań zapewniających bezpieczeństwo środowisk IT ma poziom wiedzy resellerów i integratorów?

Damian Przygodzki Każdy producent chce mieć partnerów, którzy są wyedukowani i mają doświadczenie we wdrażaniu jego produktów. To szczególnie ważne w przypadku rozwiązań ochronnych, ponieważ ich niepoprawna konfiguracja może przynieść więcej szkody niż pożytku. Dotyczy to także UTM-ów, o których przyjęło się mówić, że są znacznie łatwiejsze we wdrożeniu i obsłudze niż systemy NFGW czy IPS. Niemniej jednak ich konfiguracja zapewniająca wykorzystanie pełni możliwości urządzenia, także może przysporzyć problemów. Z tego powodu konieczne jest posiadanie odpowiednich kwalifikacji. Zachęcamy więc resellerów i integratorów do udziału w oficjalnych programach partnerskich organizowanych przez producentów. Dzięki nim mają szansę uczestniczenia w szkoleniach dla sprzedawców i inżynierów, często bezpłatnych, zakończonych egzaminem. Zdobyty certyfikat stanowi potwierdzenie dla klientów, że mają do czynienia z wiarygodnym kontrahentem, który jest w stanie zapewnić opiekę na wysokim poziomie.

CRN Co powinni zrobić partnerzy, którzy z jakiegoś powodu nie chcą lub nie mogą uzyskać certyfikacji?

Damian Przygodzki Jeśli mają dobrą, wieloletnią relację z klientem, obsługują go całościowo i chcą utrzymać taki stan rzeczy, powinni poszukać integratora, który specjalizuje się w rozwiązaniach ochronnych. Może w ich imieniu dokonać wdrożenia, przeszkolić pracowników i ewentualnie inżynierów partnera, który jest głównym właścicielem kontraktu. Kwestia serwisu pozostaje do uzgodnienia między firmami, ale – szczególnie w przypadku bardziej skomplikowanych systemów – powinno zajmować się nim przedsiębiorstwo dokonujące wdrożenia. Warto uregulować to odpowiednią umową trójstronną. Czasami może pomóc też dystrybutor.

CRN W jaki sposób?

Damian Przygodzki Jeżeli mniej doświadczony partner ma problemy ze znalezieniem podwykonawcy, możemy sami go poszukać. Jako inżynierowie technicznego wsparcia sprzedaży jesteśmy w stanie pomóc w zaprezentowaniu oferty klientowi, udzieleniu odpowiedzi na trudne pytania, m.in. dotyczące rozwiązań konkurencyjnych. Oczywiście pomagamy również w samym wdrożeniu, szkoląc jednocześnie na tym przykładzie resellera.

Dodatkowe informacje:
ABC Data Value+, ul. Daniszewska 14,
03-230 Warszawa, tel. (22) 676-09-00,
ABCData-ValuePlus@abcdata.eu

Bezpieczna sieć LAN dzięki rozwiązaniu SDN z **Allied Telesis**

Secure Enterprise Software Defined Networking (SES) – najnowsze w ofercie Allied Telesis rozwiązanie do zarządzania sieciami – służy do zapewniania bezpieczeństwa a także obniża koszty ich użytkowania. Błyskawicznie reaguje na alarmy i blokuje ruch będący skutkiem ataku w dowolnym miejscu sieci przewodowej lub bezprzewodowej.

Większość firm do ochrony sieci przed atakami wykorzystuje system wykrywania włamań (IDS) lub zapobiegania im (IPS). Jednak IPS może spowodować opóźnienia i stworzyć wąskie gardła, a większość rozwiązań IDS ostrzega, gdy wykryto zagrożenie, ale nie ma funkcji automatycznego blokowania niepożądanego ruchu. Zanim administrator zareaguje na ostrzeżenie, może być już za późno.

Blokada już u źródła

Większość IPS-ów wykrywa i blokuje podejrzany ruch pochodzący z Internetu, a więc spoza firmy. Tymczasem rozwiązanie SES Allied Telesis analizuje ruch i izoluje podejrzane urządzenia w dowolnym miejscu w sieci, dzięki czemu zapobiega zagrożeniom nie tylko na styku sieci, ale także wewnątrz niej (np. wykrywa ryzyko ataku z wykorzystaniem przyniesionego przez pracowników na urządzeniach mobilnych lub pendrive'ach złośliwego oprogramowania). Dzięki temu SES może monitorować ruch przychodzący i wewnętrzny w lokalnej sieci bez powodowania opóźnień i tworzenia wąskich gardeł. W ten sposób wszystkie urządzenia przenośne podłączane do firmowej sieci zaczynają podlegać tym samym regułom korporacyjnej polityki bezpieczeństwa.

Jest to pierwsze komercyjne rozwiązanie SDN dla sieci bezprzewodowych, o tak szerokim spektrum zastosowań. Punkty dostępowe Allied Telesis są zgodne z protokołem OpenFlow i mogą być zarządzane przez kontroler SES. Nowe reguły polityki bezpieczeństwa i aktualizacje łatwo zaimplementować, a z centralnego kontrolera do wszystkich punktów dostępowych dostarczane są w kilka sekund, co radykalnie skraca czas poświęcony na zarządzanie siecią i jej ochroną.

Secure EnterpriseSDN

Rozwiązania Allied Telesis z rodziny SES wykorzystują aplikacje IDS do identyfikowania zagrożeń i natychmiast reagują, aby odizolować dotkniętą atakiem część sieci. Mogą wówczas zainicjować automatyczną kwarantannę podejrzanego urządzenia i rozpocząć proces remediacji, aby ponownie połączyło się z siecią – bez interwencji administratora. Zasady reagowania można konfigurować w celu dostosowania ich do potrzeb firmy, a wszystkie podjęte działania są rejestrowane, co ułatwia przeprowadzenie audytu.

Otwarte i elastyczne rozwiązanie SDN

Kontroler SES może pracować w sieciach zawierających przełączniki kompatybilne z protokołem OpenFlow, jest też zgodny z szeregiem fizycznych i wirtualnych firewalli oraz innych systemów ochronnych. Nie ma potrzeby wymiany sieciowych urządzeń aktywnych, aby skorzystać z zalet tego rozwiązania, bo współpracuje z większością sprzętu wykorzystywanego w firmowych sieciach.

SES integruje się również z narzędziem Allied Telesis Autonomous Management Framework (AMF) do automatyzacji zarządzania siecią. Wówczas nie korzysta już z protokołu OpenFlow do komunikacji z urządzeniami sieciowymi, zamiast tego może używać AMF do dostarczania im poleceń. Zapewnia to wszystkie zalety rozwiązania SDN bez potrzeby korzystania z OpenFlow. Zmniejsza to ryzyko i koszty wdrożenia rozwiązań SDN, ponieważ istniejąca sieć w przedsiębiorstwie może pozostać niezmieniona.

Tomasz Odzioba
Country Manager Poland, Latvia, Lithuania & Ukraine, Allied Telesis

Wiele dostępnych na rynku rozwiązań w bardzo niejasny sposób informuje o zagrożeniu danych w infrastrukturze sieciowej. Tymczasem SES firmy Allied Telesis zapewnia monitoring sieci w każdym jej miejscu – na brzegu oraz w samym środku, uniemożliwiając np. przyniesienie do firmy złośliwego oprogramowania przez użytkowników. Rozwiązanie to można wspierać innymi produktami ochronnymi Allied Telesis, np. UTM-ami i firewallami nowej generacji.

Allied Telesis

Dodatkowe informacje:
Tomasz Odzioba, Country Manager Poland, Latvia, Lithuania & Ukraine, Allied Telesis,
tomasz_odzioba@alliedtelesis.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ ALLIED TELESIS.

Zabawa w chowanego – nie z firewallami Forcepoint

Urządzenia ochronne firmy Forcepoint umożliwiają zabezpieczenie infrastruktury sieciowej przed starannie kamuflowanymi przez cyberprzestępców atakami.

Protokoły sieciowe wykorzystywane do transmisji danych przez Internet w założeniach mają być odporne na różnego typu ataki. Ich architektura jest jednak bardzo skomplikowana, co powoduje, że w różnych rozwiązaniach IT są implementowane na różne sposoby. To otwiera drogę cyberprzestępcom. Poszukują drobnych luk, najczęściej w rzadko używanych obszarach protokołów, i starają się wykorzystać je w niestandardowy sposób, aby zwiększyć trudność wykrycia ich działań przez systemy ochronne. Ponadto przesyłany w czasie takiego ataku kod jest obudowywany dodatkowo wytwarzanym, niegroźnym, ale nietypowym ruchem sieciowym, który powoduje „dezorientację" rozwiązań zabezpieczających, a w efekcie często ich zgodę na transfer szkodliwych danych. Tego typu zaawansowane techniki kamuflowania ataków (Advanced Evasion Techniques) nazywane są także technikami unikowymi lub ewazyjnymi.

Metoda ta jest bardzo skuteczna – złośliwy kod dostarczany jest głównie przez niezałatane luki w zabezpieczeniach i z wykorzystaniem błędów dnia zerowego. Atakujący bazują nie tylko na anomaliach w protokołach sieciowych, ale także błędach w ich implementacji, np. w powszechnie używanych aplikacjach internetowych. Ponieważ ataki mogą być kamuflowane w wielu różnych warstwach stosu protokołu TCP/IP, analiza przesyłanych danych powinna odbywać się w każdej z nich.

Gdy organizacja badawcza NSS Labs wprowadziła techniki unikowe do swoich testów, okazało się, że większość oferowanych na rynku firewalli nowej generacji jest zupełnie bezradna. Pionierem w walce z tego typu zagrożeniami były rozwiązania kupionej przez Forcepoint fińskiej firmy Stonesoft.

Fizycznie i wirtualnie

Firewalle nowej generacji z oferty Forcepoint zapewniają bardzo skuteczną ochronę danych bez negatywnego wpływu na wydajność sieci. Mają wiele bardzo ciekawych funkcji, których nie ma w rozwiązaniach innych dostawców albo są, ale słabo rozwinięte (np. zaawansowane klastrowanie, multilink, SD-WAN).Producent w swoich firewallach w unikalny sposób połączył mechanizmy kontroli dostępu do infrastruktury sieciowej oraz głębokiej inspekcji przesyłanych danych w celu zapewnienia wysokiego poziomu ich bezpieczeństwa. Służą do tego: szczegółowa kontrola aplikacji, system ochrony przed włamaniami (IPS), wbudowany moduł wirtualnej sieci prywatnej (VPN) oraz aplikacyjne serwery proxy. Dzięki temu możliwe jest analizowanie i rozszyfrowywanie ruchu sieciowego, kiedy podejrzewa się, że został zmodyfikowany w celu ukrycia w nim złośliwego kodu służącego do przeprowadzenia ataku.

Firewalle Forcepoint są oferowane w różnej postaci: sprzętowej (wiele konfiguracji – począwszy od małych urządzeń dla oddziałów firm po duże rozwiązania dla centrów danych), oprogramowania do wdrażania w infrastrukturze chmurowej (Amazon Web Services i Microsoft Azure), a także wirtualnych appliance'ów (dla hypervisorów VMware ESXi, VMware NSX, Microsoft Hyper-V oraz KVM). Zarządzanie nimi wymaga systemu Security Management Center w postaci oprogramowania bądź urządzenia.

Forcepoint – marka z tradycjami

Właścicielem Forcepoint jest firma Raytheon, dostawca rozwiązań militarnych dla amerykańskiego wojska, a także m.in. rakiet Patriot dla polskiej armii. Marka Forcepoint powstała w wyniku połączenia przedsiębiorstw: Websense, Skyfence, Sidewinder, Stonesoft oraz Red Owl.

W testach przeprowadzonych przez organizację NSS Labs wśród 10 dostawców rozwiązań ochronnych systemy NGFW i IPS firmy Forcepoint otrzymały najwyższą ocenę w zakresie skuteczności zabezpieczeń.

Dodatkowe informacje: Maciej Pawelczyk, Security Project Manager, Ingram Micro, maciej.pawelczyk@ingrammicro.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI FORCEPOINT I INGRAM MICRO.

Sieć pod kontrolą z Extreme Networks

Zapewnienie bezpieczeństwa w nowoczesnej sieci wiąże się z koniecznością prowadzenia nieustannej kontroli dostępu do infrastruktury i znajdujących się w niej zasobów. Rozwiązania wyposażone w te funkcje stanowią jeden z filarów oferty Extreme Networks.

Kluczowym elementem wpływającym na ogólny stan zabezpieczeń każdej firmy i ułatwiającym wyeliminowanie zagrożeń występujących dziś w środowiskach IT jest Network Access Control. Wiele oferowanych na rynku rozwiązań NAC zapewnia tylko prostą kontrolę dostępu prowadzoną wyłącznie w momencie podłączania urządzenia do sieci, z ograniczonymi elementami oceny stanu jego zabezpieczeń, która jest niewystarczająca w obecnych czasach. Tego typu system powinien prowadzić dynamiczną i nieprzerwaną analizę, zapewniać tworzenie szczegółowych reguł polityki bezpieczeństwa i ich stałe egzekwowanie.

Proponowane przez Extreme Networks rozwiązanie ExtremeControl zostało zaprojektowane tak, aby sprostać tym wyzwaniom i zapewnić ciągłą kontrolę użytkowników i urządzeń podłączonych do sieci. Prowadzi się ją na podstawie takich informacji jak uwierzytelniona tożsamość użytkownika lub urządzenia, jego lokalizacja, strefa czasowa oraz aktualny lub przeszły stan zabezpieczeń. Z uwzględnieniem tych wszystkich kryteriów w momencie podłączania sprzętu do sieci przyznawane są przywileje dostępu, natomiast urządzenia niespełniające warunków poddaje się kwarantannie w celu poprawy stanu zabezpieczeń. Następnie ExtremeControl stale monitoruje działania użytkowników, by mieć pewność, że zachowują się normalnie, zgodnie z przyjętymi zasadami użytkowania systemów i aplikacji, określonymi przez firmową politykę bezpieczeństwa.

Rozwiązanie ExtremeControl może pracować w infrastrukturze sieciowej zbudowanej z urządzeń różnych producentów. Jest proste we wdrożeniu, intuicyjne w zarządzaniu, gwarantuje skalowalność i skutecznie eliminuje zagrożenia. Jest zaprojektowane przy użyciu otwartej architektury w celu uzyskania interoperacyjności z różnorodnymi środowiskami IT.

Centralne zarządzanie rozwiązaniem ExtremeControl umożliwia pakiet oprogramowania Extreme Management Center, dzięki któremu użytkownicy zawsze mają dostęp do odpowiednich zasobów sieci, a najważniejsze dla funkcjonowania przedsiębiorstwa systemy i procesy biznesowe są chronione przed nadużyciami.

Kontrola w każdej sieci

Do zarządzania złożonymi środowiskami sieciowymi, w których występują urządzenia IoT i BYOD, konieczne jest zagwarantowanie ochrony przed atakami typu ransomware i innymi cyberzagrożeniami. W tym zakresie Extreme Network proponuje klientom należącą do rodziny Extreme Management Center aplikację ExtremeControl, która umożliwia szczegółowy wgląd w informacje o podłączających się do sieci urządzeniach i ich użytkownikach, aplikacjach, z których korzystają, a także pełną kontrolę ich działań. Zarządzanie nimi odbywa się za pomocą jednego, intuicyjnego w obsłudze panelu sterowania, a zakres kontroli obejmuje całą sieć – od brzegu po rdzeń.

Konrad Grzybowski
inżynier systemów bezpieczeństwa, Versim

Implementacja technologii NAC lub innego rozwiązania dotyczącego bezpieczeństwa wymusza wprowadzanie zmian w procesach biznesowych i powinna być realizowana tak, aby minimalnie wpłynąć na funkcjonowanie przedsiębiorstwa. Dlatego rozwiązanie Extreme NAC może być wdrażane w kilku etapach. Pierwszym krokiem jest zaimplementowanie usług uwierzytelniania urządzeń i użytkowników oraz scentralizowanego systemu zarządzania tym procesem, audytowania oraz raportowania. Później można dodać funkcję oceniania stanu zabezpieczeń systemów końcowych i ich zgodności z polityką bezpieczeństwa oraz badania na bieżąco poziomu ochrony już po połączeniu z siecią. System można też wzbogacić o automatyczne zarządzanie eliminacją zagrożeń, w tym izolowanie, poddawanie kwarantannie oraz doprowadzanie urządzeń końcowych niespełniających reguł polityki bezpieczeństwa do stanu zgodności.

ExtremeControl zapewnia centralne definiowanie szczegółowych reguł polityki bezpieczeństwa (do których muszą dostosować się użytkownicy i urządzenia), dzięki czemu możliwe staje się spełnienie wymagań dotyczących zgodności z różnego rodzaju regulacjami.

– *Rozwiązanie to dostosowuje się do potrzeb biznesowych klientów* – mówi Konrad Grzybowski, inżynier systemów bezpieczeństwa w firmie Versim, która jest dystrybutorem Extreme Networks. – *Dzięki temu partnerzy mogą rozpocząć z nimi współpracę od wdrożenia małego rozwiązania, które z czasem rośnie. ExtremeControl da się zintegrować z wieloma innymi stosowanymi w korporacjach rozwiązaniami IT zapewniającymi bezpieczeństwo, zarządzanie urządzeniami mobilnymi, analitykę oraz z usługami w chmurze. Integratorzy mogą skorzystać także z otwartego interfejsu API do integracji rozwiązania z własnymi aplikacjami.*

Oprogramowanie ExtremeControl przypisuje poszczególnym urządzeniom końcowym takie atrybuty jak: nazwa użytkownika, typ dostępu, czas podłączenia, lokalizacja oraz wykrytą podatność na ataki. W ten sposób tworzy pełną, bazującą na rolach, kontekstową tożsamość danego elementu infrastruktury, która jest związana z użytkownikiem, niezależnie od tego, z jakiego miejsca i w jaki sposób łączy się z siecią.

Możliwość ustanowienia szczegółowych reguł polityki bezpieczeństwa i wymuszenia ich obowiązywania w całej sieci gwarantuje łatwe uzyskanie zgodności z wewnętrznymi i zewnętrznymi regulacjami. Za pomocą jednego kliknięcia można wymóc, by dane urządzenie spełniało kontekstowe reguły dotyczące jakości transmisji (QoS), pasma i wartości innych parametrów. Szczegółowe raporty zawierające informacje o wszystkich udanych i nieudanych próbach uwierzytelniania użytkowników oraz aktualizowana na bieżąco tabela stanu podłączonych do sieci urządzeń i ich użytkowników pozwalają niezwłocznie powiadamiać administratora o przewidywanych problemach.

W obliczu nieustannie zmieniających się ustawień sieci można stosować tzw. mikrosegmentację w celu uzyskania spójności zabezpieczeń, bez wprowadzania złożonych zmian w konfiguracji urządzeń sieciowych. Podczas realizacji dużych projektów infrastruktury sieciowej można ograniczyć ryzyko błędu dzięki korzystaniu ze środowiska testowego ułatwiającego weryfikację spójności nowych reguł polityki bezpieczeństwa.

Extreme i Palo Alto – para doskonała

Firmy Extreme Networks i Palo Alto Networks wiele lat temu nawiązały strategiczne partnerstwo. Dzięki niemu zapewniono integrację rozwiązania Extreme Management Center (wcześniej oferowanego pod marką NetSight) z firewallami nowej generacji Palo Alto. Dostarczają one informacji o naruszeniu reguł polityki bezpieczeństwa w sieci i wysyłają adres IP oraz MAC podejrzanego urządzenia, a NAC blokuje lub ogranicza dostęp użytkownika do sieci, zapewniając bezpieczeństwo pozostałym (nawet jeśli ich urządzenia są podłączone do tego samego portu). Użytkownik nie ma dostępu do zasobów IT do chwili, gdy administratorzy mu go umożliwią, bo otrzymali stosowne powiadomienie w portalu administratorskim, przez e-mail lub SMS.

Bezpieczny dostęp gości do sieci i usługi BYOD

W nowoczesnych sieciach podłączanie nowych urządzeń w modelu BYOD oraz zapewnianie dostępu gościom jest bardzo łatwe i bezpieczne dzięki samoobsługowym portalom (captive portal). Powinny one gwarantować uwierzytelnianie za pomocą wiadomości SMS lub za pośrednictwem portali społecznościowych, ewentualnie w modelu sponsoringu (w którym pracownik firmy wnioskuje o dostęp do sieci dla gościa i w pewien sposób bierze odpowiedzialność za jego poczynania). Nowe urządzenia są automatycznie podłączane do sieci, profilowane, a także określany jest poziom ich ochrony zgodny z obowiązującą w przedsiębiorstwie polityką bezpieczeństwa.

ExtremeControl dba o to, aby – dzięki znajomości tożsamości użytkowników – możliwe było stosowanie automatycznego rejestrowania gości bez udziału pracowników działu IT. Oprogramowanie nadzoruje ważność konta oraz czas korzystania z niego. Integratorzy mogą też dostosować do potrzeb klienta stworzoną z wykorzystaniem ExtremeControl usługę portalu dla gości, np. opatrując go marką danej firmy. Aby chronić sieć przed dostępem nieautoryzowanych urządzeń, umożliwiona została integracja z rozwiązaniami klasy EMM/MDM partnerów firmy Extreme Networks, takimi jak VMware AirWatch, Citrix i MobileIron.

W rozwiązaniu ExtremeControl wykorzystywane są dwie metody oceniania urządzeń końcowych – agentowa i bezagentowa. Agent stały lub tymczasowy może być zainstalowany w urządzeniu użytkownika lub pobrany z portalu dla gości. Instalacja agentów może być również wymuszona przez system do masowej dystrybucji oprogramowania, taki jak Group Policy lub System Center Configuration Manager. Natomiast metoda oceniania bezagentowego nie wiąże się z koniecznością instalacji jakiegokolwiek oprogramowania, wykorzystywane są inne sposoby weryfikacji stosowanych zabezpieczeń.

Extreme networks VERSIM Dystrybutor IT

Dodatkowe informacje: Dawid Królica, Area Sales Manager, Extreme Networks, dkrolica@extremenetworks.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI EXTREME NETWORKS I VERSIM.

Zaawansowana ochrona przed zagrożeniami z Juniper Networks

Korzystanie z infrastruktury publicznych środowisk chmurowych jest obecnie jednym z głównych trendów informatycznych na świecie. Ale, mimo rosnącej akceptacji dla tego typu rozwiązań, wciąż wiele firm obawia się o bezpieczeństwo informacji przechowywanych i przetwarzanych w ten sposób. Przedsiębiorcy boją się też konsekwencji nowych regulacji prawnych związanych z ochroną danych osobowych.

Coraz częściej producenci systemów zabezpieczających przenoszą je do chmury – oferują klientom jedynie korzystanie ze specjalnie przygotowanych narzędzi. Wśród usług dostępnych w chmurze publicznej można znaleźć rozwiązania do analizy plików (sandbox, Advanced Threat Prevention), zarządzania systemami ochronnymi, a nawet wirtualne repozytoria logów, których klienci mogą używać do tworzenia statystyk i raportów na temat stanu zabezpieczeń swoich sieci.

Mimo że taki sposób działania może wydawać się atrakcyjny, wygodny i coraz tańszy, to jednak wzbudza zrozumiałe wątpliwości użytkowników i ekspertów ds. bezpieczeństwa. W wielu sytuacjach wymagania dotyczące poufności danych oraz przyjęta polityka ochrony zasobów IT nie pozwalają, aby wrażliwe informacje były przetwarzane poza lokalnym środowiskiem sieciowym.

Na początku 2018 r. Juniper Networks wprowadził na rynek produkt o nazwie Juniper Advanced Threat Prevention. Jego opracowanie było możliwe dzięki przejęciu utworzonej w 2011 r. firmy Cyphort – jednego z liderów rynku systemów klasy Advanced Threat Prevention. Jest to rozwiązanie instalowane lokalnie, a dzięki temu może być atrakcyjne dla tych podmiotów, które oczekują szczegółowej kontroli przepływu informacji w firmie. JATP zawiera zaawansowany system klasy sandbox z możliwością agregacji logów pochodzących z systemów innych producentów oraz funkcją synchronizacji reguł polityki bezpieczeństwa na firewallach nowej generacji Juniper Networks i niektórych produktach konkurencyjnych. Rozwiązanie to jest dostępne w ofercie Clico – autoryzowanego dystrybutora Juniper Networks.

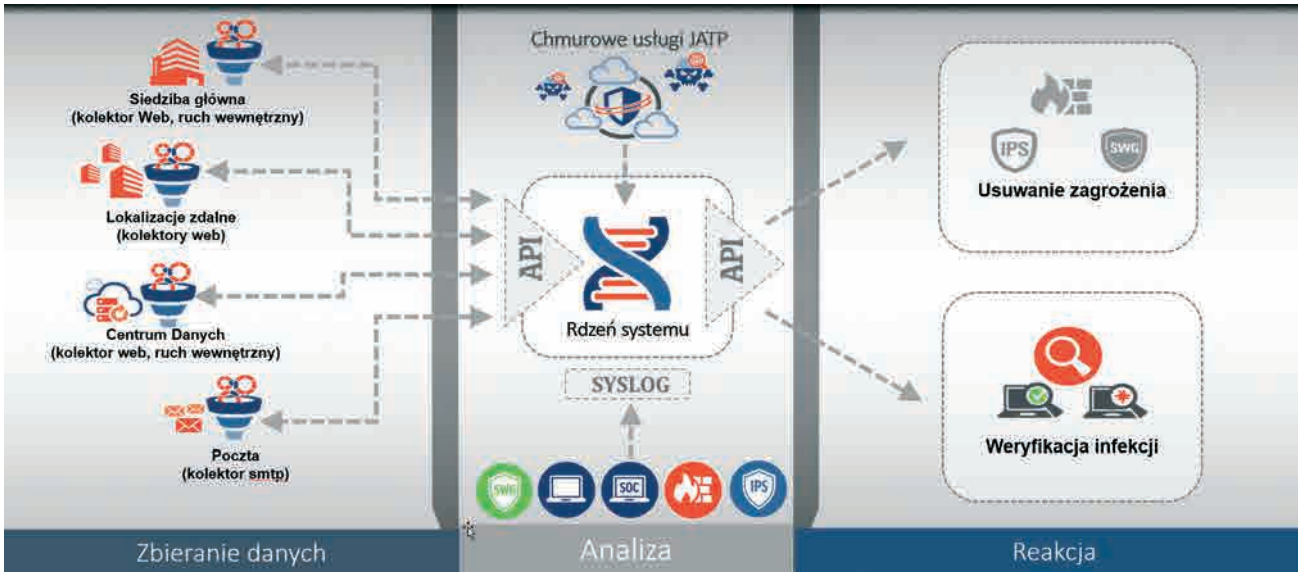
Nie tylko SIEM

Coraz bardziej złożone ataki, często skierowane na konkretne przedsiębiorstwa, duże zyski ze sprzedaży skradzionych danych lub z wyłudzeń – to główne powody, dla których nie ma dzisiaj sieci komputerowej, której administrator mógłby z czystym sumieniem ogłosić, że nigdy nie była i nie zostanie ofiarą włamania. Dlatego, poza skutecznym blokowaniem znanych ataków, równie ważne jest monitorowanie infrastruktury sieciowej za pomocą analizy logów oraz przechwytywanie ruchu sieciowego w celu wykrycia niepokojących zjawisk.

JATP może stanowić uzupełnienie, ale również – w określonych warunkach – alternatywę systemów SIEM (Security Information and Event Management) oraz NBAD (Network Behavior Anomaly Detection), które pracują w złożonym środowisku i wymagają ciągłego dostrajania i rekonfiguracji. SIEM zapewnia ogromne możliwości stworzenia niemal dowolnych reguł korelacyjnych, jednak w kontekście analizy powłamaniowej oczekiwania są nieco inne.

Dynamicznie zmieniająca się konstrukcja ataków wymaga, aby proces analizy, kategoryzacji oraz korelacji zdarzeń był zautomatyzowany i maksymalnie upraszczał eliminację skutków incydentów. JATP to zintegrowany system zawierający wiele znanych mechanizmów ochronnych, który współpracuje z rozwiązaniami innych producentów, jest elastyczny oraz skalowalny. Do głównych korzyści z jego zastosowania można zaliczyć przyspieszenie analizy informacji gromadzonych przez różne systemy ochronne oraz zdolność podjęcia zautomatyzowanej akcji prewencyjnej zapobiegającej rozprzestrzenianiu się ataku.

JATP jest dostarczany zarówno w formie wirtualnej, jak i w postaci fizycznych urządzeń. Umożliwia dywersyfikację funkcji poszczególnych kolektorów danych, co zapewnia elastyczność wdrożenia oraz łatwość rozbudowy. Podstawowym elementem systemu jest moduł Core, który służy do analizy ruchu sieciowego oraz wiadomości pocztowych, analizy dynamicznej, realizacji uczenia



maszynowego oraz korelowania logów zbieranych za pomocą protokołu syslog z zewnętrznych źródeł. Możliwe jest wdrożenie wielu typów kolektorów danych, z których każdy przekierowuje innego rodzaju ruch do centralnego modułu analitycznego.

Kolektor Web dokonuje analizy ruchu i wyodrębnienia plików transmitowanych za pomocą protokołu HTTP. Z kolei kolektor email zbiera przesyłane pocztą pliki oraz „przygląda się" podlinkowanym w e-mailu stronom internetowym, dzięki czemu stanowi efektywne narzędzie do wykrywania prób phishingu. Kolektorem może być także zapora sieciowa SRX (firewall nowej generacji marki Juniper Networks), która przekazuje do JATP pliki transmitowane przez protokoły HTTP, SMTP i IMAP (również zaszyfrowane z wykorzystaniem protokołu SSL). Dzięki działaniu SRX w trybie SSL Proxy pliki są odszyfrowywane i udostępniane modułowi analitycznemu.

Automatyczna analiza

Zagrożenia są wykrywane w trzech głównych obszarach (w ruchu HTTP, w ruchu pocztowym oraz w ruchu wewnątrz sieci), co zapewnia prześledzenie rozprzestrzeniania się złośliwego kodu (Lateran movement) za pomocą protokołu SMB. Podstawowym elementem JATP jest lokalny sandbox, umożliwiający weryfikację wielu rodzajów plików z wykorzystaniem takich metod jak analiza statyczna, reputacja, geolokalizacja, poszukiwanie adresów znanych centrów Command & Control czy wreszcie analiza dynamiczna na platformach Windows, Linux i macOS. Ponadto system śledzi wszystkie odwiedzane oraz przesyłane za pomocą poczty odnośniki do innych witryn, wykrywając w ten sposób próby namówienia użytkowników na uruchomienie strony, która nie ma statusu zaufanej.

Sama analiza pliku nie zawsze pozwala na określenie tzw. pacjenta zero w środowisku i, przede wszystkim, najczęściej nie wskazuje oryginalnego wektora ataku zastosowanego w celu wtargnięcia do sieci. W związku z tym dzięki silnikowi uczenia maszynowego system JATP analizuje dodatkowo inne zdarzenia (wykryte za pomocą metod własnych i logów dostarczonych do systemu przez zewnętrzne źródła) oraz koreluje informacje o nich pod kątem czasu wystąpienia oraz stadium ataku, zgodnie z metodologią Cyber Kill Chain.

Atutem rozwiązania jest fakt, że logi analizowane przez JATP mogą pochodzić z produktów innych firm (firewall, proxy, endpoint security itp.). Jest to zatem system, który nie tylko nie wymaga wymiany całej struktury ochronnej przedsiębiorstwa, ale stanowi jej istotne wzmocnienie. Poza analizą powłamaniową, wykonywaną w sposób ciągły, zapewnia też automatyzację procesu remediacji zaatakowanych rozwiązań, czyli przywrócenia ich do pracy w środowisku produkcyjnym po wyeliminowaniu zagrożenia. Do tego celu mogą być wykorzystane zarówno rozwiązania z portfolio firmy Juniper Networks, jak również wybrane produkty innych dostawców.

JATP to rozwiązanie kompleksowe, które charakteryzuje się potwierdzoną skutecznością, w pełni lokalnym działaniem oraz unikalnym połączeniem funkcji sandboksa ze zorientowanym na każde stadium ataku mechanizmem korelacji zdarzeń. W testach ICSA Labs w 2017 r. (jeszcze pod szyldem Cyphort) wykazano 100 proc. skuteczności JATP (w ramach przyjętej metodologii) w wykrywaniu zaawansowanych zagrożeń. Był to jedyny system z tak dobrym rezultatem wśród testowanych rozwiązań tej klasy. Dodatkowo współpraca z rozwiązaniami innych producentów, proste licencjonowanie oraz elastyczny mechanizm rozbudowy środowiska sprawiają, że JATP może być elementem istotnie podnoszącym poziom bezpieczeństwa każdej sieci.

Dodatkowe informacje: **Sławomir Karaś**, Senior System Engineer, Central Europe, Juniper Networks, skaras@juniper.net
Jarosław Bukała, Security Consultant, Clico, jaroslaw.bukala@clico.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI JUNIPER NETWORKS I CLICO.

Ilustracja AdobeStock

Kreatywność przestępców nie zna granic

Żyjemy pod ciągłym ostrzałem ze strony cyberprzestępców, chociaż nie zdajemy sobie z tego sprawy. Praktycznie każdego dnia wszystkie podłączone do Internetu urządzenia są sprawdzane przez automaty poszukujące luk w ich ochronie.

Krzysztof Jakubik

Cyberprzestępcy zarabiają na swym procederze wielkie pieniądze. Od kilku lat większe niż przynosi handel narkotykami. Nic dziwnego zatem, że z zaciekłością próbują ominąć wszystkie przygotowane przez „dobrą stronę mocy" zabezpieczenia. Celem przestępców jest monetyzacja każdego elementu ich działania. Pozyskują więc fundusze z bezpośrednich kradzieży (na przykład z kart kredytowych, rachunków bankowych), odsprzedaży wrażliwych danych, szantaży (ransomware lub groźba ujawnienia „niewygodnych" informacji), kradzieży energii elektrycznej potrzebnej na wydobycie kryptowalut. Zatem skoro mamy wojnę, trzeba przygotować się do walki.

– *Tworząc strategię ochrony przed atakami, najpierw trzeba odpowiedzieć sobie na pytanie, co w rzeczywistości powinno zostać zabezpieczone i w jaki sposób ująć te cele w polityce bezpieczeństwa* – mówi Andrzej Bugowski, IBM Business Unit Manager w Tech Dacie. – *Do najważniejszych obszarów, których ochrona jest konieczna, należą: infrastruktura IT, identyfikacja użytkowników oraz ich autoryzacja. Trzeba się upewnić, że używane w przedsiębiorstwie aplikacje zostały opracowane z uwzględnieniem najwyższych standardów ochrony. Trzeba także zbierać maksymalnie dużo informacji o funkcjonowaniu zabezpieczanego środowiska, starać się jak najwcześniej identyfikować zagrożenia i przygotować na potencjalne incydenty.*

Cryptojacking – kradzież mocy

Wśród „świeżych" pomysłów na prowadzenie cyberataków zdecydowanie wyróżnia się cryptojacking, czyli wykorzystywanie mocy obliczeniowej urządzenia ofiary do kopania kryptowalut. Oczywiście wartość „cyfrowego złota" przejętego przez cyberprzestępców z pojedynczego komputera jest relatywnie niewielka, niższa niż koszt energii elektrycznej, który poniesie ofiara. Jednak przestępcy postępują w myśl zasady, że ziarnko do ziarnka, a zbierze się miarka. Do tego typu działalności zachęcił ich wykładniczy wzrost wartości w 2017 r. takich kryptowalut jak bitcoin, monero czy ethereum.

Stosujący cryptojacking oszuści atakują laptopy, komputery stacjonarne, serwery, a nawet urządzenia mobilne. Kod kopiący kryptowaluty i przesyłający je do cyberprzestępców może być wprowadzony do urządzeń na kilka sposobów. Jednym z popularniejszych jest umieszczenie owego kodu w skrypcie JavaScript i osadzenie na stronie internetowej (przez włamanie się do hostującego ją serwera lub w skrypcie firm trzecich wyświetlających reklamy).

Proces kopania kryptowaluty przez stronę internetową ma jednak podstawową wadę – jest przerywany w momencie zamknięcia przeglądarki lub karty wyświetlającej zainfekowaną witrynę. Poza tym działalność tak umiejscowionego złośliwego kodu kopiącego kryptowaluty łatwo wykryć, wykorzystuje bowiem do maksimum moc procesora. Bazując na tej obserwacji, twórcy przeglądarek internetowych wprowadzili zabezpieczenia, które blokują zbyt zasobożerne procesy. Odpowiedzią cyberprzestępców było wprowadzenie ograniczeń w kodzie, dzięki którym wykorzystuje tylko część mocy obliczeniowej i działa praktycznie niezauważenie. Okazało się także, że istnieją kopiące skrypty dla systemu Android, które rozpoczynają pracę tylko po podłączeniu telefonu lub tabletu do zasilania, co ma uchronić baterię przed szybkim rozładowaniem i uśpić czujność użytkowników.

Oprócz tego, że cyberprzestępcy tworzą skrypty osadzane na stronach internetowych, starają się zarażać urządzenia ofiar klasycznymi metodami dystrybucji malware'u. Z punktu widzenia atakującego zaletą tradycyjnego modelu, ale jednocześnie jego wadą, jest to, że złośliwa aplikacja musi być uruchomiona przez cały czas, tylko wtedy przestępca będzie miał zyski. Znika więc ryzyko ręcznego wyłączenia jej przez użytkownika (tak jak w przypadku przeglądarki internetowej), ale obecność uruchomionego przez cały czas procesu wykorzystującego znaczną część mocy obliczeniowej procesora (nawet po wprowadzeniu ograniczeń) wzbudzi czujność modułu heurystycznego w oprogramowaniu antywirusowym.

Stosujący tę metodę dystrybucji kodu cyberprzestępcy są bardzo skuteczni, przebiegli i bezczelni. Gdy kod napotka „konkurencyjne" oprogramowanie kopiące cyberwaluty, natychmiast zabija ów proces. Hakerzy sprawdzają też, jaki system operacyjny (Windows, macOS, Linux) i w jakiej architekturze (32 lub 64 bity) jest uruchomiony na komputerze ofiary, aby dostarczyć najbardziej efektywny kopiący mechanizm. Zdarza się również, że instalują trojana zdalnego dostępu (RAT), dzięki któremu nie tylko działają w ukryciu na urządzeniu użytkownika, ale także mają nad nim pełną kontrolę (mogą usuwać i modyfikować pliki, przesyłać i pobierać je oraz instalować inne złośliwe oprogramowanie).

Cryptojacking coraz częściej jest wykrywany na urządzeniach mobilnych z systemem Android. Do uruchomienia kopiącego kodu najczęściej dochodzi w wyniku zainstalowania aplikacji z nieoficjalnego źródła. Nowe wersje Androida są jednak wyposażone w wiele mechanizmów wykrywających ›

Na czym polega Cyber Kill Chain?

Cyber Kill Chain to lista faz cyberataku. Została opracowana przez amerykański koncern zbrojeniowy Lockheed Martin. Jest świetnym narzędziem do opisywania sposobu ataku cyberprzestępców na firmę.

1. **Rozpoznanie.** Na długo przed rozpoczęciem ataku przestępcy przeprowadzają rozpoznanie środowiska, aby znaleźć jego słabe punkty. Zbierają dane pracowników, adresy e-mail i inne informacje, aby znaleźć najkorzystniejszą formę ataku.
2. **Zbrojenie.** Jeśli zachodzi taka konieczność, wnioski z fazy nr 1 wykorzystywane są do modyfikacji narzędzi przestępczych lub tworzenia nowych, które pozwolą dostać się do środowiska IT ofiary i przeprowadzić atak.
3. **Dostawa.** Gdy przestępcy są gotowi do ataku, starają się dostarczyć złośliwy kod. Mogą wykorzystać do tego celu różne narzędzia: e-mail, zainfekowane strony internetowe, ale też podrzucone pod siedzibę przedsiębiorstwa pendrive'y.
4. **Eksploatacja.** W tym momencie rozpoczyna się prawdziwe włamanie. Wykorzystując słabe strony zabezpieczeń, hakerzy uruchamiają złośliwy kod w środowisku ofiary.
5. **Instalacja.** Złośliwy kod pobiera „zadania" z zarządzanego przez przestępców centrum Command & Control.
6. **Zdalne zarządzanie.** Cyberprzestępcy mają zdalną kontrolę nad wybranymi elementami środowiska IT ofiary, mogą więc przystąpić do podjęcia akcji.
7. **Cel akcji osiągnięty.** Przestępcy miewają różne cele – zaszyfrowanie dysku i zażądanie okupu, wykradzenie poufnych danych, nazw i haseł użytkowników itd.

O cyberatakach trzeba myśleć nie jak o pojedynczych incydentach, ale jak o ciągłym procesie. Ochrona nie może skupiać się wyłącznie na przeciwdziałaniu w fazie nr 3, czyli dostarczeniu złośliwego kodu, ponieważ atak prawdopodobnie rozpoczął się wcześniej i będzie trwał znacznie dłużej, w zależności od celu cyberprzestępców.
Warto podkreślić, że nie każdy rodzaj ataku jest podzielony na fazy zamieszczone na omawianej liście. Skupia się ona na atakach z wykorzystaniem złośliwego kodu, ale nie uwzględnia wielu działań mających na celu zmanipulowanie użytkowników (social engineering).

oprogramowanie zużywające dużą część mocy obliczeniowej procesora, dzięki czemu wyeliminowanie kopiącego złośliwego kodu jest prostsze niż w przypadku zwykłych komputerów.

Generalnie sposób walki z cryptojackingiem powinien przypominać stosowany wobec innego rodzaju złośliwego kodu. Konieczne jest posiadanie oprogramowania antywirusowego (kod kopiący kryptowaluty nie będzie zbyt często zmieniany, więc rośnie szansa wykrycia go) oraz regularne aktualizowanie systemu operacyjnego i aplikacji (szczególnie przeglądarek internetowych). Dzięki temu zostaną wyeliminowane luki wykorzystywane do wprowadzenia do komputera złośliwego kodu. Na telefonach komórkowych i tabletach warto stosować oprogramowanie do zarządzania (MDM), które dobrze radzi sobie z cryptojackingiem.

Ważne są też działania edukacyjne podjęte z myślą o pracownikach i administracji przedsiębiorstwa. Koniecznie trzeba ich przekonać, by zwracali uwagę, czy komputer nie pracuje wolniej albo czy się nie przegrzewa (co łatwo zaobserwować w przypadku laptopów). Wyraźnym sygnałem obecności w firmie złośliwego kopiącego kodu będzie też zauważalny wzrost wysokości rachunków za energię elektryczną.

Hasło cenniejsze niż wszystko

Na czarnym rynku zestaw – nazwa użytkownika i hasło do (praktycznie dowolnej) usługi – sprzedawany jest kilkakrotnie drożej niż skradzione numery aktywnych kart kredytowych. Dlaczego? Większość osób stosuje te same hasła w wielu internetowych usługach. Loginem zaś bardzo często są ich adresy e-mail. Po zalogowaniu się do jednej usługi w dziale „dane użytkownika" można zdobyć wiele informacji (datę urodzenia, miejsce zamieszkania, odpowiedzi na pytania kontrolne itp.), które ułatwią zalogowanie się do kolejnych lub przeprowadzenie procesu odzyskiwania hasła.

Zdarzało się wręcz, że cyberprzestępcy organizowali „konkursy" z bardzo atrakcyjnymi, chociaż nieistniejącymi w rzeczywistości nagrodami, w których trzeba było założyć konto i podać wiele danych bardzo istotnych dla bezpieczeństwa. Z powodu naiwności użytkowników skuteczność tego typu działania jest przeogromna, a niebezpieczeństwo dla przedsiębiorstw duże, bowiem wiele osób w niewiele znaczących serwisach stosuje te same hasła, co w pracy.

Atak, w ramach którego cyberprzestępcy próbują uzyskać dostęp do wielu kont użytkowników, nazwany został credential stuffingiem. Obrona przed nim jest bardzo trudna (ale nie niemożliwa), bo jej główne narzędzie to edukacja użytkowników, a z ich przyzwyczajeniami walczyć wyjątkowo ciężko. Możliwa jest jednak automatyzacja niektórych działań zabezpieczających. Większość ataków typu credential stuffing uruchamia się za pomocą botów, których działaniu zapobiegnie firewall aplikacji sieciowych. Dobrym rozwiązaniem jest zastosowanie systemów pojedynczego logowania (SSO) oraz dwuskładnikowego uwierzytelniania. W większych przedsiębiorstwach warto rozważyć wprowadzenie systemu zarządzania tożsamością użytkowników.

Blockchain sposobem na DDoS?

Technika blockchain stosowana jest obecnie głównie do zdobywania wirtualnych walut, ale być może wkrótce przyczyni się także do walki z atakami typu DDoS. Charakterystyczne dla niej rozproszenie przetwarzania danych i wyeliminowanie pojedynczych punktów uczestniczących w realizacji transakcji, które mogą być obiektem ataku, daje nadzieję na sukces. DDoS polega na tym, że z wielu rozproszonych punktów następuje zmasowane uderzenie na jeden konkretny punkt (serwer lub punkty styku z Internetem). Gdy, dzięki zastosowaniu rozproszonej techniki blockchain, tego punktu nie będzie można zidentyfikować, atak typu DDoS przestaje w ogóle mieć sens. Natomiast trzeba pamiętać, że jest to zabezpieczenie samego procesu transakcyjnego. Zagrożone nadal będą na przykład serwery dające dostęp do tych usług (miało już miejsce wiele ataków na giełdy kryptowalut).

Jeżeli współpracujący z klientem integrator ma wpływ na kształt jego internetowych aplikacji, koniecznie należy zadbać o szyfrowanie wszystkich przesyłanych informacji. Warto monitorować nieudane próby uwierzytelniania oraz klasyfikować je. Ułatwi to zaobserwowanie pewnych prawidłowości statystycznych i odróżnienie użytkowników, którzy zawsze zapominają haseł, od działających „w ich imieniu" botów. Dobrym rozwiązaniem jest modyfikacja formularza logowania i wprowadzenie dynamicznych pól. Ich zmieniająca się lokalizacja na ekranie lub kolejność występowania utrudni stworzenie zautomatyzowanego skryptu.

Ransomware wciąż na fali

Szantażujące, szyfrujące oprogramowanie ransomware niewątpliwie było w 2017 r. zagrożeniem numer jeden. Można by zakładać, że po serii bardzo udanych tego typu ataków (m.in. WannaCry, NotPetya i Bad Rabbit), wielokrotnie nagłaśnianych w najważniejszych na świecie mediach, dziś każdy użytkownik komputera zdaje sobie sprawę z zagrożenia. Niestety, to założenie nieprawidłowe.

Dwiema najskuteczniejszymi metodami ochrony przed ransomware'em jest tzw. higiena użytkowania komputera (odwiedzanie tylko zaufanych stron, wyczulenie na e-maile phishingowe, korzystanie z antywirusa). A gdy już do zaszyfrowania danych dojdzie – zapewnienie sobie możliwości odzyskania danych z backupu. Niestety, na te metody przestępcy też znaleźli sposób. Analitycy zagrożeń wykryli już „buszujące" w Internecie kody ransomware'u, które nie były wykrywane przez moduły heurystyczne żadnego pakietu antywirusowego i omijały wszelkie zabezpieczenia zainstalowane u użytkowników prywatnych i w małych firmach. Jest też sposób na zbyt wyczulonych użytkowników. Nawet jeśli nie otworzą linka z oszukańczego e-maila, zaufają swoim znajomym, którym... cyberprzestępcy zapłacą prowizję od skutecznie przeprowadzonego ataku. Tego typu ryzyko mogą na firmę sprowadzić zwolnieni z pracy użytkownicy, a przy okazji zyskać niezłą „odprawę".

Pułapki czyhają również na osoby, które wykonują regularny backup. Ransomware

z reguły szyfruje nie tylko dane na komputerze, na którym został zainstalowany i uruchomiony, ale też na dołączonych do niego zewnętrznych pamięciach oraz udziałach sieciowych (np. z serwera NAS). Poza tym istnieje ryzyko, że świeżo zaszyfrowane pliki nadpiszą te właściwe, gdy kopie backupowe wykonywane są cały czas na tym samym nośniku. W takiej sytuacji zawsze trzeba pamiętać o włączeniu wersjonowania plików (przechowywania kilku wersji). Zalecane jest też tworzenie backupu na nośnikach wymiennych.

Czy dzięki ransomware'owi cyberprzestępcy mają przewagę? Trudno powiedzieć, wiele bitew z nimi zostało wygranych, ale na pewno nie można mówić o zbliżającym się końcu wojny. Producenci rozwiązań zabezpieczających twierdzą, że wkrótce konieczne będzie zatrudnienie sztucznej inteligencji, analizującej znacznie dokładniej działanie uruchamianego na komputerach kodu, niż robią to obecnie rozwiązania typu sandbox.

Natomiast na pewno nie wolno rezygnować z oprogramowania antywirusowego, gdyż wykrywa wszystkie znane już moduły szyfrujące. Można też zaproponować klientowi wdrożenie narzędzi wprowadzających do środowiska użytkownika białe listy aplikacji i analizujących przebieg uruchomionych procesów. Potrafią wykryć trwającą przez dłuższy czas próbę otwierania dużej liczby plików i zmiany ich zawartości, co jednoznacznie wskazuje na trwający proces szyfrowania. Naturalnie konieczne jest kontynuowanie działań edukacyjnych. Gdy prowadzą je przedstawiciele współpracującego z klientem VAR-a lub integratora, jest szansa, że pracownicy podejdą do szkolenia poważniej niż w przypadku prowadzonego przez dział IT. Zawsze też należy wykonywać backup (i weryfikację spójności skopiowanych danych). Nie tylko ze względu na ransomware.

Uporczywe ataki wciąż w modzie

Już od kilku lat za jedno z największych zagrożeń uznawane są ataki typu Advanced Persistent Threat, kierowane przeciwko precyzyjnie wybranym firmom i prowadzone według starannie przygotowanej strategii, po wcześniejszym rozpoznaniu.

Rodzaje zagrożeń różnych obszarów związanych z IT w przedsiębiorstwie

Klient
- ataki CSRF (Cross-Site Request Forgery)
- ataki MITB (Man In The Browser)
- ataki XSS (Cross-Site Scripting)
- złośliwe oprogramowanie
- ataki SQL injection

Usługi związane z aplikacją
- ataki XSS (Cross-Site Scripting)
- ataki CSRF (Cross-Site Request Forgery)
- ataki SQL injection
- złośliwe oprogramowanie
- ataki DoS (blokada usług)
- ataki na interfejsy API
- ataki MITM (Man In The Middle)
- ataki z wykorzystaniem funkcji aplikacji

Sieć
- ataki DDoS
- podsłuch
- wykorzystywanie protokołów

Dostęp
- kradzież danych uwierzytelniających
- ataki typu credential stuffing
- przechwytywanie sesji
- ataki brute force
- phishing

Protokół TLS/SSL
- ataki związane z ujawnianiem pamięci
- spoofing certyfikatu
- przechwytywanie sesji
- wykorzystywanie protokołów

Serwer DNS
- zatruwanie serwera DNS
- spoofing serwera DNS
- przechwytywanie serwera DNS
- ataki słownikowe
- ataki DDoS

Źródło: F5 Networks

– *Ochrona przed występującymi dziś zagrożeniami musi być wszechstronna* – mówi Michał Jarski, VP Sales EMEAA w firmie Wheel Systems. – *Nie można już bazować wyłącznie na firewallach i zabezpieczeniach sygnaturowych, ponieważ cyberprzestępcy zwykle nie atakują od frontu, ale przez konta uprawnionych użytkowników. Konieczne stało się skrupulatne obserwowanie wszystkich obszarów związanych z IT, które mogą być wykorzystane do ataku: każdy podłączony do sieci system jest potencjalnym punktem wejścia. Należy zwrócić uwagę szczególnie na procesy, w obsługę których zaangażowani są użytkownicy o wyższych uprawnieniach, przede wszystkim na logowanie. Najważniejsze jest szybkie ustalenie, czy loguje się właściwa osoba, czy ktoś podszywający się pod uprawnionego użytkownika. Nagrywanie zainicjowanych przez nich zdalnych sesji jest zawsze dobrym pomysłem, bo może być to jedyny dowód incydentu.*

Zespół Global Research & Analysis Team (GReAT), działający w strukturach firmy Kaspersky Lab, wskazał, że w I kwartale 2018 r. miało miejsce ujawnienie luk w procesorach firm AMD i Intel, które mogą zostać wykorzystane do przeprowadzenia ataków typu APT (chociaż na razie zademonstrowano tylko ataki przykładowe, udowadniające istnienie luki). Co prawda producenci systemów operacyjnych wydali już aktualizacje, ale wiadomo, że nie wszyscy administratorzy podchodzą wystarczająco skrupulatnie do ich instalacji. Trudno też zakładać, że wkrótce nastąpi masowa wymiana sprzętu na pozbawiony wad.

Eksperci podkreślają, że cyberprzestępcy coraz częściej do przeprowadzania ataków będą wykorzystywali luki w zabezpieczeniach sprzętu sieciowego (przede wszystkim routerów), jako kolejnego elementu infrastruktury IT, którego oprogramowanie powinno być na bieżąco aktualizowane, a nie jest. Jako przykład można wskazać ujawniony w marcu atak na routery MikroTik przeprowadzony przez grupę Slingshot. Ciekawostką było wykrycie złośliwego oprogramowania wykorzystanego przeciwko organizatorom igrzysk olimpijskich w koreańskim Pyeongchang.

Wywiad i kontrwywiad zabezpieczą firmy

Oferowany przez WatchGuard Technologies zestaw ochronny Total Security Suite zawiera szereg zabezpieczeń sygnaturowych i reputacyjnych oraz mechanizm sandbox, który ułatwia eliminowanie nowych, nieznanych lub ukrytych zagrożeń.

Skuteczna strategia obronna systemów IT, poza szczelnymi zabezpieczeniami technicznymi i szkoleniami użytkowników, powinna uwzględniać również działania analogiczne do działań wywiadu i kontrwywiadu. Wywiad powinien dostarczać informacje dotyczące aktualnego poziomu zagrożenia w Internecie oraz wykorzystywanych metod ataków i włamań. Kontrwywiad to forma ochrony obejmująca sieć wewnętrzną, a także stanowiska robocze i serwery, której celem jest wykrycie włamania lub infekcji i odizolowanie dotkniętych nią komputerów.

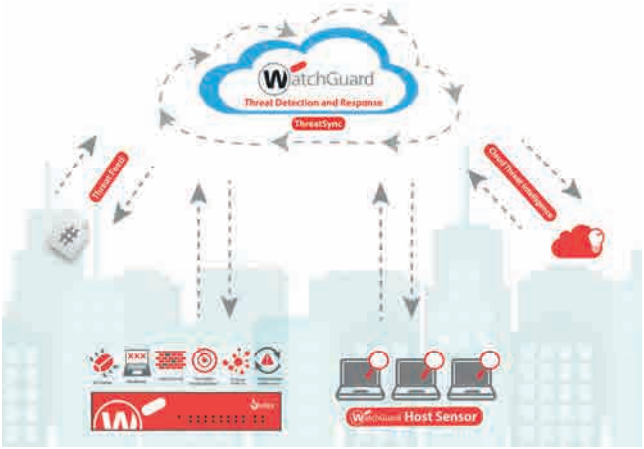
– *Mniejsze przedsiębiorstwa oraz średniej wielkości instytucje z reguły nie mają działu bezpieczeństwa IT, zatem trudno im wdrożyć rozwiązania typu wywiad i kontrwywiad* – zauważa Jerzy Trzepla, Territory Sales Manager w firmie WatchGuard Technologies. – *Dlatego, jako producent rozwiązań bezpieczeństwa sieciowego, przeznaczający swoje produkty właśnie dla tego segmentu rynku, gdy dostrzegliśmy ten brak, zaoferowaliśmy klientom zestaw ochronny Total Security Suite.*

Coraz więcej ataków

Aby wzbogacić wiedzę osób zarządzających bezpieczeństwem, WatchGuard publikuje kwartalne raporty na temat stanu zagrożeń w Internecie. Z najnowszego, dotyczącego czwartego kwartału 2017 r., wynika m.in., że liczba ataków z wykorzystaniem złośliwego oprogramowania (w porównaniu z notowaną w poprzednim kwartale) wzrosła o 33 proc., przy czym bardzo zwiększyła się ilość nowego malware'u (o 167 proc.). W tym samym czasie nasilenie ataków sieciowych wzrosło o 328 proc., a 53 proc. spośród wykrytego szkodliwego oprogramowania było już wcześniej znane (wykryte dzięki analizie sygnatur), natomiast aż 46 proc. próbek złośliwego kodu wymagało analizy w sandboksie.

Analiza od środka

Rosnąca liczba zagrożeń, mimo wdrażania wielu klasycznych zabezpieczeń, zwiększa ryzyko skutecznego zaatakowania komputerów w sieci wewnętrznej. Konieczne zatem staje się wdrożenie mechanizmów analizy behawioralnej do wykrywania zainfekowanych maszyn, które zwracają uwagę na niestandardowe działanie, co mogłoby wskazywać na szkodliwy charakter uruchamianego kodu.



Tego typu analizę zapewnia funkcja Threat Detection & Response (TDR) zawarta w pakiecie Total Security Suite. Wykrywa ona zagrożenie bezpieczeństwa przez przypisanie każdemu ze zdarzeń w ich sekwencji odpowiedniej wagi, w zależności od oszacowanego poziomu ryzyka. Istotną zaletą systemu TDR jest też korelacja zdarzeń wykrywanych na urządzeniach końcowych oraz zdarzeń sieciowych, dzięki czemu możliwe jest wcześniejsze wykrycie ataku i jego zablokowanie, uzyskanie informacji dotyczących sposobu i drogi ataku, a w konsekwencji skuteczniejsza reakcja na infekcję.

Resellerzy i integratorzy, którzy są zainteresowani przetestowaniem rozwiązania TDR dla platform Windows, macOS i Linux, mogą poprosić o udostępnienie licencji testowej pod adresem Jerzy.Trzepla@watchguard.com.

Kwartalne raporty firmy WatchGuard dotyczące stanu zagrożeń w Internecie można znaleźć w serwisie Secplicity.

Dodatkowe informacje: **Jerzy Trzepla**, Territory Sales Manager, WatchGuard Technologies, watchguard@bakotech.pl
Wojciech Pietrow, Product Manager, Bakotech, Wojciech.Pietrow@bakotech.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI WATCHGUARD TECHNOLOGIES I BAKOTECH.

Polityka bezpieczeństwa *coraz popularniejsza*

QNAP przeprowadził badanie dotyczące opinii polskich menedżerów IT na temat zagrożeń typu ransomware. Sprawdzono m.in. skalę tego zjawiska w MŚP oraz stopień uwzględnienia go w dokumentach firmowej polityki bezpieczeństwa.

Prawie połowa (47,6 proc.) uczestników badania potwierdziła, że ich przedsiębiorstwo ma kompletną i spójną politykę zabezpieczania i przetwarzania danych. Niewiele mniej, bo 31,4 proc. respondentów, zadeklarowało natomiast, że w firmie istnieje sformalizowany dokument dotyczący ochrony i przetwarzania danych, ale dotyczy jedynie wybranych najważniejszych obszarów. Jedynie co dziesiąty ankietowany przyznał, że w jego przedsiębiorstwie nie ma procedur bezpieczeństwa, lecz wykorzystuje się wybrane narzędzia, takie jak oprogramowanie antywirusowe lub systemy do tworzenia kopii zapasowych.

Za najbardziej skuteczne rozwiązanie badani uznali posiadanie aktualnego oprogramowania antywirusowego lub pakietu zabezpieczeń (73,3 proc.), jednak drugą w kolejności (63,8 proc.) najchętniej wymienianą metodą ochronną okazało się stosowanie dobrych praktyk, czyli działań bazujących na wiedzy użytkowników i wzmacnianiu ich czujności (np. ostrożnego traktowania plików nieznanego pochodzenia), a także wyrobienia nawyku pobierania danych tylko z zaufanych źródeł.

Ochrona przed ransomware'em

Za najbardziej skuteczne w ochronie przed ransomware'em respondenci uznali posiadanie aktualnego oprogramowania antywirusowego (72,4 proc.), stosowanie dobrych praktyk (63,8 proc.), natychmiastowe instalowanie aktualizacji oprogramowania (36,2 proc.) oraz pełny lub różnicowy backup danych (33,3 proc.).

Może dziwić bardzo słaba pozycja narzędzi związanych z backupem – kopie migawkowe wskazało jedynie 10,5 proc. respondentów. Podobnie nisko sklasyfikowane zostało szyfrowanie kluczowych danych (15,2 proc.). Tylko nieliczni (4,8 proc.) za skuteczną metodę ochrony danych przed ransomware'em uznali wykorzystanie serwerów NAS jako jednego z miejsc przechowywania kopii bezpieczeństwa.

– *Wyniki te ewidentnie wskazują na konieczność kontynuowania działań edukacyjnych dotyczących funkcjonalności serwerów NAS i możliwości wykorzystania ich do ochrony przed zaszyfrowaniem danych* – twierdzi Grzegorz Bielawski, Country Manager w polskim oddziale QNAP.

Grzegorz Bielawski
Country Manager, QNAP

Dużym zaskoczeniem dla nas było, że chociaż niemal połowa ankietowanych osób wykorzystuje serwery NAS jako jedną z form backupu danych, to wysoką skuteczność tego typu rozwiązań w roli jednej z lokalizacji kopii bezpieczeństwa wskazało tylko 7,6 proc. z nich. Tymczasem to właśnie backup na serwery NAS i wykonywanie kopii migawkowych z już zgromadzonych w serwerze danych są bardzo skuteczną i tanią metodą ochrony. Warto przekonywać do tego klientów, tym bardziej że funkcję tę zapewniają wszystkie serwery firmy QNAP, nawet te najtańsze, z procesorami ARM.

Bezpieczeństwo przez różowe okulary

Praktycznie wszyscy (99 proc.) uczestnicy badania pozytywnie ocenili poziom zabezpieczeń swojej firmy, a 96 proc. – poziom ochrony przed ransomware'em. Co zaskakujące, w tej grupie znalazły się także wszystkie osoby, które zadeklarowały nieistnienie w ich przedsiębiorstwach jakichkolwiek sformalizowanych reguł polityki bezpieczeństwa, a nawet te, które wprost przyznają, że w ich firmach nie są wykorzystywane żadne narzędzia służące do zwiększania bezpieczeństwa danych.

Niemniej jednak blisko co trzeci badany przyznał, że firma, w której pracuje, była ofiarą ataku zakończonego utratą danych, ale w większości przypadków nie spowodowało to znaczących problemów związanych z funkcjonowaniem przedsiębiorstwa (68,8 proc.). Natomiast polskie firmy doświadczone atakami na ich środowiska IT rzetelnie podeszły do przeciwdziałania kolejnym naruszeniom bezpieczeństwa. Aż 71,9 proc. ankietowanych przyznało, że wystąpienie incydentów spowodowało udoskonalenie wykorzystywanych mechanizmów zabezpieczania danych.

W efekcie co piąty uczestnik badania zadeklarował, że w ciągu najbliższego roku jego firma zwiększy nakłady na rozwiązania ochronne, 41 proc. ankietowanych, że wydatki te będą takie same jak dotychczas, a jedynie 3,8 proc. zapowiedziało uszczuplenie budżetu przeznaczonego na tego typu inwestycje. Niestety, zauważalna grupa przedsiębiorstw (14,3 proc.) nie planuje w bieżącym roku przeznaczyć na ochronę kluczowych danych jakichkolwiek środków finansowych.

Dodatkowe informacje: Grzegorz Bielawski, Country Manager, QNAP, gbielawski@qnap.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ QNAP.

Ivanti upraszcza wielowarstwową ochronę

Co roku w wyniku działań cyberprzestępców dwukrotnie rośnie liczba wycieków danych. Sięgają oni po wszelkie możliwe sposoby, aby napełnić swoje portfele lub kryptowalutowe konta. Ivanti uważnie przygląda się temu trendowi i proponuje rozwiązania, które zapewniają zabezpieczenie infrastruktury IT nawet w miejscach nie zawsze uznawanych za podatne na ataki.

Ten przypuszczony przez cyberprzestępców szturm można jednak zatrzymać. Wystarczy, że administratorzy IT nie tylko skupią się na technicznych aspektach zabezpieczeń, ale też stworzą odpowiednie procedury w przedsiębiorstwie oraz regularnie będą prowadzili szkolenia pracowników. Ma to szczególne znaczenie tam, gdzie dopuszcza się podłączanie do firmowej sieci sprzętu prywatnego lub pozwala użytkownikom na korzystanie z Internetu za pośrednictwem służbowych urządzeń mobilnych poza siedzibą przedsiębiorstwa.

Bardzo ważne jest również usprawnienie pracy administratorów. Powinni bardzo szybko reagować na nowe zagrożenia, a to możliwe jest tylko wtedy, gdy zautomatyzowane zostaną wykonywane przez nich, powtarzalne zadania. Ma to szczególne znaczenie, ponieważ w przypadku ponad 90 proc. ataków do szkód dochodzi już w pierwszej minucie od podjęcia działań przez cyberprzestępców.

Najważniejsze są aktualizacje

Znakomita większość wykorzystywanych obecnie przez złośliwe oprogramowanie luk została wykryta już wcześniej, a producenci „dziurawych" aplikacji stworzyli odpowiednie łatki. Tak było m.in. w przypadku wszystkich dużych ubiegłorocznych ataków za pomocą ransomware'u. Według badań zespołu Verizon RISK w 2015 r. w wielu atakach przestępcy wykorzystywali luki w oprogramowaniu, które powstało w... 2007 r.

Dla wszystkich ekspertów ds. bezpieczeństwa oczywiste jest, że regularne łatanie oprogramowania to obecnie jedna z najskuteczniejszych metod ochrony przed atakami. Jak jednak zapewnić systematyczną aktualizację oprogramowania na wszystkich komputerach bez konieczności wcześniejszego sprawdzania łatek pod kątem poprawności ich pracy czy zgodności z innym używanym w firmie oprogramowaniem oraz zatrudniania batalionu informatyków do przeprowadzenia ich instalacji?

Ivanti oferuje bogaty wybór narzędzi, które – dzięki zdefiniowanym przez producenta regułom polityki aktualizacji – zapewnią inwentaryzację wszystkich posiadanych przez klienta systemów operacyjnych i aplikacji (zarówno w środowiskach fizycznych, jak i wirtualnych), a następnie zweryfikują ich wersje i sprawdzą dostępność łatek, a w końcu zainstalują je. Producent proponuje również plug-in do oprogramowania zarządzającego Microsoft System Center Configuration Manager, który upraszcza proces instalowania aktualizacji przez konsolę SCCM. Wartość tego oprogramowania wynika m.in. z faktu, że Patch Manager for SCCM firmy Ivanti łata nie tylko różne systemy operacyjne, ale przede wszystkim oprogramowanie firm trzecich. Dzięki dostępności API oprogramowanie Ivanti może być integrowane z innymi rozwiązaniami ochronnymi, skanerami podatności na ataki oraz narzędziami konfiguracyjnymi i raportującymi.

Jeśli nie możesz załatać – blokuj!

Łatanie oprogramowania nie zda egzaminu w przypadku ataków dnia zerowego. Wykorzystywane w takiej sytuacji luki nie są znane autorom atakowanej aplikacji, więc siłą rzeczy nie mają jeszcze przygotowanej odpowiedniej aktualizacji. Istnieje też wiele firm, które – z różnych powodów – korzystają ze starych wersji nierozwijanego już oprogramowania, często opracowanego specjalnie na ich zlecenie. W przedsiębiorstwach czasami dochodzi także do zjawiska „shadow IT", gdy użytkownicy bez wiedzy administratorów samodzielnie instalują potrzebne im do pracy oprogramowanie lub korzystają z nieautoryzowanych usług chmurowych.

Strategii postępowania w takich sytuacjach może być kilka. Restrykcyjna zakłada stworzenie białej listy dopuszczonych przez administratorów do użytku aplikacji i blokadę wszystkich pozostałych. Strategie mniej restrykcyjne mogą zakładać korzystanie także

>>> Trzy pytania do...

Bogdana Lontkowskiego, dyrektora regionalnego Ivanti na Polskę, Czechy, Słowację i kraje bałtyckie

CRN Co obecnie stanowi największe wyzwanie dla firm w kontekście zabezpieczania ich zasobów IT?

Bogdan Lontkowski Niestety, wciąż bardzo wiele rzeczy. Przedsiębiorstwa często w ogóle nie są świadome tego, co posiadają, więc w konsekwencji nie wiedzą, co chronić. Nie aktualizują używanego oprogramowania, przez co zostawiają otwarte drzwi dla cyberprzestępców i to jest chyba dziś największe zagrożenie. Coraz częściej można spotkać się z – jak najbardziej błędną – opinią, że nie ma już sensu stosowanie antywirusów. A przede wszystkim, w firmach brakuje procedur, które klarownie opisywałyby, w jaki sposób należy dbać o środowisko IT, zarządzać uprawnieniami dostępu, edukować użytkowników i reagować w przypadku wystąpienia problemu.

CRN Opracowanie i stosowanie procedur ochronnych jest też jednym z głównych wymogów stawianych przez RODO...

Bogdan Lontkowski Dokładnie tak, dlatego ogromnie ważne jest skrupulatne przyjrzenie się całemu środowisku IT, nie tylko w jego technicznej warstwie. Widzimy, że coraz lepiej w tej dziedzinie radzą sobie nasi partnerzy. Stają się konsultantami biznesowymi, często ratując klientów przed niemałymi problemami. Dlatego zawsze gorąco namawiamy współpracujących z nami integratorów, aby rozwijali swoją ofertę usługową, niezależnie od działalności sprzedażowej.

CRN Czy Ivanti oferuje im specjalne licencje oprogramowania służącego właśnie do świadczenia usług?

Bogdan Lontkowski Tak, mamy w ofercie tego typu licencje, dzięki którym partnerzy zyskują dużą swobodę kreowania oferty. To oni pozostają użytkownikami oprogramowania, ale mogą zainstalować je i we własnej infrastrukturze, i u klienta. Może to być bardzo dobre uzupełnienie ich oferty eksperckiej, bazującej na modelowaniu procesów IT klienta i szkoleniu zarówno administratorów, jak i użytkowników. Oczywiście wymagamy też, aby pracownicy firm integratorskich ukończyli odpowiednie kursy i zyskali kwalifikacje na jak najwyższym poziomie.

z aplikacji spoza listy. W takiej sytuacji jednak administratorzy powinni być wyposażeni w narzędzia, które na przykład w momencie wystąpienia zmasowanego, globalnego ataku, zagwarantują szybkie przejście do najbardziej rygorystycznego modelu, z zastosowaniem białej listy. Również w takim przypadku pomogą narzędzia firmy Ivanti – zapewniają bowiem bardzo bogaty zestaw funkcji ułatwiających zarządzanie aplikacjami i blokowanie wykonania nieautoryzowanego i niezaufanego kodu.

Ochrona w każdym punkcie

Ivanti ma także w ofercie zaawansowaną platformę służącą do ochrony urządzeń końcowych, która umożliwia stworzenie i wdrożenie globalnych reguł polityki bezpieczeństwa stacji roboczych, diagnozę stanu ich bezpieczeństwa i zdalne zarządzanie oraz raportowanie itd. Narzędzia te współpracują z opisanymi wcześniej rozwiązaniami Ivanti do zautomatyzowanego zarządzania aktualizacjami oraz uruchamianymi aplikacjami. Bez problemu mogą być również używane z popularnymi aplikacjami antywirusowymi.

Oprogramowanie firmy Ivanti zawiera cały szereg funkcji, które administratorzy mogą wykorzystać do ochrony swojego środowiska IT. Jedną z rekomendowanych (także w RODO) jest wymuszenie szyfrowania danych na podłączanych do komputera przenośnych urządzeniach pamięci (pendrive'ach i twardych dyskach). Można też zablokować uruchamianie skryptów pobranych z Internetu lub udzielać zgody na ich wykonywanie tylko przez wybrane aplikacje. Moduł skanujący zachowanie uruchomionych na komputerze procesów jest też w stanie szybko wykryć próbę równoczesnego zaszyfrowania wielu plików i zablokować ją, ponieważ to zjawisko ewidentnie wskazuje na działanie ransomware'u.

Administrator musi wiedzieć

Nawet najlepsze rozwiązania ochronne spełnią swoje zadanie tylko w połowie, jeśli nie będą informowały administratorów o aktualnym poziomie bezpieczeństwa oraz wykrytych problemach. W narzędziach firmy Ivanti to zagadnienie jest potraktowane bardzo poważnie. Osoby zarządzające środowiskiem IT, korzystając z oprogramowania tego producenta, mają pełny wgląd w informacje dotyczące jego ochrony. Mogą także w prosty sposób tworzyć raporty o różnym poziomie ogólności i złożoności przedstawianych informacji (dla zarządu, dyrektorów, kierowników linii biznesowych, użytkowników aplikacji itd.).

Rozwiązania te zapewniają integrację z wieloma innymi narzędziami do zarządzania infrastrukturą IT i monitorowania jej. Dzięki temu nie trzeba opracowywać skryptów ani zatrudniać dodatkowych osób, które byłyby odpowiedzialne wyłącznie za zapewnienie ciągłości pracy i mozolne wypełnianie arkuszy kalkulacyjnych z raportami.

Autoryzowanymi dystrybutorami oprogramowania Ivanti w Polsce są firmy: Alstor, Headtechnology oraz Prianto.

Dodatkowe informacje:
Bogdan Lontkowski, dyrektor regionalny na Polskę, Czechy, Słowację i kraje bałtyckie, Ivanti, bogdan.lontkowski@ivanti.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ IVANTI.

IBM Security – *przemyślana strategia ochrony*

Wieloletnie doświadczenie IBM-a w zakresie budowania systemów bezpieczeństwa i kompleksowe podejście do rozwiązań IT w wielu sektorach pozwoliło stworzyć grupę produktów IBM Security, które chronią wszystkie obszary teleinformatycznych środowisk klientów.

Celem, który postawili przed sobą inżynierowie IBM-a, było zaprojektowanie swego rodzaju układu odpornościowego, który chroni przedsiębiorstwo przed zarażeniem, a jeśli do niego dojdzie, upraszcza i skraca jak to tylko możliwe czas leczenia oraz minimalizuje ewentualne straty. Obecnie rozwiązania producenta zapewniają zabezpieczenie wszystkich firmowych zasobów (infrastruktury, aplikacji, danych i procedur), a także kontrolowanie zachowań użytkowników.

Zawarte w IBM Security rozwiązanie **QRadar SIEM** umożliwia monitorowanie sieci i korelację informacji o zdarzeniach. Kontrola stacjonarnych i przenośnych urządzeń użytkowników końcowych odbywa się za pomocą oprogramowania **BigFix** i **MaaS360**. Wiele produktów z rodziny IBM Security gwarantuje także ochronę aplikacji działających w chmurze.

Pracownicy pod kontrolą

Według przeprowadzonych przez ekspertów ds. bezpieczeństwa analiz najwięcej włamań pochodzi z wewnątrz firmy, a odpowiedzialni za nie są pracownicy etatowi oraz sezonowi. Dlatego jednym z najważniejszych elementów bezpiecznego środowiska IT w przedsiębiorstwie jest system chroniący dostęp do aplikacji – umożliwiający identyfikację użytkowników i zarządzanie ich uprawnieniami.

Rozwiązania IBM-a gwarantują kompleksową ochronę w tym zakresie. Przełożony użytkownika, a nawet on sam może wnioskować o stworzenie konta z odpowiednimi uprawnieniami do konkretnych systemów i na określony czas. Gdy dana osoba przestanie być pracownikiem firmy, jej uprawnienia zostaną automatycznie zablokowane, co chroni cenne dane przed niepowołanym dostępem lub kradzieżą.

Andrzej Bugowski
IBM Business Unit Manager, Tech Data

W środowiskach IT często można zauważyć odizolowane od siebie „wyspy" – obszary wymagające ochrony, takie jak styk sieci z Internetem, rdzeń sieci, urządzenia końcowe, aplikacje itd. Indywidualne zajmowanie się każdym z nich to jak poszukiwanie lekarstwa na poszczególne objawy choroby. Takie punktowe rozwiązywanie problemów w przypadku zabezpieczeń środowiska IT rzadko bywa skuteczne. Wymaga bowiem wielu ludzi do ochrony poszczególnych obszarów, co wpływa na rozproszenie odpowiedzialności. Administratorzy często nie wiedzą o podjętych przez kolegów akcjach, więc działają po omacku. Dlatego konieczne jest wdrożenie systemu, który będzie ustanawiał procedury administracyjne i koordynował działania poszczególnych osób odpowiedzialnych za ich realizację.

Kolejnym obszarem, o którego zabezpieczenie trzeba zadbać, są bazy danych. Rozwiązanie **Guardium Data Activity Monitor** gwarantuje ochronę przed nieautoryzowanym dostępem do baz danych, a także szyfruje przechowywane w nich informacje i dostarcza mechanizmów dynamicznego maskowania danych (tzw. pseudonimizacji). Informacje o wszelkiego rodzaju odchyleniach od normy zaobserwowanych przez produkty Guardium są automatycznie przesyłane do centralnego repozytorium, jakie stanowi QRadar SIEM, gdzie następuje analiza i korelacja informacji o incydentach, ułatwiająca wczesne wykrywanie zagrożeń.

Wiarygodne źródła i szybkie decyzje

IBM ma w ofercie także narzędzia z rodziny **Cognitive** wspomagające szybkie podejmowanie decyzji i odpowiednich działań związanych z cyberochroną. Produkt **Watson for Cybersecurity** pełni funkcję wirtualnego eksperta, który ma dostęp do bardzo rozbudowanych baz wiedzy IBM X-Force, agregujących informacje z Internetu, oraz fragmentów darknetu. Pozwala na znacznie szybsze zabezpieczenie danego zasobu, gdyż zawiera gotowe scenariusze działań, opracowane dla konkretnych sytuacji, które mogą zaistnieć.

W prawidłowo zabezpieczonym środowisku powinna być wdrożona wyspecjalizowana platforma zarządzająca całym procesem reagowania na incydenty naruszenia bezpieczeństwa: inicjująca konkretne akcje, które należy podjąć po wykryciu zagrożenia, powiadamiająca odpowiednie osoby i nadzorująca wykonanie poszczególnych kroków (koncepcja jej działania podobna jest do realizacji planu disaster recovery). Tego typu platformę oferuje IBM – rozwiązanie **Resilient** można zintegrować z systemami różnych dostawców, dzięki czemu nie jest konieczna wymiana stosowanych już w firmie produktów ochronnych.

Dodatkowe informacje:
Andrzej Bugowski, IBM Business Unit Manager, Tech Data, andrzej.bugowski@techdata.com

Intercept X – przyszłość bezpieczeństwa IT

Głębokie uczenie (deep learning), jako zaawansowana forma uczenia maszynowego, umożliwiło zmianę podejścia do zabezpieczania urządzeń końcowych. Dzięki tej technice proponowane przez Sophos rozwiązanie Intercept X zapewnia ich proaktywną ochronę przed nieznanymi zagrożeniami.

Firma Sophos jest jednym z najbardziej doświadczonych na rynku dostawców rozwiązań cyberochronnych i od lat wykorzystuje w nich także mechanizm głębokiego uczenia. Zastosowano go po raz pierwszy w celu wykrywania złośliwego oprogramowania w 2010 r., gdy w amerykańskiej Agencji Zaawansowanych Projektów Badawczych w Obszarze Obronności (DARPA) stworzono pierwszy program „cybergenetyczny". Zakładano, że będzie pomocny w wykrywaniu DNA złośliwego kodu i różnego typu cyberataków. Dzisiaj podobne algorytmy są zaimplementowane w oferowanym przez Sophos rozwiązaniu Intercept X.

Wielu producentów deklaruje, że ich narzędzia wykorzystują nauczanie maszynowe, ale w rzeczywistości skuteczność tych rozwiązań bywa różna. Inspiracją stosowanego przez Sophos mechanizmu bazującego na sieciach neuronowych, wykorzystywanego do wykrywania złośliwego kodu, była praca ludzkiego mózgu. Jest to ten sam rodzaj uczenia maszynowego, jaki jest stosowany w algorytmach służących do rozpoznawania twarzy, przetwarzania naturalnego języka, programowania samochodów autonomicznych i w innych dziedzinach naukowych aktywnie wspieranych przez komputery.

Głębokie uczenie jest znacznie skuteczniejsze niż inne metody uczenia maszynowego, takie jak random forest, algorytm centroidów czy sieci bayesowskie, ale wymaga ogromnej ilości danych oraz dużej mocy obliczeniowej. Dzięki wieloletniemu doświadczeniu działu SophosLabs oraz wykorzystywaniu zbieranej przez ponad 30 lat olbrzymiej bazy próbek złośliwego kodu (która codziennie jest zasilana informacjami z ponad 100 mln urządzeń końcowych użytkowników oprogramowania producenta) model stworzony przez Sophos jest niezawodny.

Tradycyjne metody uczenia maszynowego charakteryzują się też tym, że analizowane bazy danych mają bardzo dużą objętość, niekiedy zajmują na dysku wiele gigabajtów. Sophos opracował sposób skutecznego kompresowania danych, dzięki czemu ich baza zajmuje mniej niż 20 MB na urządzeniu końcowym i praktycznie nie wpływa na jego wydajność.

Optymalizacja wykorzystywania zasobów pamięci ma duże znaczenie, bo większość rozwiązań ochronnych działa w sposób reaktywny i zdecydowanie zbyt wolno. Liczba oraz poziom skomplikowania ataków wciąż rośnie, dlatego stosowane dotychczas metody zabezpieczeń przestały wystarczać. Dla przykładu, SophosLabs analizuje dziennie ponad 400 tys. nowych próbek złośliwego kodu, a 75 proc. z nich nigdy się nie powtarza.

Głębokie uczenie przetestowane

Sophos dba o przejrzystość stosowanej metody wykrywania zagrożeń. Była prezentowana podczas takich konferencji jak Black Hat, a także testowana przez niezależne instytucje. Jedną z nich jest VirusTotal, która w sierpniu 2016 r. wystawiła rozwiązaniu Intercept X pozytywną ocenę. Podobnie było w testach przeprowadzonych przez NSS Labs. We wszystkich przypadkach podkreślano bardzo wysoką wydajność pracy rozwiązania i małą liczbę fałszywych alarmów.

MARIUSZ RZEPKA
Territory Manager
Eastern Europe, Sophos

Stosowana w Intercept X neuronowa sieć, na której bazuje koncepcja głębokiego uczenia, działa jak ludzki mózg. Dzięki temu zapewnia bardzo wysoką skuteczność wykrywania zarówno znanego złośliwego kodu, jak i ataków dnia zerowego. Gwarantuje także niższy niż w przypadku tradycyjnych rozwiązań współczynnik fałszywych alarmów. Potwierdzili to analitycy z laboratorium ESG, którzy w raporcie z grudnia 2017 r. poinformowali, że Intercept X zatrzymał każdy rodzaj zasymulowanego skomplikowanego ataku.

Dlatego Sophos postawił sobie za cel, aby stosowany przez niego mechanizm głębokiego uczenia był bardzo szybki. Udało się go osiągnąć – w ciągu 20 ms można zasymulować miliony sposobów zachowania danego pliku (przed jego uruchomieniem), dokonać dogłębnej analizy działania i ocenić, czy jest to złośliwy kod.

Autoryzowanymi dystrybutorami rozwiązań Sophos w Polsce są firmy AB i Konsorcjum FEN.

SOPHOS

Dodatkowe informacje: MARIUSZ RZEPKA, TERRITORY MANAGER EASTERN EUROPE, SOPHOS, MARIUSZ.RZEPKA@SOPHOS.COM

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SOPHOS.

Cognito ujawni tożsamość ataku

Stworzone przez Vectra Networks rozwiązanie Cognito to platforma wykorzystująca sztuczną inteligencję do automatyzacji wykrywania ataków i reagowania na nie. Działa w chmurach publicznych, prywatnych centrach danych i środowiskach korporacyjnych. Skutecznie odnajduje ukryte i nieznane zagrożenia, zanim wyrządzą szkody.

Cognito zdobywa informacje o prowadzonych cyberatakach dzięki analizie całego ruchu sieciowego wykorzystującej zaawansowane techniki uczenia maszynowego (w tym głębokie uczenie i sieci neuronowe). Stała ochrona jest zapewniona dzięki algorytmom sztucznej inteligencji oraz zaawansowanej analizie matematycznej. System nie opiera skuteczności wykrywania zagrożeń na bazie sygnatur, definicji ataków oraz jakichkolwiek aktualizacjach. Firma Vectra określa swoje rozwiązanie mianem „analityka bezpieczeństwa w oprogramowaniu", przedstawia jako kolejnego członka zespołu działu SOC (Security Operations Center), który nie śpi, nie je, nie choruje, ale cały czas pracuje, uczy się i tropi intruzów.

Na rozwiązanie Vectry składa się jednostka centralna (urządzenia z serii X) – „mózg" Cognito agregujący informacje z podłączonych do niego sensorów (urządzenia z serii S). Zbierają one „surowe" dane z przełączników rdzeniowych i dostępowych z wykorzystaniem funkcji port mirroring. Dzięki niewielkim rozmiarom i bardzo prostej instalacji mogą być wdrażane w sieci na wiele sposobów, także w oddziałach firmy lub np. punktach sprzedaży detalicznej, które ona prowadzi.

Statystycznie ok. 80 proc. ruchu generowanego w centrum danych nigdy nie opuszcza korporacyjnej sieci i nie jest monitorowane przez tradycyjne brzegowe narzędzia ochronne. Dla administratorów, którzy chcą mieć zapewnioną widoczność całego ruchu i wykrywać zagrożenia funkcjonujące w środowisku wirtualnym VMware ESXi, przeznaczone są wirtualne sensory vSensors, które łączą się z dowolnym przełącznikiem VMware vSwitch. Istnieje także możliwość integracji rozwiązania Cognitoz oprogramowaniem VMware vCenter, dzięki czemu zapewniony zostaje szczegółowy wgląd w wirtualne środowisko.

Urządzenia Vectra są umieszczane w infrastrukturze w sposób pasywny, dzięki czemu nie naruszają istniejącej topologii sieci. Jako dane wejściowe dostają „surową" kopię ruchu sieciowego, a nie tylko logi (jak w rozwiązaniach SIEM) lub dane statystyczne (jak w systemach bazujących na protokołach NetFlow, sFLOW, jflow czy IPFIX). Informacje te są wprowadzane do algorytmów mechanizmu uczenia maszynowego, które umożliwiają stworzenie mapy zagrożeń. Tym samym rozwiązanie firmy Vectra nie rozpoznaje konkretnego ataku, ale informuje o tym, na jakim etapie działania jest atakujący.

Proces „polowania" na cyberataki jest w pełni automatyzowany. Cognito ujawnia miejsca, gdzie ukrywa się przestępca (a także odtwarza ścieżkę, przez którą przedostał się do firmowej infrastruktury) i sprawdza, jakie jest jego zadanie. W ten sposób skraca nawet o 29 razy (na podstawie osiągniętych rezultatów u klientów Vectry) czas potrzebny na analizę przez administratora zdarzeń związanych z bezpieczeństwem. Oprócz oczywistej korzyści w postaci szybsze-

GARTNER W NAJNOWSZYM RAPORCIE „MAGIC QUADRANT FOR IDPS" PO RAZ PIERWSZY OD PIĘCIU LAT SKLASYFIKOWAŁ JAKIEŚ PRZEDSIĘBIORSTWO W SEKCJI „WIZJONERZY". TRAFIŁA TAM FIRMA VECTRA. ZDANIEM ANALITYKÓW DO KOŃCA 2020 R. 60 PROC. ROZWIĄZAŃ IDPS BĘDZIE WYKORZYSTYWAŁO TAKIE METODY JAK UCZENIE MASZYNOWE ORAZ ANALIZA ZACHOWAŃ UŻYTKOWNIKÓW. OBECNIE WSPÓŁCZYNNIK TEN WYNOSI PONIŻEJ 10 PROC.

go wyeliminowania zagrożenia Cognito zapewnia panaceum na niedobór personelu, a szczególnie analityków bezpieczeństwa, z którym borykają się prawie wszystkie działy IT.

Szyfrowanie to nie problem

Zaszyfrowanie danych może umożliwić ukrycie wielu elementów ataku. Tradycyjne narzędzia ochronne do analizy wykorzystują głęboką inspekcję pakietów (deep packet inspection), co jest nieskuteczne w przypadku szyfrowanego ruchu. Tymczasem Cognito zapewnia wgląd w ruch sieciowy w czasie rzeczywistym (wewnątrz sieci, infrastruktury wirtualnej, płynący z/do Internetu oraz środowiska przetwarzania w chmurze).

Wykorzystane przez Vectrę zautomatyzowane metody wykrywania zagrożeń, wspierane przez sztuczną inteligencję, stanowią przełom w kontekście analizy ruchu szyfrowanego. Koncentrują się na identyfikacji zagrożeń w sposób, w jaki się one zachowują, a nie na zawartości lub kodzie, z którego korzystają. W ten sposób nawet ataki ukryte w szyfrowanych danych mogą zostać wykryte i zarządzający bezpieczeństwem ma szansę na poprawę stanu ochrony, zanim zagrożenia doprowadzą do poważnych incydentów i naruszeń bezpieczeństwa.

Rozwiązanie firmy Vectra swoim działaniem obejmuje każde urządzenie z dostępem do sieci IP – komputery, serwery, drukarki, systemy Internetu rzeczy itd. Zapewnia identyfikację i ocenę reputacji także urządzeń prywatnych użytkowników (BYOD) oraz wszelkich systemów operacyjnych i aplikacji. Weryfikuje ruch w środowisku wirtualnym w chmurze prywatnej i publicznej oraz w aplikacjach SaaS.

Analiza dokonywana przez Cognito bazuje na danych opracowanych w przyjętym i zaakceptowanym przez branżę zabezpieczeń języku strukturalnym STIX (Structured Threat Information Expression), który służy do opisywania budowy złośliwego kodu i zasad jego funkcjonowania. Zebrane dane są korelowane z informacjami o zaobserwowanych działaniach atakującego, dzięki czemu zapewnione jest lepsze oszacowanie ryzyka. Cognito potrafi również wykryć próby dostępu do poufnych informacji przez nieupoważnionych pracowników firmy, a także wszelkiego typu naruszenia zasad związanych z korzystaniem z pamięci USB, internetowych serwisów do przechowywania i udostępniania danych oraz innych sposobów ich przenoszenia.

Ponadto Cognito współpracuje z firewallami nowej generacji, oprogramowaniem do ochrony urządzeń końcowych i systemami NAC, dzięki czemu zapewnia automatyczne blokowanie nieznanych i niestandardowych cyberataków. Rozwiązanie to może pomóc w wykrywaniu działania ransomware'u we wszystkich fazach ataku. Dzięki ciągłemu monitorowaniu ruchu w sieci wewnętrznej w ciągu kilku sekund identyfikuje zachowanie charakterystyczne dla szyfrującego złośliwego kodu. Udostępnia administratorom informacje o zaobserwowanych poleceniach skanowania podłączonych do sieci urządzeń pod kątem podatności na ataki, potrafi też ujawnić sam proces dystrybucji kodu ransomware.

Wyłącznym dystrybutorem Vectra Networks w Polsce jest firma Yellow Cube.

>>> Trzy pytania do...

Doroty Otczyk, Country Managera w polskim oddziale Yellow Cube

CRN Yellow Cube jest nowym podmiotem w Polsce...

Dorota Otczyk Tak, rozpoczęliśmy działalność polegającą na dystrybucji z wartością dodaną w 2018 r. Polska to największy rynek w Europie Środkowo-Wschodniej, który był, można powiedzieć, brakującym ogniwem, ostatnim elementem w naszej strategii dążenia do zdobycia pozycji lidera wśród dystrybutorów rozwiązań bezpieczeństwa IT w tym regionie. Centrala grupy znajduje się na Węgrzech, a pozostałe biura zlokalizowane są na Słowacji, Ukrainie i w Rumunii.

CRN Jaka jest strategia Yellow Cube na polskim rynku?

Dorota Otczyk Koncentrujemy się na rozwijaniu oferty najnowocześniejszych rozwiązań w zakresie zabezpieczeń IT. Reprezentujemy producentów zarówno nieznanych na rynku Europy Środkowo-Wschodniej, jak i renomowanych dostawców, którzy są ekspertami w swoich dziedzinach. Yellow Cube buduje unikalną wizję cyberbezpieczeństwa, działając jako wyłączny regionalny dystrybutor, który nie ma w portfolio rozwiązań konkurujących ze sobą vendorów. W Polsce rozpoczynamy dystrybucję, koncentrując się na jednym produkcie o największym potencjale – rozwiązaniu Cognito firmy Vectra Networks. Dziś wszyscy mówią o sztucznej inteligencji, bo idealnie odpowiada na aktualne wyzwania w obszarze bezpieczeństwa IT – dużą ilość informacji do przetworzenia oraz braki kadrowe w zespołach ds. cyberbezpieczeństwa. Następnie kolejno będziemy wprowadzać inne rozwiązania chroniące infrastrukturę IT, takie jak SCADA, oraz zapewniające monitorowanie aktywności pracowników firmy.

CRN Na jakich zasadach będziecie współpracowali z partnerami?

Dorota Otczyk W tej chwili budujemy kanał partnerski w Polsce. Nasz program regulujący zasady współpracy z resellerami i integratorami jest bardzo prosty i przejrzysty. Współdziałamy bezpośrednio wyłącznie z nimi, bo to oni mają zbudowane relacje z klientami i klienci im ufają. W przypadku pierwszego produktu, jakim jest rozwiązanie Vectra, stawiamy na edukację. Obecnie koncentrujemy się na organizacji warsztatów technicznych oraz zdalnych sesji szkoleniowych. Wszystkich zainteresowanych tym, co się dzieje w naszej firmie, zapraszam do odwiedzenia strony www.yellowcube.eu, a także zaprenumerowania newslettera.

Dodatkowe informacje: Dorota Otczyk, Country Manager, Yellow Cube, dorota.otczyk@yellowcube.eu

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI VECTRA NETWORKS I YELLOW CUBE.

Ilustracja AdobeStock

Pokonać malware: nowe fronty walki

Laboratoria producentów oprogramowania zabezpieczającego zwykle potrafią dotrzymać tempa cyberprzestępcom. Budżety IT w firmach niestety nie są aż tak elastyczne.

Wojciech Urbanek

Zwroty akcji w cyberprzestępczym światku zaskakują nawet najlepszych specjalistów z branży IT. Nie inaczej było w ubiegłym roku. Obok poważnych epidemii pojawiły się nowe rodzaje infekcji, a jednocześnie rozkwitał przestępczy proceder powiązany z kryptowalutami (cryptojacking). Wprawdzie w ostatnim czasie najczęściej dyskutowano o atakach ransomware, niemniej jednak cyberprzestępcy działali na wiele sposobów.

Według badań Malwarebytes Labs w ubiegłym roku liczba wykrytych porywaczy przeglądarek (hijacker) wzrosła o 40 proc., a programów szpiegujących o 30 proc. W drugiej połowie 2017 r. analitycy zaobserwowali niepokojące zjawisko wysypu trojanów bankowych. Liczba wirusów z tej grupy w porównaniu z notowaną w analogicznym okresie 2016 r. wzrosła o 102 proc.

Warto zaznaczyć, że na liście największych szkodników zagrażających użytkownikom biznesowym znalazły się adware i tzw. riskware tools, czyli programy z natury nieszkodliwe, których nieumiejętne stosowanie może być bardzo niebezpieczne.

Co czeka nas w tym roku? Przewidywanie nawet niezbyt odległej przyszłości

w segmencie zabezpieczeń infrastruktury IT jest wyjątkowo niewdzięcznym zadaniem. Czy ktokolwiek spodziewał się wybuchu afery związanej z lukami w procesorach Intela i AMD? Część specjalistów uważa, że ta historia będzie miała dalszy ciąg. Jednak jej wydźwięk może mieć pozytywny wpływ na właścicieli firm oraz szefów działów IT. Niewykluczone, że strach przed skutkami poważnych ataków zmobilizuje ich do częstszej aktualizacji systemów.

W ubiegłym roku rzadko wspominano o incydentach związanych z Internetem rzeczy. Eksperci podejrzewają, że to cisza przed burzą, a kolejni następcy Mirai mogą pojawić się w każdej chwili. Nie jest żadną tajemnicą, że bieżący rok w branży zabezpieczeń IT stać będzie pod znakiem RODO. Rozporządzenie stanie się jednym z motorów napędowych rynku systemów ochronnych. Na nową dyrektywę należy spojrzeć też z perspektywy przestępców. Hakerzy zauważają, że wielu przedsiębiorców ma mgliste pojęcie o RODO, nie można zatem wykluczyć, że wykorzystają ich niewiedzę – będą szukać uchybień związanych z niewłaściwym zarządzaniem danymi, aby je wykraść i szantażować właścicieli firm.

Mobilny front

Według obliczeń Ponemon Institute wyciek pojedynczego rekordu z firmowych danych wiąże się ze stratą 141 dol. To kwota, wobec której trudno przejść obojętnie. Tymczasem hakerzy uderzają z coraz to nowych stron. Obecnie jednym z największych wyzwań staje się ochrona smartfonów. Choć jeszcze trzy lata temu amerykańska firma Damballa, monitorująca połowę ruchu mobilnego w Stanach Zjednoczonych, wykazała, że jedynie 10 tys. telefonów z ogólnej liczby 151 mln tych urządzeń wykazało oznaki infekcji malware'em. Mając takie dane, specjaliści szybko porównali ewentualność zarażenia smartfonu złośliwym oprogramowaniem z prawdopodobieństwem uderzenia pioruna. Okazało się, że druga opcja jest... bardziej prawdopodobna.

Jednak ubiegłoroczne analizy Gartnera pokazują, że żarty się skończyły, a użytkownicy smartfonów muszą stawić czoła zmasowanej ofensywie hakerów. Analitycy przewidują, że w ciągu najbliższych dwóch lat ilość malware'u atakującego te urządzenia wzrośnie o 440 proc. O ile w 2017 r. złośliwe aplikacje opracowane z myślą o smartfonach stanowiły zaledwie 7,5 proc. wszystkich wirusów, o tyle w 2019 r. będzie ich ponad 30 proc. Według dostawców systemów bezpieczeństwa rynek rozwiązań do ochrony sprzętu mobilnego jest najbardziej perspektywicznym obszarem, o dużym potencjale wzrostu.

– *Rodzimi administratorzy mają większą kontrolę nad danymi przechowywanymi na firmowych komputerach niż na smartfonach. W Polsce BYOD polega przede wszystkim na wykorzystywaniu prywatnych terminali do obsługi poczty firmowej. Z kolei Twitter, Facebook i programy pocztowe stały się aplikacjami zawodowymi. Skala kontaktów powoduje, że ich użytkownicy mogą przenosić złośliwy malware lub bezwiednie dostarczać hakerom informacje o topologii systemu IT* – mówi Mariusz Kochański, wiceprezes Veracompu.

Z upływem czasu firmy i instytucje zaczną dostrzegać narastające zagrożenia. Na listy klientów zaopatrujących się w systemy chroniące flotę mobilnych terminali trafią nie tylko przedsiębiorstwa przemysłowe i banki, ale również organizacje rządowe, placówki opieki zdrowotnej i służby mundurowe. Według prognoz MarketsandMarkets globalny rynek oprogramowania antymalware przeznaczonego dla mobilnych terminali na koniec 2020 r. osiągnie wartość 5,7 mld dol., czyli ponad dwa razy większą niż w 2015 r. Rodzimi resellerzy dostrzegają wzrost zainteresowania aplikacjami ochronnymi do smartfonów.

– *W grupie rozwiązań do ochrony danych najszybciej rośnie sprzedaż produktów przeznaczonych dla użytkowników telefonów komórkowych oraz tabletów. Właściciele terminali z Androidem bardzo często decydują się na zakup antywirusów, ze względu na liczbę zagrożeń. Inni klienci chętnie wdrażają systemy MDM umożliwiające centralnie zarządzanie mobilnym sprzętem* – wyjaśnia Karol Labe, właściciel Miecz Net.

(Nie)nasycony rynek

Rynek klasycznych rozwiązań zabezpieczających przed złośliwym oprogramowaniem wydaje się być nasycony. Teoretycznie każdy użytkownik biznesowy powinien mieć pakiet ochronny na komputerze. Jednak rzeczywistość nie wygląda aż tak różowo, czego dowodzą chociażby wyniki badania niedawno przeprowadzonego przez UKE wśród małych polskich przedsiębiorstw. Prawie 9 proc. respondentów nie zatrudnia osoby odpowiedzialnej za bezpieczeństwo, a 60 proc. pracowników nie ma pojęcia, jak sprawdzić, czy połączenie z Internetem jest bezpieczne. Natomiast 70 proc. firm przyznało, że korzysta z antywirusów oraz aplikacji antyspyware. Przytoczone dane pokazują, że w tym segmencie rynku wciąż tkwią rezerwy. Poza tym oprócz przedsiębiorców niefrasobliwie podchodzących do ochrony cyfrowych zasobów, istnieją też tacy, którzy poszukują nowych, bardziej skutecznych aplikacji zabezpieczających.

– *Tradycyjne podejście do ochrony danych na stacjach roboczych nie zawsze się sprawdza. Dlatego pojawia się miejsce dla rozwiązań nowej generacji, które coraz lepiej chronią przed takimi zagrożeniami jak ransomware* – twierdzi Marek Krauze, Sales Engineer w Trend Micro. >

Zdaniem integratora

Przemysław Sobczyk, IT Manager, Perceptus

Popyt na oprogramowanie antywirusowe nieustannie się zwiększa. Jednym z najważniejszych czynników jest wzrost liczby urządzeń. Niemal każdy posiadacz chroni swój komputer, do tego dochodzą jeszcze smartfony i tablety. Sprzedaż napędza także RODO, które znacznie zwiększa wymagania w zakresie bezpieczeństwa, podobnie jak ataki typu ransomware. Mimo że skuteczność programów antywirusowych jest bardzo duża, musimy pamiętać o tym, że nie zapewniają stuprocentowego bezpieczeństwa, ponieważ stanowią tylko jeden z elementów cyfrowej ochrony.

Wojciech Kotkiewicz, menedżer technicznego wsparcia sprzedaży, ABC Data

Paweł Jurek, wicedyrektor ds. rozwoju, Dagma Bezpieczeństwo IT

Wolfgang May, Channel Manager na region Europy Środkowej i Wschodniej, Barracuda Networks

W opinii branży

WOJCIECH KOTKIEWICZ Porównanie liczby stacji roboczych i serwerów w typowej firmie zdecydowanie wypada na korzyść tych pierwszych. Zatem popyt na aplikacje typu antymalware, przeznaczone do ochrony komputerów PC, jest zdecydowanie większy. Nie możemy jednak zapominać o farmach serwerów, gdzie wirtualizacja mocno się zakorzeniła, a każdy fizyczny serwer może udostępniać zasoby setkom maszyn wirtualnych. Ochrona urządzeń mobilnych to temat związany z trendem BYOD. W zasadzie każdy ma urządzenie mobilne i niezależnie, czy jest ono prywatne czy służbowe, powinno być należycie chronione. Niestety, wydaje mi się, że ochrona sprzętu przenośnego jest lekceważona, zabezpieczane są przede wszystkim stacje robocze i serwery.

PAWEŁ JUREK W segmencie aplikacji ochronnych największą zmianę zauważamy w grupie rozwiązań przeznaczonych do urządzeń mobilnych. Stacje robocze i serwery są od lat solidnie zabezpieczone rozwiązaniami antywirusowymi. Do niedawna urządzenia mobilne traktowano w firmach po macoszemu. To zmieniło się już w ubiegłym roku i widzimy coraz większe zainteresowanie należytym zabezpieczeniem tego typu sprzętu. Symptomem tej zmiany jest znacznie większe zainteresowanie aplikacjami typu MDM.

WOLFGANG MAY Rozwiązania ochronne szybko ewoluują, aby sprostać wyzwaniom związanym z nowymi zagrożeniami i wektorami ataku. Obecnie największymi problemami dla firm są złożoność i nieustanna ewolucja sposobów ataku. Z jednej strony obserwujemy szybki rozwój przedsiębiorstw, z drugiej wzrost liczby naruszeń bezpieczeństwa i zwiększenie zapotrzebowania na rozwiązania ochronne, również te wykorzystujące chmurę obliczeniową. Rosnąca popularność zaawansowanych ataków dnia zerowego i ransomware, które mają na celu ominięcie tradycyjnych mechanizmów obronnych wykorzystujących sygnatury, wymagają zaawansowanych, wielowarstwowych rozwiązań zabezpieczających.

Pewne zmiany widać też w segmencie aplikacji przeznaczonych do ochrony serwerów. Rozrastająca się w serwerowniach liczba wirtualnych maszyn wymaga zastosowania specjalnych środków. Tym należy tłumaczyć rosnący popyt na pakiety antywirusowe oferujące bezagentową obsługę tych systemów. Innym problemem spędzającym administratorom sen z oczu są ataki dnia zerowego. Dlatego m.in. firmy wykazują zainteresowanie tzw. wirtualną poprawką (virtualpatch). To mechanizm umieszczany w warstwie zabezpieczeń, wykrywający i blokujący złośliwy kod.

– *Przedsiębiorcy dostrzegają, że bardzo istotną kwestią jest zabezpieczanie wszelkiego rodzaju serwerów, bowiem na nich znajdują się najcenniejsze dane. Popyt na narzędzia do ich ochrony będzie się zwiększał bardzo dynamicznie* – przewiduje Marek Krauze.

Jednak niewykluczone, że dalekosiężne plany producentów aplikacji zabezpieczających zburzy rewolucyjna koncepcja Cisco. Koncern z San Jose od pewnego czasu lansuje sieć intuicyjną, która zdaniem producenta przewiduje działanie złośliwego kodu, zatrzymuje zagrożenia i sama się uczy.

– *Chronimy klientów w tzw. rozszerzonej sieci – w centrach danych, środowiskach wirtualnych, chmurze, urządzeniach mobilnych i punktach końcowych. Uważamy, że takie kompleksowe podejście do bezpieczeństwa jest obecnie najskuteczniejsze i zaczynają to dostrzegać również klienci* – przekonuje Łukasz Bromirski, dyrektor ds. technologii w polskim oddziale Cisco. Czy zatem już wkrótce zniknie podział na aplikacje chroniące smartfony, desktopy i serwery? Rodzimi resellerzy nie wierzą w taki rozwój wypadków.

– *Coraz częściej słyszymy o rozwiązaniach antywirusowych typu „next generation", ale klienci najbardziej ufają klasycznym systemom* – twierdzi Karol Labe.

Konsolidacja rynku

Według badań przeprowadzonych przez Cisco niektóre firmy korzystają z systemów bezpieczeństwa pochodzących od 50 dostawców. Taki stan rzeczy nie ułatwia pracy administratorom sieci, a w pewnych sytuacjach wręcz naraża przedsiębiorstwo na cyberataki.

– *Nazywamy ten paradoks luką w efektywności ochrony. Każdy nowy punkt, który dodaje firma, tylko w niewielkim stopniu poprawia skuteczność systemu, a jednocześnie zwiększa jego złożoność. Przedsiębiorstwa wcale nie stają się bardziej bezpieczne dzięki wdrożeniu dziesiątek rozwiązań od różnych dostawców, gdyż narzędzia zabezpieczające działają niezależnie i nie zapewniają efektu skali* – mówi Łukasz Bromirski.

Jednak nie wszystkim podoba się tego typu koncepcja. Zwolennicy wolnego rynku uważają, że klienci powinni mieć do wyboru różne opcje: zakup zintegrowanego rozwiązania bądź kompletowanie systemu ochrony składającego się z wielu elementów, niekoniecznie pochodzących od jednego dostawcy. Dyktat kilku silnych koncernów mógłby być

G DATA
MADE IN GERMANY

Szukasz doskonałej ochrony serwerów i stacji roboczych?

Wykorzystując elastyczny sposób licencjonowania, dobierasz ochronę do swoich potrzeb.
W ramach licencji oprogramowania G DATA Business planujesz ochronę serwerów i stacji roboczych, dbając tylko o odpowiednie wykorzystanie zakupionej ilości licencji. Serwer zarządzający? To nie problem! - instalujesz dowolną ilość w sieci.
Modułowa budowa oprogramowania, pozwala na dopasowanie oferty ochrony dla każdego.
Sprawdź nas.

Łukasz Nowatkowski
IT / Marketing Director

	Antivirus Business	Client Security Business	Endpoint Protection Business
Ochrona przed malware, spamem i phishingiem			
AntiRansomware	•	•	•
Ochrona antywirusowa	•	•	•
Ochrona w czasie rzeczywistym	•	•	•
Ochrona HTTP	•	•	•
BankGuard	•	•	•
Exploit Protection	•	•	•
USB Keyboard Guard	•	•	•
Antispam	o	•	•
Linux Web Security Gateway	o	o	o
Linux Mail Security Gateway	o	o	o
Exchange Mail Security	o	o	o
Mobile Device Management			
Ochrona w czasie rzeczywistym	•	•	•
Antitheft	•	•	•
Filtr aplikacji	•	•	•
Ochrona kontaktów	•	•	•
System & Network Management			
Firewall	–	•	•
Report Manager	•	•	•
Katalog sprzętu i oprogramowania	•	•	•
Network Monitoring	o	o	o
Polityka bezpieczeństwa w firmie			
Kontrola urządzeń	–	–	•
Kontrola aplikacji	–	–	•
Kontrola treści WEB	–	–	•
PatchManagement	o	o	o

o moduł opcjonalny

Moje pliki, mój biznes.

www.gdata.pl
www.gdata.pl/go/livewiew

być niekorzystny zarówno dla klientów, jak i dla resellerów. Natomiast wyraźnie widać, że producenci coraz częściej starają się dostarczać nabywcom rozwiązania gwarantujące pełną funkcjonalność w zakresie ochrony.

– *W wersji utopijnej najlepszym rozwiązaniem byłoby posiadanie wszystkich rozwiązań od jednego dostawcy. Uwzględniając procesy integracji i zarządzania, to model prawie idealny, oczywiście pomijając kwestie monopolu i wynikających z tego wad. My preferujemy koncepcję ochrony wielowarstwowej, w której ważna jest ochrona nie tylko punktów końcowych i urządzeń mobilnych, ale także serwerów poczty, plików i proxy* – tłumaczy Robert Dziemianko, Marketing Manager w polskim oddziale G Data Software.

Konsolidacja na rynku bezpieczeństwa jest nieunikniona, ale chyba tylko nieliczni wierzą, że w grze pozostanie zaledwie kilku najważniejszych dostawców. Bardziej realnym scenariuszem jest zacieśnianie współpracy między producentami. Dyskusje na ten temat toczą się od dawna. W kwietniu firmy uczyniły ważny krok w kierunku zjednoczenia sił. Grupa 34 koncernów z branży IT podpisała porozumienie Cybersecurity Tech Accord, które ma na celu koordynację działań w zakresie wykrywania podatności na ataki oraz opracowywania rozwiązań ochronnych. Na razie trudno wyrokować, czy projekt przyniesie sukces. Wygląda natomiast na to, że producenci z branży zabezpieczeń zdają sobie sprawę, że w pojedynkę nie wygrają wojny z cyberprzestępcami. Jednak sam fakt, że koncerny łączą siły, nie gwarantuje sukcesu.

– *Nawet nowoczesne procesory ARM i Intel, choć wyposażone w zaawansowane mechanizmy ochrony pamięci, rejestrów, okazują się podatne na ataki Meltdown i Spectre, i to mimo kupienia przez Intela firmy McAfee. A ta transakcja miała przecież zapewnić transfer know how w zakresie bezpieczeństwa* – mówi Mariusz Kochański.

Łowienie naiwniaków

Walka producentów rozwiązań ochronnych z hakerami przypomina wyścig zbrojeń. Czasami jedni i drudzy wyciągają z arsenału nową ciężką broń, ale nie rezygnują też ze starych, sprawdzonych metod. Ulubioną bronią cyberprzestępców są sztuczki socjotechniczne, mające na celu wydobycie od pracowników poufnych informacji. W jaki sposób z nimi walczyć? Dostawcy aplikacji zabezpieczających nie są w tym przypadku jednomyślni. Cisco stawia na analitykę behawioralną, umożliwiającą opracowanie polityki bezpieczeństwa uwzględniającej niepożądane działania użytkowników.

Rynek rozwiązań do zabezpieczania sprzętu mobilnego jest najbardziej perspektywicznym obszarem, o dużym potencjale wzrostu.

– *Aż 92 proc. uczestników naszego ostatniego badania docenia wartość tego typu rozwiązań* – przyznaje Łukasz Bromirski.

Zwolennikiem tego typu rozwiązań jest też Trend Micro. Producent podkreśla, że najnowsze zdobycze technologiczne, takie jak uczenie maszynowe i sztuczna inteligencja, znacznie ułatwiają wykrywanie cyberataków bazujących na socjotechnice. Ale nie wszyscy ufają cudownej mocy sztucznej inteligencji. Kluczem do zatrzymania phishingu i innych podobnych ataków jest ciągła edukacja personelu, gdyż nawet najbardziej dopracowany software nie uchroni naiwnych użytkowników przed kliknięciem w fałszywy link.

– *Należycie przeszkolony pracownik to 90 proc. sukcesu. Jeżeli normą są obowiązkowe szkolenia BHP czy przeciwpożarowe, podobne wytyczne trzeba zastosować w kwestii cyberbezpieczeństwa. Ważne jest też zachowanie równowagi między bezpieczeństwem a wygodną pracą. Dlatego lepiej uczyć personel, niż wprowadzać restrykcje* – tłumaczy Magdalena Baraniewska, Country Channel Manager w F-Secure.

Znalezienie złotego środka jest niezwykle trudne, o czym świadczą m.in. wyniki badań przeprowadzonych przez firmę Positive Technologies wśród amerykańskich i brytyjskich przedsiębiorstw. Na ataki typu phishing dało się nabrać 9 proc. pracowników działów informatycznych oraz 3 proc. specjalistów ds. bezpieczeństwa.

Jak się odnaleźć?

Rynek aplikacji ochronnych cechuje pewien dualizm. Z jednej strony rozwój zagrożeń, a także niedobór fachowców pozwala sądzić, że to prawdziwe eldorado dla resellerów oraz integratorów. Z drugiej strony pojawiają się problemy związane ze zbyt skromnymi budżetami IT oraz niskim poziomem wiedzy na temat cyberzagrożeń. Według Cisco połowa polskich przedsiębiorców wskazuje ograniczenia budżetowe jako największą przeszkodę we wdrażaniu rozwiązań ochronnych. Większość firm nie potrafi oszacować skuteczności i kosztów działań w zakresie bezpieczeństwa informacji. Co gorsza, tego typu inwestycje traktuje się z reguły jak dodatkowy koszt, a nie jak sposób na minimalizację ryzyka utraty danych lub paraliżu infrastruktury.

Wiele rozbieżności budzą też kwestie podziału środków. Z badań przeprowadzonych przez Centrify oraz Dow Jones Customer Intelligence wynika, że 62 proc. dyrektorów generalnych uważa złośliwe oprogramowanie za największe zagrożenie, a ich opinię podziela zaledwie 35 proc. pracowników działów IT.

– *Współpraca w niezwykle ważnym dla klienta zakresie cyberochrony może pomóc nawiązać bliższe relacje i otworzyć nowe perspektywy biznesowe w postaci zamówienia kolejnych usług i produktów IT* – podsumowuje Magdalena Baraniewska.

Jak widać, poruszanie się w świecie cyberbezpieczeństwa przypomina stąpanie po cienkim lodzie. Integratorzy poważnie myślący o tym segmencie rynku muszą stawiać na podnoszenie kwalifikacji i zatrudnianie fachowców, bowiem prędzej czy później otrzymają swoją szansę.

ESET – więcej niż antywirus

Dla dużych przedsiębiorstw kluczowa jest wiedza o wszystkich potencjalnych wektorach ataku na firmową sieć. Dlatego w ich interesie leży uzyskiwanie informacji z różnych źródeł. Jednym z nich może być usługa ESET Threat Intelligence.

Grzegorz Klocek
Product Manager ESET w Polsce, Dagma Bezpieczeństwo IT

Resellerzy obsługujący dużych klientów powinni zainteresować się ofertą firmy ESET, która już wkrótce ulegnie poważnym zmianom. Pojawią się w niej nowe narzędzia i usługi opracowane z myślą o najgroźniejszych i najtrudniejszych do wykrycia atakach. Najważniejszym jej elementem będzie autorskie rozwiązanie klasy Endpoint Detection & Response, które da klientom wgląd we wszystkie procesy przebiegające w firmowej sieci i umożliwi szczegółową kontrolę wszystkiego, co jest uruchamiane na poszczególnych komputerach, nawet aplikacji, które nie zostały zaklasyfikowane jako niebezpieczne. Będzie to potężne narzędzie w rękach świadomego administratora, które zapewni kontrolę każdego pliku wykonywalnego. Oprogramowanie to będzie powiązane z nowymi usługami świadczonymi przez producenta, takimi jak indywidualna analiza zagrożeń APT atakujących przedsiębiorstwo, a także sandboxing w chmurze ESET, współpracujący z agentami na stacjach roboczych.

Ataki ukierunkowane, zagrożenia typu APT, exploity dnia zerowego oraz działanie botnetów są trudne do wykrycia przez administratorów posiadających dostęp do informacji jedynie z wnętrza firmowej sieci. Nie zawsze wystarczy też korzystanie wyłącznie z antywirusa. Dlatego z myślą o przedsiębiorstwach, których eksperci ds. bezpieczeństwa potrzebują dostępu do jednej z najbardziej wiarygodnych na świecie baz danych o zagrożeniach (np. z sektora bankowego, energetycznego, wojskowego), ESET stworzył usługę Threat Intelligence.

Wykorzystuje ona informacje pozyskiwane przez ponad 100 mln stacji roboczych z oprogramowaniem antywirusowym ESET, które wysyłają uzyskane dane do chmurowego systemu reputacyjnego ESET Live Grid. Po wstępnej agregacji są one przesyłane do centrów R&D, rozrzuconych po całym świecie, w których eksperci dokonują dogłębnej analizy informacji (jeden z takich ośrodków znajduje się w Krakowie; wykrywa się tam i analizuje zagrożenia oraz rozwija produkty producenta). Dzięki temu ESET Threat Intelligence zapewnia klientom unikalną wiedzę, która pomaga oszacować ryzyko ataku na infrastrukturę firmową i zminimalizować je, a jednocześnie poprawić skuteczność działania własnych zabezpieczeń.

Na skuteczność usługi ESET Threat Intelligence szczególny wpływ ma wykorzystanie chmurowego systemu reputacji plików ESET Live Grid. Każde oprogramowanie antywirusowe firmy ESET podczas sprawdzania pliku lub adresu URL najpierw weryfikuje ich obecność w lokalnej bazie zagrożeń i na białej liście, co poprawia wydajność skanowania. W przypadku braku informacji zwrotnej wysyła zapytanie do systemu ESET Live Grid. W ten sposób trafiają do niego potencjalnie niebezpieczne pliki i aplikacje, których zawartość jest automatycznie weryfikowana, m.in. w procesach sandboxingu i analizy behawioralnej.

Cała wiedza w raportach

W ramach ESET Threat Intelligence dla każdego klienta opracowywany jest indywidualny, szczegółowy raport, który dotyczy potencjalnie planowanych lub właśnie trwających ataków skierowanych przeciwko jego firmie. Reguły wyszukiwania zagrożeń mogą być określone z wykorzystaniem języka YARA. Raport zawiera istotne informacje o częstotliwości ataków, adresach URL zawierających złośliwy kod, miejscach, w których został wykryty, danych dotyczących zaobserwowanej jego aktywności itp.

Klienci zyskują też dostęp do regularnie opracowywanych raportów zawierających dane ilościowe o zidentyfikowanych rodzinach złośliwego oprogramowania i zagrożeniach, których celem jest przyłączenie kolejnych urządzeń do sieci botnet. W raportach znajduje się także lista znanych serwerów C&C zarządzających botnetami oraz spis celów danego ataku.

Eksperci zalecają łączenie różnych metod ochronnych w celu zminimalizowania ryzyka infekcji lub ataku. Dlatego usługa ESET Threat Intelligence nie wymaga, aby w firmowej sieci klienta były wdrożone rozwiązania ESET. Dzięki temu może ona działać jako dodatkowa warstwa zabezpieczeń, spełniająca rolę systemu wczesnego ostrzegania przed nadciągającymi atakami, o których dostawca rozwiązań ochronnych wykorzystywanych w danym przedsiębiorstwie może nie widzieć. Usługa może też być wykorzystywana do uzyskiwania dodatkowych informacji na temat konkretnego ataku, który został już wykryty w firmowej sieci, by ułatwić podjęcie odpowiedniej decyzji dotyczącej ochrony.

Wyłącznym dystrybutorem ESET w Polsce jest firma Dagma Bezpieczeństwo IT.

Dodatkowe informacje: Grzegorz Klocek, Product Manager ESET w Polsce, Dagma Bezpieczeństwo IT, klocek.g@dagma.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI ESET I DAGMA BEZPIECZEŃSTWO IT.

Ilustracja AdobeStock

Cel: *wysoka dostępność*

Strategia ochrony środowisk wirtualnych w dużym stopniu powinna różnić się od zabezpieczania klasycznych serwerów, desktopów i sieci. Awaria fizycznego serwera uniemożliwi korzystanie z usług we wszystkich hostowanych wirtualnych maszynach, dlatego działania minimalizujące ryzyko takiego zdarzenia należy prowadzić na kilku poziomach.

Krzysztof Jakubik

Według inżynierów i analityków zajmujących się zwalczaniem złośliwego kodu w drugiej połowie ubiegłej dekady najlepszym oprogramowaniem antywirusowym były... wirtualne maszyny. Cyberprzestępcy wiedzieli, że to je najczęściej wykorzystywano do analizy zachowania internetowych robaków, więc wbudowywali w wirusa mechanizm dezaktywujący jego działanie, gdy ten wykrył, że jest uruchomiony w wirtualnej maszynie (co utrudniało obserwację efektów jego działania). Dzisiaj sytuacja znacznie się zmieniła, gdyż do analizy złośliwego kodu wykorzystuje się zautomatyzowane rozwiązania, a coraz częściej także uczenie maszynowe. Nikt już nie analizuje próbek, jak dziesięć lat temu, bo po prostu powstaje ich zbyt dużo. Jednocześnie w wirtualnych maszynach przetwarzane są cenne dane i cyberprzestępcy nie odpuszczają już sobie tak łakomych kąsków. Dlatego ochrona wirtualnych środowisk jest nie tylko wskazana, ale wręcz konieczna.

Ich zabezpieczanie to jednak skomplikowany proces. Narzędzia ochronne, za pomocą których należy egzekwować takie same reguły polityki bezpieczeństwa, jakie obowiązują w całym przedsiębiorstwie, są inne niż w przypadku środowiska fizycznego. Administratorzy lub współpracujący z firmą partnerzy muszą być też gotowi, by o ochronę środowiska wirtualnego dbać z podobną starannością jak o bezpieczeństwo pozostałej części infrastruktury IT.

– *Nadrzędnym celem powinno być zapewnienie wysokiej dostępności infrastruktury IT w przedsiębiorstwie* – podkreśla Marcin Zmaczyński, dyrektor polskiego oddziału Aruba Cloud. – *Jedynie wtedy zarząd może być pewny, że biznes nie jest zagrożony. Należy do tego wykorzystać nie tylko wszystkie dostępne środki technicz-*

ne (oprogramowanie antywirusowe, narzędzia do kontroli informacji przesyłanych w sieci itp.), ale też organizacyjne, m.in. systematyczne wykonywanie kopii backupowych i przechowywanie ich w firmie oraz w innym, odległym miejscu (w ramach planu disaster recovery).

Wirtualny antywirus

W środowisku wirtualnym stosowanie antywirusów jest konieczne. Problem jednak stanowi fakt, że dobór oprogramowania ochronnego dla wirtualnych maszyn jest zdecydowanie trudniejszy niż w przypadku zwykłych desktopów, kiedy bierze się pod uwagę tylko dwa parametry – cenę i skuteczność. Przede wszystkim należy sprawdzić, czy wybrany dostawca ma rozwiązanie do wykorzystywanego przez klienta systemu (Citrix, Microsoft, VMware, projekty KVM). W środowisku wirtualnym ma też znaczenie, jaki rodzaj danych jest przetwarzany w poszczególnych maszynach (czy służą jako serwer baz danych, plików, hostingu stron internetowych lub poczty, wirtualny desktop). Dlatego stosowane są trzy sposoby ochrony infrastruktury wirtualnej: bezagentowy (agentless), z lekkim agentem (light agent) i pełnym agentem (full agent).

Metoda bezagentowa wymaga uruchomionej osobnej maszyny wirtualnej z zainstalowanym silnikiem antywirusowym (Security Virtual Appliance). W ten sposób odbywa się skanowanie w celu wykrycia złośliwego oprogramowania w pozostałej części wirtualnej infrastruktury. Rozwiązanie to ma jednak pewną wadę: wszyscy dostawcy hypervisorów (z wyjątkiem projektów KVM) zapewniają skanowanie „z zewnątrz", ale w dość ograniczonym zakresie (najbardziej otwarty jest VMware z usługą vShield). Nie ma zatem możliwości zastosowania bardziej zaawansowanych metod ochrony, takich jak kontrola działania aplikacji, analiza heurystyczna, tworzenie białych list, prowadzenie kwarantanny itp.

Funkcjonalność zbliżoną do oferowanej przez zwykłe antywirusy zapewnia rozwiązanie wykorzystujące pełnego agenta zainstalowanego w każdej wirtualnej maszynie (takiego samego jak stosowany do ochrony urządzeń końcowych), lecz i ono ma wady. Po pierwsze negatywnie wpływa na wydajność każdej maszyny wirtualnej, podobnie jak klasyczne antywirusy instalowane na zwykłych pecetach. Po drugie trudno zarządzać takim oprogramowaniem z powodu szybko (często w niekontrolowany sposób) rozrastającej się infrastruktury wirtualnej. Konieczność zapanowania nad licencjami oraz weryfikacją poprawności pracy antywirusa, kontrolowania aktualizacji agentów i baz sygnatur powoduje, że nierzadko do obsługi tego środowiska potrzebny jest dodatkowy pracownik.

Wartym uwagi kompromisem jest wykorzystanie tzw. lekkich agentów łączących się z centralnym modułem zawierającym silnik antywirusowy w oddzielnej wirtualnej maszynie, ale wykonujących również wiele zadań, których nie zrealizuje się w modelu bezagentowym. W przypadku lekkich agentów zdecydowanie mniejszy jest negatywny wpływ na wydajność wirtualnych maszyn. Aktualizacja oprogramowania antywirusowego ma miejsce tylko raz (w silniku), więc paczki z nowymi sygnaturami nie muszą być instalowane w każdej instancji agenta. W ten sposób nie dochodzi do przeciążenia fizycznego serwera, a to pozwala unikać niedostępności usług świadczonych za pomocą wirtualnych maszyn.

Dynamika zmian w środowiskach wirtualnych jest dużo większa niż w fizycznych.

Wirtualne sieci też potrzebują ochrony

Całe firmowe środowisko sieciowe, włącznie z jego wirtualną odnogą, jest równie ważną dziedziną do ochrony jak zawartość maszyn wirtualnych. Cyberprzestępcy wykorzystujący ransomware nie będą bowiem wybierać – jeśli znajdą lukę (nieważne czy w fizycznej, czy w wirtualnej sieci), z pewnością ją wykorzystają. A po uzyskaniu dostępu do wirtualnej infrastruktury mogą dość prosto wyłączyć lub usunąć maszyny oraz zakłócić pracę hypervisora lub fizycznego serwera, na którym się on znajduje.

Niestety, produkowane urządzenia ochronne nie mogą zabezpieczać wirtualnej infrastruktury, ponieważ nie zostały zaprojektowane w tym celu i „nie rozumieją" tego, co się wewnątrz niej dzieje. W ten sposób w środowisku klientów powstaje luka, którą powinno się czym prędzej wypełnić, gwarantując ochronę nie tylko na brzegu sieci, ale także w jej wnętrzu.

Środowisko wirtualne charakteryzuje się kilkoma unikalnymi cechami, które nie występują w infrastrukturze składającej się wyłącznie z fizycznych serwerów. Generowanie i uruchamianie na przykład nowych wirtualnych serwerów trwa minuty, a nie jak wcześniej dni lub tygodnie. Można zatem wyobrazić sobie, że cyberprzestępcy wymuszają stworzenie dodatkowej wirtualnej maszyny i osadzają tam złośliwy kod wykradający firmowe informacje. W dużych chmurowych środowiskach bez ochrony sieciowej administratorzy przez długi czas nie wykryją działań hakerów. Pomocne może okazać się wyłącznie oprogramowanie analizujące w czasie rzeczywistym dane >

Zdaniem integratora

Radosław Kluczny, dyrektor handlowy, Alterkom

Przed wdrożeniem rozwiązania do ochrony środowiska wirtualnego warto skontaktować się z jego producentem, który najlepiej zna specyfikę produktu i wskaże ewentualne kryteria doboru, szczególnie jeśli oczekiwania klientów integratora są nietypowe. Każdy producent stosuje własne rozwiązania u siebie i, siłą rzeczy, także musiał je odpowiednio zabezpieczyć. Dlatego wie, jak zrobić to najskuteczniej. Kolejnym krokiem powinna być rozmowa z producentami rozwiązań ochronnych, ale tylko z takimi, którzy są certyfikowanymi partnerami technicznymi producenta, którego rozwiązanie jest wykorzystywane przez klienta.

Sebastian Kisiel, inżynier wsparcia sprzedaży, Citrix

Kornelia Szlósarczyk, Product Manager Nakivo, Konsorcjum FEN

Tomasz Krajewski, Regional Presales Manager, Eastern EMEA, Veeam

W opinii branży

SEBASTIAN KISIEL Producenci rozwiązań do budowy wirtualnej infrastruktury zapewniają szkolenia dla partnerów i klientów obejmujące kwestie związane z ochroną. Nie pojawia się jednak ona jako osobny temat ani przedmiot na kursie certyfikacyjnym. Wychodzimy z założenia, że dbać o bezpieczeństwo należy podczas wszystkich działań – związanych z projektowaniem środowiska wirtualnego, administrowaniem nim i optymalizacją jego pracy, tym bardziej że kwalifikacje trzeba nieustannie poszerzać, bo cyberprzestępcy ciągle zmieniają metody ataku.

KORNELIA SZLÓSARCZYK Wiedza klientów o możliwościach zapewniania wysokiej dostępności zasobów w środowiskach wirtualnych rośnie bardzo powoli. Nadal skupiają się wyłącznie na backupie wirtualnych maszyn i często nawet nie kontrolują poprawności procesu ani możliwości szybkiego odzyskania dostępu do danych. Dostrzegamy też, że nawet nasi partnerzy bywają niewystarczająco skuteczni w edukowaniu klientów. Poddają się, gdy klient nie chce słuchać o nowych funkcjach i żąda zrealizowania planu minimum. W tej sytuacji pomocna będzie oferowana już w oprogramowaniu do backupu maszyn wirtualnych funkcja automatycznej kontroli spójności wykonanej kopii i dostępności do danych chwilę po wystąpieniu awarii.

TOMASZ KRAJEWSKI Zachęcamy integratorów, aby budowali u siebie miniserwerownie, w których przechowywane będą zapasowe kopie danych ich klientów. To stosunkowo niedroga inwestycja, która bardzo się opłaci. Dzięki niej odbiorcy zyskują możliwość współpracy z podmiotem, który darzą dużym zaufaniem. Partnerzy pomogą też w całkowitym przejęciu odpowiedzialności za wykonywanie backupu i zdalne zarządzanie tym procesem, czyli Backup as a Service. W takim modelu świadczenia usługi klienta nie interesuje, w jaki sposób wykonywane są kopie, ważna dla niego jest umowa SLA, która określa gwarantowany czas przechowywania danych i ich odzyskania po awarii.

przesyłane przez wirtualną sieć i podejmujące decyzje na podstawie przyjętej w firmie polityki bezpieczeństwa.

Dostawcy klasycznych rozwiązań ochronnych w ostatnich latach znacznie rozszerzyli ofertę i wprowadzili do niej produkty albo ściśle współpracujące z wirtualną infrastrukturą, albo bezpośrednio w niej instalowane. Pojawiły się UTM-y, firewalle nowej generacji i systemy IDS/IPS w postaci wirtualnych appliance'ów. Producenci zapowiadają też coraz więcej rozwiązań bazujących na uczeniu maszynowym.

Warto, by integratorzy sprawdzili, czy producent fizycznych rozwiązań ochronnych, z których korzysta klient, oferuje wirtualne odpowiedniki. Ich wdrożenie ułatwiałoby konfigurację środowiska i wprowadzenie reguł polityki bezpieczeństwa.

Backup – jeszcze więcej wyzwań

Obok ochrony przed działaniami cyberprzestępców, które mogą spowodować niedostępność wirtualnego środowiska, należy stosować zabezpieczenia przed różnego typu zdarzeniami losowymi, awariami i błędami administratorów. Służą do tego dwie główne metody – backup oraz replikacja wirtualnych maszyn. Niestety, tutaj także wdrożenie sprawnie działających procedur stanowi wyzwanie.

Dynamika zmian w środowiskach wirtualnych jest dużo większa niż w fizycznych. Prostota tworzenia nowych maszyn powoduje, że bardzo łatwo w procesie zabezpieczania niektóre pominąć. Najczęściej nieobjęcie ich ochroną, także przed utratą danych, zdarza się, gdy prowadzone są testy aplikacji, a następnie wirtualny serwer przenoszony jest do środowiska produkcyjnego. Ryzyko wzrasta w bardzo rozbudowanych środowiskach wirtualnych, działających w trybie prywatnej chmury, w których poszczególne departamenty przedsiębiorstwa mają prawo powoływać do życia wirtualne maszyny bez akceptacji administratora. Dlatego, gdy brakuje procedur organizacyjnych, które obejmą ochroną wszystkie maszyny, bardzo łatwo o katastrofę.

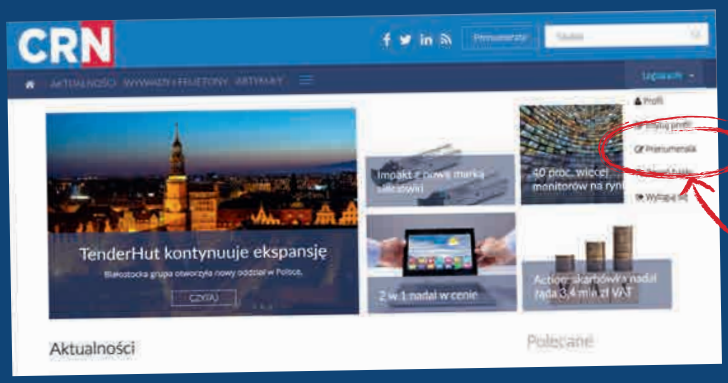
Dostawcy rozwiązań wirtualizacyjnych gwarantują ich wysoką dostępność dzięki implementacji interfejsu API. Pozwala on twórcom oprogramowania do backupu i odzyskiwania danych „zaglądać" do wnętrza maszyn wirtualnych i znacznie poszerzać możliwości ochrony. W ten sposób zapewniono m.in. tworzenie kopii migawkowych aktywnych wirtualnych maszyn, w których uruchomione są aplikacje. Wykonanie zwykłej kopii takiej maszyny nie zdawało egzaminu. Jej zawartość zmieniała się w wyniku pracy aplikacji, stworzone kopie były wewnętrznie niespójne i nie udawało się ich odzyskać w przypadku awarii. Dopiero wniknięcie do wnętrza wirtualnej maszyny pozwalało na chwilę zamrozić aplikację, aby wykonać kopię danych.

– *Narzędzie do wykonywania kopii bezpieczeństwa maszyn wirtualnych powinno zapewniać także bardzo szybkie ich odtwarzanie* – mówi Grzegorz Bielawski,

ZAPISZ SIĘ NA
BEZPŁATNY NEWSLETTER CRN POLSKA

OTRZYMASZ 3 RAZY W TYGODNIU:

- najświeższe informacje o trendach w kanale sprzedaży rozwiązań IT w Polsce i na świecie
- zapowiedzi najważniejszych konferencji i wydarzeń dla resellerów i integratorów IT
- wiedzę dotyczącą biznesu, wspomagającą rozwój Twojej firmy



Jak to zrobić?

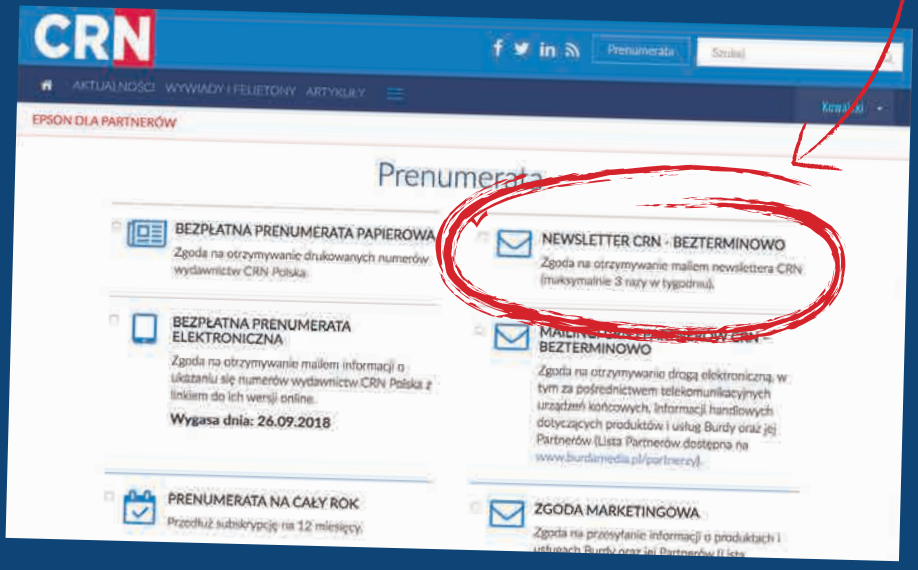
To proste. Mając konto* na CRN.PL:

1. **zaloguj się**
2. **kliknij Prenumerata**
3. **kliknij ikonę NEWSLETTER CRN**
4. **i zapisz wprowadzone zmiany**

JEŚLI NIE PAMIĘTASZ HASŁA DO SWOJEGO KONTA...

- możesz je odzyskać na stronie: https://www.crn.pl/resetting/request
- możesz wysłać mail na adres prenumerata@crn.pl z prośbą o włączenie newslettera

Z otrzymywania newslettera można w każdej chwili zrezygnować, edytując profil swojego konta na CRN.pl lub wysyłając mail na adres prenumerata@crn.pl



* Jeśli jeszcze nie masz konta na CRN.pl, możesz je założyć na stronie: ww.crn.pl/login

NAJLEPIEJ POINFORMOWANE PISMO W BRANŻY IT!

szef polskiego oddziału firmy QNAP. – *Dziś żaden administrator nie zgodzi się czekać na odtworzenie maszyny wirtualnej dziesięć lub więcej godzin, bo w znacznie krótszym czasie stworzy ją od nowa.*

Kryterium wyboru oprogramowania do backupu środowisk wirtualnych i zapewniania ich wysokiej dostępności powinien być przede wszystkim certyfikat przyznany producentowi przez dostawcę hypervisora. To gwarantuje poprawność wykonania kopii, spójności zawartych w niej danych i możliwość ich odtworzenia po awarii. Oczywiście chronić trzeba nie tylko wirtualne maszyny, ale też obsługujące je hypervisory.

Wiele parametrów do rozważenia

Przy backupie wirtualnych maszyn bardzo ważna jest redukcja zajmowanego przez nie miejsca. Kompresja danych nie jest w tym przypadku efektywna, zdecydowanie lepiej sprawdza się deduplikacja. Jeżeli w wielu wirtualnych maszynach w danej firmie stosowane są te same wersje systemów operacyjnych, to powtarza się znaczna liczba bloków (wszystkie pliki systemowe). Zdarza się więc, że współczynnik deduplikacji sięga nawet 80–90 proc. w skali całego wirtualnego środowiska. Oczywiście deduplikacja ma wpływ na wydajność kopiowania, ale znacznie mniejszy niż kompresja.

Wchodzące właśnie w życie rozporządzenie RODO oraz inne obowiązujące regulacje prawne (a także przepisy wewnętrzne przedsiębiorstw) nakazują szyfrowanie kopii danych, szczególnie jeśli są wynoszone poza siedzibę firmy. W realizacji tego procesu są przydatne taśmy w standardzie LTO, które we wszystkich użytkowanych obecnie wersjach zapewniają szyfrowanie. Sprawdzają się w długoterminowym przechowywaniu kopii wirtualnych maszyn, zapewniają bowiem bardzo dużą pojemność i wciąż są najtańsze w obsłudze (dzięki niskiej cenie jednostki pojemności i niepobieraniu energii przez nieużywane taśmy).

Kolejną istotną kwestią jest zaplanowanie procedury przywrócenia środowiska do pracy w przypadku awarii. Należy regularnie sprawdzać poprawność wykonania kopii backupowej maszyn wirtualnych. Funkcję tę zapewnia coraz większa liczba aplikacji do backupu. Zaraz po wykonaniu kopii zakładają tymczasową wirtualną maszynę, do której próbują odzyskać dane i sprawdzić ich integralność. Konieczne jest również zapewnienie dostępu do pojedynczych plików w wirtualnej maszynie (tzw. odzyskanie granularne).

Warto pamiętać o obowiązku opracowania planu działania w przypadku katastrofy, takiej jak awaria serwera lub macierzy dyskowej przechowującej obrazy wirtualnych maszyn. Plan powinien zawierać wiele ustaleń organizacyjnych, m.in. podział obowiązków, informacje o sposobie zabezpieczania i odzyskiwania danych oraz kolejność odzyskiwania poszczególnych maszyn. Ułatwieniem jest fakt, że maszyny mogą być przywrócone do pracy na dowolnym serwerze z zainstalowanym hypervisorem. Niektórzy producenci oprogramowania zabezpieczającego zapewniają uruchomienie wirtualnej maszyny bezpośrednio z kopii zapasowej na serwerze backupu i równoczesne przywracanie jej do środowiska podstawowego.

Do backupu wirtualnych maszyn świetnie nadają się serwery plików NAS. Nie muszą mieć szczególnie dużej wydajności, a przy dzisiejszej monstrualnej pojemności dysków, przekraczającej 10 TB, nie ma też problemu z zapewnieniem miejsca na kopie. Warto tylko, żeby dostawca rozwiązania miał certyfikat od wykorzystywanego w firmie producenta środowiska wirtualizacyjnego, bo zagwarantuje to spójność zabezpieczanych danych. Niektórzy producenci serwerów NAS zapewniają także instalowane w nich oprogramowanie do backupu wybranych zasobów i przesyłania do chmury.

Sposoby zabezpieczania wirtualnych maszyn

Zadania	Opis i przykłady
Migracja maszyn wirtualnych	• Przenoszenie działających wirtualnych maszyn pomiędzy fizycznymi serwerami z wykorzystaniem takich narzędzi jak VMotion, XenMotion lub Live Migration. • Zapewnia możliwość równomiernego rozłożenia obciążenia na poszczególnych serwerach lub przeniesienia maszyn z jednego serwera na inne w celu przeprowadzenia na nim prac serwisowych.
Zapewnienie wysokiej dostępności	• Automatyczne przenoszenie działających wirtualnych maszyn między serwerami w przypadku nadmiernego obciążenia fizycznego hostującego je serwera. • Konieczne jest zapewnienie infrastruktury sieciowej o szerokim paśmie i małych opóźnieniach w celu zapewnienia szybkiej migracji oraz stosowanie macierzy RAID w celu wyeliminowania ryzyka utraty maszyn w wyniku awarii dysku.
Replikacja	• Wykonanie w sposób synchroniczny lub asynchroniczny kopii wirtualnej maszyny na zapasową macierz dyskową. • Relatywnie droga w realizacji, ponieważ wymaga inwestycji w dodatkowy sprzęt, który pełni funkcję wyłącznie polisy ubezpieczeniowej.
Kopie migawkowe (snapshots)	• Wykonywana regularnie kopia stanu wirtualnej maszyny w danym czasie. • Może być wykonywana na różnych poziomach (systemu operacyjnego gościa, hypervisora, macierzy dyskowej).
Backup i odzyskiwanie	• Kopia wirtualnej maszyny i/lub znajdujących się w niej danych, wykonywana w celu przywrócenia jej do pracy w momencie awarii podstawowego systemu, utraty wirtualnej maszyny lub naruszenia spójności znajdujących się w niej danych. • Może być wykonywana z wykorzystaniem agentów zainstalowanych w wirtualnej maszynie lub bezagentowo (na poziomie hypervisora). • Dane mogą być kopiowane na tę samą macierz dyskową, na której przechowywany jest oryginał, przez sieć pamięci masowych SAN (na inną macierz dyskową) lub sieć lokalną LAN (np. na serwer NAS).
Archiwizacja	• Kopia danych z wirtualnej maszyny w celu ich długoterminowego przechowywania na wewnętrzne potrzeby firmy lub w celu zapewnienia zgodności z prawem albo wewnętrznymi regulacjami. • Kopii mogą podlegać dane ustrukturyzowane (bazy danych), częściowo ustrukturyzowane (poczta elektroniczna) lub nieustrukturyzowane (pliki).

Wirtualne maszyny zawsze dostępne na serwerach **Synology**

Ochrona wirtualnych maszyn jest związana nie tylko z ich zabezpieczeniem przed uruchomieniem złośliwego kodu. Równie ważne są ich backup oraz replikacja.

Serwerom NAS firmy Synology producenci rozwiązań wirtualizacyjnych przyznali oficjalne certyfikaty stwierdzające, że można na nich udostępniać wirtualne maszyny z odpowiednio wysoką wydajnością i niezawodnością w takich środowiskach jak VMware vSphere, Microsoft Hyper-V, Citrix XenServer oraz OpenStack Cinder.

Szczególnie wart wspomnienia jest certyfikat przyznany przez firmę VMware, potwierdzający pełną kompatybilność z systemem vSphere 6.5 oraz rozwiązaniem VAAI. Dzięki wykorzystaniu mechanizmu Hardware Assisted Locking (ATS) tworzenie wielu wirtualnych maszyn na serwerze NAS może odbywać się nawet dziewięć razy szybciej niż bez dodatkowego wsparcia. Z kolei dzięki mechanizmowi Block Zeroing tworzenie maszyn wirtualnych z parametrem Write Same jest prawie 140 razy szybsze niż w przypadku jednostek LUN bez rozwiązania VAAI. Natomiast funkcja Full Copy sprawia, że kopiowanie maszyn wirtualnych do jednostki LUN z rozwiązaniem VAAI może być nawet 34 razy szybsze.

Natychmiastowa ochrona dzięki migawkom

W większości serwerów Synology można zapisywać pliki w formacie Btrfs, który zapewnia bardzo wydajne tworzenie migawkowych kopii danych (snapshot) oraz odzyskiwanie ich w wersji z określonego momentu w przeszłości za pomocą jedynie ułamka pamięci RAM i zasobów obliczeniowych serwera potrzebnych do wykonania tradycyjnych kopii zapasowych.

Ta metoda świetnie nadaje się do ochrony maszyn wirtualnych, ponieważ zapewnia spójność zawartych w nich danych. Ponadto współpraca serwerów Synology z oprogramowaniem VMware Site Recovery Manager upraszcza przywracanie środowiska do pracy dzięki możliwości uruchamiania funkcji Disaster Recovery bezpośrednio z serwera VMware vCenter Server. Strategię przechowywania danych można łatwo dostosowywać do potrzeb firmy w celu optymalizacji wykorzystania przestrzeni dyskowej serwera.

W serwerach NAS firmy Synology działa system operacyjny Disk Station Manager, który oprócz ochrony danych z wykorzystaniem migawek zapewnia ich replikację. Dostępne są również narzędzia dla administratorów umożliwiające skrócenie czasu potrzebnego na przełączanie na system zapasowy w przypadku awarii podstawowego oraz monitorowanie każdego zadania replikacji. Administratorzy mogą też okresowo przeprowadzać test przełączania awaryjnego, aby mieć pewność, że procedury odzyskiwania zadziałają prawidłowo. Dla każdego zadania replikacji generowany jest raport, który pomaga w ocenie i optymalizacji środowiska sieciowego.

Wydajne rozwiązanie HA

Niespodziewane przerwy w dostępie do maszyn wirtualnych bywają dla firm bardzo kosztowne. Dlatego w wybranych serwerach Synology znalazła się funkcja Synology High Availability (SHA), która zapewnia połączenie dwóch serwerów NAS w klaster wysokiej dostępności. W takiej konfiguracji jeden z nich pełni rolę serwera aktywnego, a drugi – pasywnego (w trybie gotowości). Aktywny serwer obsługuje wszystkie żądania dostępu do danych i usługi, a jednocześnie dane z niego są stale replikowane na serwer pasywny.

Magdalena O'Dwyer
Product Manager, Synology

Proces ochrony wirtualnych maszyn znacząco różni się od zabezpieczania zwykłych plików. Niedostępność wirtualnego środowiska lub znaczne spowolnienie jego pracy może bardzo negatywnie wpłynąć na ciągłość funkcjonowania przedsiębiorstwa. Dlatego konieczne jest zapewnienie nie tylko możliwości nieprzerwanego korzystania z obrazów wirtualnych maszyn, ale także zagwarantowanie odpowiednio wysokiej wydajności uruchomionych procesów.

Komunikacja między tymi serwerami odbywa się za pomocą połączenia Heartbeat. Gdy serwer aktywny stanie się niedostępny, automatycznie aktywowany jest serwer pasywny, co umożliwia odzyskanie dostępu do plików i aplikacji w ciągu kilku minut.

Kolejną ważną funkcją w serwerach NAS firmy Synology jest LUN Clone. Dzięki niej administrator jednym kliknięciem uruchamia proces tworzenia kopii wirtualnych jednostek LUN.

Dystrybutorami serwerów Synology w Polsce są firmy: AB, ABC Data, EPA Systemy i Veracomp.

Synology

Dodatkowe informacje:

Magdalena O'Dwyer, Product Manager, Synology, magdalenad@synology.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SYNOLOGY.

DRaaS – *zabezpiecz się zanim będzie za późno*

Istnieje wiele rodzajów zagrożeń, które mogą spowodować, że firma zostanie odcięta od zasobów IT, a przywracanie jej biznesowej sprawności może zająć dni, a nawet tygodnie. Panaceum na tego typu problemy są usługi Disaster Recovery as a Service.

Opublikowany w styczniu raport „KPMG Barometr Cyberbezpieczeństwa" zawiera prognozę, że w tym roku zwiększy się ilość złośliwego oprogramowania oraz liczba cyberataków, także tych całkowicie paraliżujących działanie firm i instytucji. Kolejnym zagrożeniem dla danych i infrastruktury informatycznej, równie kłopotliwym, będą awarie wywołane czynnikami naturalnymi, błędami ludzkimi lub przerwami w dostawie zasilania. Przyczyny te zmieniają sposób myślenia o ochronie danych, wymuszają zwiększenie nakładów na działy IT i odpowiednie zabezpieczanie środowisk.

Firmy zdają sobie sprawę ze skali czyhających na nie zagrożeń i dążą do zwiększenia bezpieczeństwa swojej infrastruktury IT. Z raportu „Thales Data Threat Report" wynika, że 73 proc. respondentów zajmujących się kwestiami ochrony zasobów w dużych firmach przewiduje wzrost wydatków na ochronę w ciągu najbliższych dwunastu miesięcy, co oznacza skok w porównaniu z wynikami badań w roku ubiegłym o 58 proc. Przedsiębiorcy podchodzą też coraz przychylniej do rozwiązań chmurowych, bo zapewniają one poważne oszczędności, a także redukcję i uproszczenie firmowej infrastruktury informatycznej. Stąd rosnące zainteresowanie rozwiązaniami Disaster Recovery as a Service, które w przeciwieństwie do Backup as a Service umożliwiają przywrócenie całej infrastruktury, łącznie z wszystkimi hostowanymi aplikacjami, systemami plików i bieżącymi konfiguracjami systemów.

Na usługę DRaaS składają się działania prowadzące do stworzenia i wdrożenia planu reakcji w momencie wystąpienia katastrofy (disaster recovery plan). W ramach tego rozwiązania usługodawcy oferują uruchomienie – na bazie własnej infrastruktury – zapasowego centrum danych, do którego replikowane są dane. Przewagą modelu DRaaS nad tworzeniem własnego systemu wysokiej dostępności jest m.in. fakt, że renomowani dostawcy usług dysponują certyfikowanym zespołem, który ma bogate doświadczenie w radzeniu sobie z typowymi oraz niestandardowymi sytuacjami kryzysowymi.

Co więcej, w odpowiedzi na indywidualne potrzeby klienta definiowene są procesy związane z backupem środowiska zapasowego na serwery w centrum danych dostawcy usługi. Następnie rozwiązanie to jest wdrażane, odpowiednio konfigurowane i regularnie testowane. Oznacza to, że plan działania w przypadku awarii jest nie tylko opracowany, ale także

wielokrotnie wypróbowany w praktyce. Przykładowo, w przypadku usług DRaaS świadczonych przez Aruba Cloud, aby sprawdzić działanie planu awaryjnego, należy jedynie w dowolnym momencie uruchomić proces testowy. Test polega na odzyskaniu systemu przez aktywację serwerów w przestrzeni awaryjnej, bez ingerencji w pracę serwerów produkcyjnych (w przestrzeni głównej). W ten sposób można sprawdzić poprawność procesów replikacji i całego planu awaryjnego.

System replikacji używany w usłudze Aruba Cloud bazuje na rozwiązaniach firmy Zerto, które optymalizują, deduplikują i kompresują chronione dane, by zredukować czas potrzeby na ich odzyskanie (od kilku sekund do kilku minut, nawet w przypadku połączeń międzynarodowych).

Dla małych i dużych

Korzystanie z usług DRaaS ma sens nie tylko w przypadku działalności biznesowej, dla której nieodzowna jest ciągłość. Przedsiębiorstwa traktujące swoich klientów dojrzale powinny nieustannie zwiększać nakłady na bezpieczeństwo IT, stosując dodatkowo rozwiązania chmurowe. Jednak, jak wynika z badania Aruba Cloud „Użytkowanie usług chmurowych w przedsiębiorstwach działających w Polsce", przeprowadzonego w październiku 2017 r., większość instytucji trzyma i zabezpiecza dane we własnym zakresie, na swoich serwerach. Tylko 27 proc. firm przekonało się do rozwiązań chmurowych.

Co zatem powstrzymuje migrację do chmury? Podstawowym problemem jest poczucie braku kontroli nad danymi w kontekście bezpieczeństwa. W tej kwestii badanie Aruba Cloud pokazuje dwa oblicza firm. Z jednej strony przedsiębiorcy rozumieją, że chmura jest środowiskiem bezpiecznym i dostrzegają jej zalety. Z drugiej jednak – boją się przekazać swoje cenne dane do chmury, sądząc, że będą poza ich zasięgiem i kontrolą.

Niedawno udostępniono informację, że Departament Obrony USA chce w ciągu 10 lat przenieść całą swoją infrastrukturę IT do chmury. Ujawniono również kwoty, jakie na ten cel może przeznaczyć – nawet miliard dolarów rocznie. W środowisku chmurowym od pewnego czasu swoje dane trzyma CIA. Nie ma chyba lepszej rekomendacji niż to, że do takiej formy ich przechowywania przekonały się instytucje, które muszą dbać o bezpieczeństwo danych, bo są najbardziej wrażliwe, jak można sobie wyobrazić. Instytucje te często przez lata polegały na własnej infrastrukturze, która na pewno była bezpieczna, ale zdecydowały się skorzystać z możliwości, jakie daje środowisko chmury.

Infrastruktura udostępniana w modelu cloud jest bardzo zaawansowanym i kompleksowym rozwiązaniem, z reguły posiadającym najwyższe certyfikaty bezpieczeństwa. Centra danych Aruba Cloud mają najwyższy, czwarty rating amerykańskiego instytutu ANSI. Certyfikat ten gwarantuje, że bez względu na rodzaj problemu – cyberatak, katastrofę naturalną czy po prostu brak prądu – infrastruktura zapasowa zapewni bezpieczeństwo przechowywanych danych i dostęp do nich. Chmura ma też tę zaletę, że nie trzeba kupować całego pakietu, jak to często bywa w rozwiązaniach typu hosting, lecz płaci się za realnie zużywane zasoby (procesor, dysk twardy, łącza sieciowe). Nigdy nie płaci się za coś, co nie jest używane.

>>> Trzy pytania do...

Marcina Zmaczyńskiego, dyrektora polskiego oddziału Aruba Cloud

CRN Jaka jest obecnie wiedza o możliwościach usług ochronnych w chmurze?

Marcin Zmaczyński Obserwujemy, że znajomość korzyści przynoszonych przez rozwiązania DRaaS szybko rośnie, także w małych i średnich firmach. To właśnie ten sektor może być największym beneficjentem usługi odzyskiwania danych po awarii. W przypadku DRaaS klient ponosi głównie koszty związane z zaangażowaniem pracowników do oceny i wyboru dostawcy. Także czas pełnego wdrożenia usługi jest zdecydowanie krótszy. Obecnie coraz więcej małych i średnich podmiotów decyduje się na zreplikowanie swojego środowiska IT i przeniesienie go do chmury, automatycznie przerzucając odpowiedzialność za zapewnienie dostępności aplikacji i danych na usługodawcę. Klient nie musi samodzielnie utrzymywać zapasowego centrum danych i dbać o jego bezpieczeństwo, a usługa w chmurze kosztuje niewiele. Takie rozwiązanie nie przekracza możliwości finansowych większości firm i coraz liczniejsze mogą sobie na nią pozwolić.

CRN Jakie firmy najbardziej skorzystają na usługach DRaaS?

Marcin Zmaczyński Trudno wskazać przedsiębiorstwa z konkretnej branży, które we współczesnej gospodarce cyfrowej nie odniosłyby korzyści z wykupienia tej usługi. Warto wspomnieć, że zarówno na świecie, jak i w Polsce nie tylko klienci końcowi, ale także usługodawcy dostrzegają możliwości wynikające z rozwijających się usług DRaaS. Z punktu widzenia klientów odzyskiwanie dostępu do środowiska IT po awarii jako usługa to wygodny, skuteczny i efektywny kosztowo sposób zapewnienia nieprzerwanej działalności firmy, która obecnie stanowi o przewadze konkurencyjnej. Z kolei dla usługodawców DRaaS może stać się źródłem dodatkowych dochodów, dzięki rozbudowaniu oferty o pakiety nowych usług.

CRN Co zyskują firmy, przenosząc dane do chmury Aruba Cloud?

Marcin Zmaczyński Przede wszystkim ochronę infrastruktury realizowaną w profesjonalny, prosty i bezpieczny sposób. Jedną z głównych korzyści płynących z usług jest ograniczenie kosztów. W ostatnich latach, kiedy kryzys dotknął wielu branż, firmy były nastawione na oszczędzanie. To sprawiło, że duża część infrastruktury IT zdążyła się zestarzeć, co w połączeniu z przepracowaniem personelu jest idealnym „przepisem" na awarię systemu.

Dodatkowe informacje:
Marcin Zmaczyński, dyrektor polskiego oddziału Aruba Cloud, marcin.zmaczynski@arubacloud.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ ARUBA CLOUD.

Ilustracja AdobeStock

Systemy autentykacji: *wyjście z cienia*

Przedsiębiorcy często nie doceniają roli systemów do uwierzytelniania. Jednak narastająca fala ataków, a także nieskuteczność popularnych produktów przeznaczonych do ochrony danych, w końcu zmieni ich punkt widzenia.

Wojciech Urbanek

Niemal co tydzień media donoszą o poważnych wyciekach danych. Jak dotąd, liderem niechlubnego rankingu jest Yahoo, które pozwoliło hakerom przejąć... 3 mld kont użytkowników. W pierwszej trójce znalazły się poza tym serwisy Adult Friend Finder oraz eBay, z których wyparowały dane dotyczące (odpowiednio) 412 mln oraz 145 mln kont internautów. O ile pierwsza pozycja zestawienia wydaje się być raczej niezagrożona, o tyle dwaj pozostali usługodawcy mają duże szanse, aby w miarę szybko opuścić swoje wyjątkowo wstydliwe miejsca. Ryzyko wycieku danych w najbliższych latach będzie rosło za sprawą cyfrowej transformacji, upowszechniania się usług chmurowych oraz coraz większej liczby pracowników z dostępem do istotnych informacji firmowych.

Według raportu IBM Security w 2017 r. na całym świecie wyciekło ponad 2,9 mld rekordów – niemal 25 proc. mniej niż rok wcześniej. Statystyka na pierwszy rzut oka wygląda dość obiecująco, niemniej jednak jej autorzy podkreślają, że spadek jest rezultatem przedefiniowania strategii hakerów, którzy mocniej skoncentrowali się na atakach ransomware. Wspólny element większości skomplikowanych cyberataków stanowi zdobycie przez przestępców danych uwierzytelniających do kont użytkowników uprzywilejowanych. Potwierdzają to wyniki sondażu przeprowadzonego w 2017 r. przez firmę Thycotic, w którym 31 proc. hakerów wskazało konta uprzywilejowane jako najszybszy i najłatwiejszy dostęp do wrażliwych danych. Na drugim miejscu respondenci wymieniali konta e-mail (27 proc.), a na trzecim komputery (21 proc.). Natomiast według analizy Forrestera ok. 80 proc. incydentów kradzieży informacji odbywa się za pomocą przejęć kont pracowników.

Ważna linia obrony

Człowiek od lat jest najsłabszym elementem systemu bezpieczeństwa. Mimo wielu akcji edukacyjnych ludzie wciąż popełniają te same błędy. Niestety, w dużej społeczności zawsze znajdzie się osoba, która coś zlekceważy, zapomni lub przeoczy. Co gorsza, przechwycenie jednego rekordu pracownika może spo-

Zdaniem integratora

Marcin Gryga, IT Security Architect w netology

Największą popularnością wśród produktów w naszej ofercie cieszą się rozwiązania PAM 2FA oraz MFA. Te dwa rodzaje systemów są obecnie stosunkowo popularne ze względu na wprowadzane przepisy. W mojej ocenie rozwiązania IAM, umożliwiające weryfikację uprawnień użytkownika w wielu systemach jednocześnie, będą kluczowym systemem w przyszłości nawet w średniej wielkości przedsiębiorstwach. Monitorowanie dostępu do poszczególnych aplikacji staje się obecnie zasadniczym czynnikiem umożliwiającym zmniejszenie ryzyka wycieku danych po włamaniu.

wodować efekt domina i doprowadzić do wycieku milionów profili gromadzonych w firmowych bazach danych. Systemy uwierzytelnienia tworzą pierwszą linię obrony przed niefrasobliwymi lub celowo działającymi na szkodę przedsiębiorstw pracownikami. Jednak firmy stosunkowo rzadko sięgają po tego typu rozwiązania. Istnieje liczne grupa przedsiębiorców kompletnie niezainteresowanych uwierzytelnianiem.

– *Twierdzą, że nie potrzebują tego typu produktów* – mówi Marta Zborowska, Sales Director w Connect Distribution.

W jaki sposób do nich dotrzeć i zmienić ich sposób myślenia?

– *Niektóre firmy poważnie traktują rekomendacje organizacji Center of Internet Security zalecającej uruchomienie weryfikacji dwuetapowej, czyli 2FA lub uwierzytelniania wieloskładnikowego, a więc MFA, w każdej aplikacji biznesowej. Najczęściej przedsiębiorstwa zaczynają od rozwiązań 2FA, które następnie aktualizują do MFA. Dopiero w kolejnych etapach rozważają wdrożenie systemów IAM oraz PAM* – tłumaczy Marcin Gryga, IT Security Architect w netology.

Kluczową kwestą wydaje się dobór rozwiązania adekwatnego do potrzeb i możliwości finansowych potencjalnego nabywcy. W mniejszych firmach proces nadawania uprawnień i zarządzania tożsamością jest dość prosty i nie wymaga zastosowania specjalistycznych narzędzi.

– *Klienci zamiast tokenów sprzętowych często wybierają aplikacje na smartfony. Dużą popularnością cieszą się też rozwiązania w chmurze, bowiem nie wymagają instalowania kolejnego urządzenia w firmowej serwerowni* – utrzymuje Michał Jarski, VP EMEA w Wheel Systems.

Niemniej jednak skala trudności związanych z zarządzaniem tożsamością niewspółmiernie wzrasta w przypadku większych przedsiębiorstw. W sukurs przychodzą dostawcy systemów Identity & Access Management, które zapewniają podstawowe funkcje związane z dostępem użytkowników do zasobów informatycznych, takich jak aplikacje, bazy danych, zasoby pamięci masowej i sieci. Według MarketsandMarkets globalne przychody ze sprzedaży IAM w 2021 r. osiągną 14,8 mld dol. Dla porównania w 2016 r. przekroczyły nieznacznie 8 mld dol. Analitycy przewidują, że skumulowany roczny wskaźnik wzrostu w latach 2016–2021 wyniesie 13 proc.

Eksperci od zabezpieczeń nie ukrywają, że wdrożenie IAM rozwiązuje tylko część problemów z zarządzaniem dostępem. Najbardziej łakomym kąskiem dla hakerów, co pokazują m.in. wyniki cytowanego wcześniej badania Thycotic, są użytkownicy mający uprzywilejowane prawa dostępu. Do tego ekskluzywnego grona wchodzą zazwyczaj administratorzy IT, informatycy oraz serwisanci. Ich wiedza, a także niemal nieograniczone możliwości w zakresie penetrowania sieci i pamięci masowych, mogą zagrażać bezpieczeństwu przedsiębiorstwa.

Receptą na zminimalizowanie ryzyka jest zainwestowanie w system Privileged Account Management. Oprogramowanie wspomaga monitorowanie i zarządzanie kontami o specjalnych uprawnieniach oraz umożliwia nadzór nad sesjami uprzywilejowanymi. Jeszcze do niedawna były to niszowe produkty – w 2016 r. przychody na globalnym rynku PAM nie przekroczyły miliarda dolarów. Ich przyszłość rysuje się jednak w jasnych barwach. Firma badawcza MarketsandMarkets prognozuje, że sprzedaż PAM w latach 2016–2021 będzie rosnąć w tempie 30 proc. rocznie. Ciekawe są też spostrzeżenia analityków Gartnera. Ich zdaniem do 2020 r. ponad połowa incydentów naruszających bezpieczeństwo usług IaaS oraz Paas będzie efektem braku rozwiązań PAM oraz odpowiedniej polityki bezpieczeństwa w zakresie użytkowników uprzywilejowanych.

Czego nie lubią hakerzy?

Dostawcy produktów do zarządzania tożsamością oraz zindywidualizowanym dostępem liczą, że polski rynek zacznie się bardziej otwierać na tego typu rozwiązania. Nadzieje opierają zwłaszcza na nowych ustawach (RODO, PCI DSS), ›

Podstawowe różnice między rozwiązaniami IAM i PAM

Identity & Access Management	Privileged Account Management
Zarządza indywidualnie nawet tysiącami tożsamości.	Centralnie zarządza jedynie uprzywilejowanymi tożsamościami w przedsiębiorstwie; proces może obejmować wiele systemów znajdujących się w firmie.
Zarządza tworzeniem i usuwaniem tożsamości oraz powiązanymi z nimi uprawnieniami.	Zarządza dostępem do uprzywilejowanych użytkowników i powiązanymi z nimi uprawnieniami. Rolę nadzorcy pełni osoba o tożsamości nadanej przez IAM.
Zapewnia uprawnienia na stałe, do momentu usunięcia (np. „użytkownik X ma teraz uprawnienia Y").	Zapewnia dostęp do uprzywilejowanych kont/podwyższonych uprawnień dla zdefiniowanych okien czasowych (minut lub godzin), na tyle długo, aby wykonać wymagane zadanie.

a także na narastającej fali wycieków danych spowodowanych kradzieżą haseł.

– 62 proc. zgłoszonych naruszeń bezpieczeństwa to ataki na punkty końcowe. Kiedy ich zabezpieczenia zostaną pokonane, hakerzy mogą dostać się do uprzywilejowanych kont i zdobywać dodatkowe uprawnienia umożliwiające penetrowanie sieci i wykradzenie najważniejszych informacji firmowych – twierdzi Marta Zborowska.

W wielu przypadkach tradycyjne systemy bezpieczeństwa, takie jak firewalle i antywirusy, nie stanowią poważnej przeszkody dla cyberprzestępców pragnących uzyskać dostęp do najważniejszych danych. 43 proc. hakerów biorących udział w badaniu Thycotic uznało oprogramowanie antywirusowe oraz antymalware za najmniej efektywne i najłatwiejsze do sforsowania rodzaje zabezpieczeń. Z kolei 30 proc. palmę pierwszeństwa w tej niezbyt chwalebnej kategorii przyznało firewallom. Za najcięższe do przejścia przeszkody ankietowani uznali wielostopniowe uwierzytelnianie (38 proc.) oraz szyfrowanie (32 proc.).

Rozwiązania do wielostopniowego uwierzytelniania cieszą się rosnącym zainteresowaniem użytkowników. Wartość tego segmentu rynku w 2016 r. wyniosła na świecie nieco ponad 5 mld dol., a w 2022 r. ma nieznacznie przekroczyć 12 mld dol. Oczywiście prym w tym zestawieniu wiedzie autoryzacja dwuskładnikowa, w której oprócz loginu należy podać także dodatkowy kod, np. otrzymany SMS-em. Jednak firmy zaczynają też stosować rozwiązania do wielopoziomowej weryfikacji tożsamości. W takim systemie zabezpieczeń po podaniu nazwy użytkownika i hasła wykorzystywane są inne narzędzia do identyfikacji – tokeny, urządzenia biometryczne, certyfikaty lub karty magnetyczne.

JAROSŁAW EITELTHALER
Product Manager
Entrust Datacard, Veracomp

Systemy uwierzytelniania powinny być skalowalne, bo wdraża się je nie tylko w dużych przedsiębiorstwach, ale także w niewielkich biurach – najmniejsze mogą obsłużyć 25 użytkowników. To produkty łatwe we wdrożeniu i codziennym utrzymywaniu. Jednak modernizacja lub wymiana wiąże się zwykle z przemodelowaniem wewnętrznych procedur, co jest często największym hamulcem takich przedsięwzięć. Trzeba pamiętać, że instalacji systemów autentykacji, które nie są zbyt drogie, najczęściej nie uznaje się za samodzielny projekt informatyczny, tylko za zakupy przy okazji wymiany serwerów lub rozbudowy infrastruktury.

Pokaż swoją twarz

Mimo rozwoju nowych technologii użytkownicy najczęściej korzystają z haseł tekstowych, a siła przyzwyczajenia jest na tyle duża, że nie ma co liczyć, iż szybko z nich zrezygnują. Jednak tradycyjne narzędzia muszą być wspierane innowacyjnymi metodami autentykacji. Dlatego rośnie popularność biometrii wykorzystującej indywidualne cechy człowieka: odciski palców, kontury dłoni, geometrię i obraz twarzy, wzór siatkówki lub tęczówki oka, próbki głosu itp. Jednak nie są to rozwiązania gwarantujące stuprocentowe bezpieczeństwo. Specjaliści od cyberochrony często prezentują na konferencjach możliwości oszukania czytników korzystających z biometrii. Na razie nie udało im się pokonać jedynie urządzeń skanujących układ żył, ale naukowcy i programiści nie ustają w wysiłkach, aby wyeliminować słabe punkty rozwiązań biometrycznych. Rozwijana jest biometria behawioralna umożliwiająca identyfikację człowieka na podstawie jego zachowań.

– Pracujemy nad metodami, które będą wykrywać zmiany zachowań wynikające z przemęczenia, pracy w stresie, szantażu albo siłowego przejęcia stanowiska pracy. Wszystko po to, aby przeciwdziałać w czasie rzeczywistym zarówno nadużyciom i włamaniom, jak i zwykłym pomyłkom – wyjaśnia Michał Jarski.

Obiecujące są też próby użycia, w procesach uwierzytelniania, bardzo modnej ostatnio technologii blockchain.

– Myślę, że może się ona sprawdzić w weryfikacji tzw. śladu audytowego lub autentyczności danych biometrycznych. Choć dziś trudno przewidzieć, w jakim kierunku podąży rynek – przyznaje Marcin Gryga.

Podane przykłady świadczą o ogromnym potencjale rynku systemów uwierzytelniania i kontroli dostępu. Potwierdzają to producenci rozwiązań ochronnych.

– Obserwujemy rosnące zainteresowanie systemami do kontroli i uwierzytelniania dostępu do danych wśród dużych firm, dojrzałych informatycznie. RODO zainicjowało przyspieszony kurs w tym zakresie i należy się spodziewać, że wzmożony popyt na wspomniane rozwiązania pojawi się ze strony średnich firm – twierdzi Bogdan Lontkowski, dyrektor regionalny Ivanti na Polskę, Czechy, Słowację i kraje bałtyckie.

Warto zatem zdobywać nowe kwalifikacje i certyfikaty, aby włączyć się do walki o segment rynku, na którym w najbliższych latach przewidywany jest znaczny wzrosty obrotów. Oprócz wiedzy technicznej przydadzą się też umiejętności sprzedażowe, bowiem wielu polskich przedsiębiorców nieufnie podchodzi do tematu autentykacji.

Co różni PAM-y, PIM-y, SUPM-y i IAM-y?

PAM to skrót od Privileged Account Management (zarządzanie kontami uprzywilejowanymi). W fachowych publikacjach często można spotkać też pojęcie PIM, pochodzące od Privileged Identity Management, oznaczające zarządzanie uprzywilejowanymi tożsamościami. Pojęcia PAM oraz PIM stosowane są zamiennie. Specjalną grupę tworzą narzędzia SUPM (Superuser Privilege Management), czyli służące do zarządzania przywilejami superużytkowników. Klasycznym przykładem jest Sudo (Super User Do) – polecenie w systemie Linux oraz Unix, które umożliwia wywoływanie programów z uprawnieniami innych użytkowników, w szczególności administratora nazywanego rootem, bez znajomości haseł. W systemach Microsoft Windows występuje analogiczna komenda „run as". Z kolei IAM (Identity & Access Management) to system do zarządzania tożsamością i dostępem użytkowników.

Uprzywilejowany dostęp bez tajemnic

Urządzenia firmy Wheel Systems gwarantują pełny wgląd w sesje uprzywilejowane w firmowych zasobach IT. Zapewniają unikalną możliwość odtworzenia działań cyberprzestępców oraz chronią przed pomyłkami i wykonaniem niebezpiecznych komend.

Według firmy Verizon aż 55 proc. naruszeń bezpieczeństwa jest związanych z wykorzystaniem kont uprzywilejowanych, a 60 proc. incydentów wynika z błędów popełnionych przez administratorów. Uprzywilejowany dostęp umożliwia wgląd w ważne zasoby IT (serwery, pamięci masowe, urządzenia sieciowe i stacje robocze) oraz modyfikację ich ustawień. Poza tym przejęcie dostępu do kont uprzywilejowanych przez osobę z zewnątrz może doprowadzić do wycieku poufnych danych i ich upublicznienia, co wystawia na szwank reputację przedsiębiorstwa i niweczy zaufanie klientów. Dlatego tak ważne jest zastosowanie sprawdzonych rozwiązań, które w sposób ciągły będą zarządzały wszystkimi uprzywilejowanymi elementami, w tym kontami użytkowników oraz zdalnymi sesjami.

Takie rozwiązanie oferuje firma Wheel Systems. Urządzenia z rodziny Fudo PAM (Privilege Access Management) zapewniają wiele funkcji gwarantujących bezpieczeństwo zasobów IT. Wbudowane w nie narzędzie Secret Manager służy do zarządzania hasłami, które przechowywane są w miejscu bezpiecznym i niewidocznym dla użytkownika uprzywilejowanego. Jego zaletą jest możliwość określania czasu ważności hasła, jego złożoności i długości.

Bardzo ważną funkcję spełnia moduł Privileged Session Monitoring służący do monitorowania, zapisywania oraz analizy sesji prowadzonych z wykorzystaniem uprzywilejowanego dostępu. Dzięki temu do minimum ograniczona jest konieczność dokonywania analizy po wykryciu włamania – natychmiastowy dostęp do podejrzanych sesji umożliwia odtworzenie ich w trybie wideo i uzyskanie takiego samego widoku, jaki miał cyberprzestępca. Narzędzie to może być wykorzystane także przez administratorów do udowodnienia, że nie popełnili błędów w procesie konfiguracji danego systemu.

Nowe Fudo z uczeniem maszynowym

W II połowie 2018 r. do oferty Wheel Systems trafi nowa wersja produktu Fudo o nazwie PMP (Privilege Misuse Prevention). Inżynierowie producenta rozbudowali ją o funkcję wychodzącą poza ramy rozwiązania PAM. Do istniejącej bazy rejestrującej i monitorującej sesje uprzywilejowane dodane zostaną moduły prewencyjne. Będą one na bieżąco oceniać, czy użytkownik podejmuje typowe działania, czy zachowuje się podejrzanie, bo popełnił błąd lub dokonuje właśnie sabotażu.

Nowe mechanizmy będą bazowały w dużej części na zastosowaniu sztucznej inteligencji. Będą badane takie cechy biometryczne jak sposób pisania na klawiaturze lub wykorzystania myszki, ale także zostaną wykorzystane innowacyjne metody badania poziomu stresu. Celem jest zapewnienie prawdziwej prewencji – zapobieganie niepożądanym sytuacjom, gaszenie płomyków w zarodku, zanim staną się pożarem. Sztuczna inteligencja zostanie zaprzęgnięta do pracy tam, gdzie się sprawdza najlepiej: w analizowaniu ogromnych ilości danych w czasie rzeczywistym, wyłapywaniu anomalii oraz weryfikowaniu zgodności danych z wcześniej zarejestrowanymi profilami.

Sztuczna inteligencja to jednak nie wszystko. Producent zapewnia, że wachlarz możliwości prewencyjnych będzie systematycznie rozwijany – trwają już prace nad kolejnymi innowacyjnymi mechanizmami. Wersja demonstracyjna urządzenia Fudo PMP została zaprezentowana podczas kwietniowej konferencji RSA Conference 2018. Obecnie trwają zaawansowane prace nad wprowadzeniem na rynek gotowej wersji produktu.

Główne moduły rozwiązania Fudo PAM

- **Secret Manager** – narzędzie do zarządzania hasłami do kont uprzywilejowanych
- **Privileged Session Monitoring** – system do monitorowania sesji uprzywilejowanych, ich rejestracji i analizy w czasie rzeczywistym
- **Efficiency Analyzer** – rozwiązanie umożliwiające analizę produktywności użytkowników w ramach nawiązanych sesji
- **Application to Application Password Manager** – mechanizm zarządzający hasłami dla aplikacji
- **Privilege Misuse Prevention (nowość)** – moduł analizujący zachowanie użytkowników i przeciwdziałający nadużyciom (będzie dodawany do Fudo PAM jako aktualizacja oprogramowania)

FUDO SECURITY

Dodatkowe informacje: Błażej Marciniak, Product Director, Fudo Security (marka Wheel Systems), b.marciniak@wheelsystems.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ WHEEL SYSTEMS.

Ilustracja AdobeStock

Wallix ułatwi przygotowania do RODO

Zarządzanie dostępem uprzywilejowanym (Privileged Access Management) jest jednym z kluczowych elementów zapewniających zgodność z nowymi przepisami o ochronie danych osobowych.

Regulacje zawarte w RODO wpłyną na wiele zagadnień związanych z IT i praktykami dotyczącymi bezpieczeństwa. Nowe przepisy wykraczają daleko poza obszar ochrony prywatności – rozporządzenie bezpośrednio wpływa na procesy IT w przedsiębiorstwach. Będą mieć znaczenie w zarządzaniu danymi, ich ochronie, rozwoju oprogramowania i administrowaniu systemami.

Tym samym wejście w życie RODO to dla działów IT wiele nowych wyzwań. Reguły polityki dotyczące zarządzania danymi i ich ochrony trzeba będzie zmodyfikować, dostosować do nowych przepisów wiele kluczowych procesów biznesowych, choćby w celu zagwarantowania prawa „do zapomnienia" i przenoszenia danych. W obliczu zagrożenia dotkliwymi karami i ze względu na tempo wprowadzania zmian przedsiębiorstwa muszą starać się ograniczyć do minimum ryzyko naruszenia bezpieczeństwa informacji

Skomplikowane, ale... proste

Z jednej strony RODO może być postrzegane przez pryzmat złożonych przepisów i schematów przepływu informacji oraz raportowania, ale z drugiej regulacje można uznać za całkiem proste. Ich zawiłość da się przełożyć na cztery łatwe do zrozumienia zasady, których należy przestrzegać:

1. zapobiec incydentowi naruszenia bezpieczeństwa,
2. jeśli się zdarzy, wiedzieć, jak do niego doszło,
3. zlikwidować jego skutki najszybciej, jak to możliwe,
4. udowodnić, że szkody zostały naprawione.

Najważniejsze zalety PAM

Privileged Access Management jest tym obszarem zabezpieczeń, w którym za pomocą narzędzi i z zastosowaniem odpowiednich praktyk chroni się firmę przed przypadkowym lub umyślnym nadużyciem uprzywilejowanego dostępu. Rozwiązanie PAM:

- oferuje bezpieczny i łatwy sposób autoryzowania i monitorowania wszystkich użytkowników uprzywilejowanych we wszystkich systemach,
- przyznaje i odbiera przywileje użytkownikom systemów, w których są autoryzowani,
- zapewnia centralne i sprawne zarządzanie ochroną w systemach heterogenicznych,
- tworzy niemodyfikowalną ścieżkę audytu dla każdego działania uprzywilejowanego.

Dla wielu działów IT i zespołów ds. bezpieczeństwa wymienione cztery zasady nie są niczym nowym. Jednak nawet ci, którzy według nich postępują, będą musieli – wobec zagrożenia wysokimi karami – działać znacznie szybciej niż do tej pory. A to oznacza lepsze kontrolowanie uprzywilejowanych użytkowników, czyli takich, którym przydzielono w systemie prawa administratora. Potrzebna będzie szczegółowa wiedza, kto, co i kiedy robił z najważniejszymi systemami i zasobami przedsiębiorstwa.

Zdaniem integratora

Marcin Gryga, IT Security Architect, netology

Wdrożenie systemu do zarządzania dostępem uprzywilejowanym Wallix jest szybkie i proste – podczas PoC pierwsze uruchomienie zazwyczaj nie zajmuje nawet godziny. Rozwiązanie umożliwia definiowanie kont uprzywilejowanych oraz odpowiednich do nich uprawnień. Monitoruje sesje administracyjne, więc administrator jest w stanie zweryfikować kto, kiedy i w jaki sposób logował się na konta uprzywilejowane. System klasy PAM nie tylko pomaga zminimalizować ryzyko włamań z wykorzystaniem uprawnień administracyjnych, ale także tworzy tzw. niezaprzeczalny ślad dowodowy dla kont uprzywilejowanych. W razie incydentu może się to okazać bardzo pomocne podczas współpracy z organem nadzorującym. Rozwiązanie Wallix może służyć jako centralny punkt wejścia do firmy dla użytkowników z zewnątrz i być wykorzystywane do rozliczania prac podwykonawców. Rejestrowanie sesji ułatwia monitorowanie parametrów SLA. Natomiast dzięki automatycznej zmianie haseł ograniczone jest ryzyko skutecznego ataku typu brute-force. Bastion zapewnia też odtworzenie pełnej sesji, co może być dowodem w razie konfliktu z podwykonawcą lub sprawy sądowej.

PAM – pomoc w zachowaniu zgodności

Uprzywilejowany użytkownik dysponuje dostępem do systemu na poziomie administratora albo „roota". Dlatego może np. dodawać, modyfikować lub usuwać konta pocztowe na serwerze Microsoft Exchange Server. Takie prawa dostępu powinny być szczegółowo kontrolowane i łatwo odbierane, gdy nie są już potrzebne.

Zgodność z RODO wymaga śledzenia dostępu na poziomie administratora w każdym systemie, w którym przetwarzane są dane osobowe. Może to w przypadku międzynarodowej firmy odnosić się do zarządzania danymi i ich ochrony w wielu obszarach.

Dokumentowanie dostępu uprzywilejowanego jest niezbędne w przestrzeganiu przepisów RODO. Umożliwia je rozwiązanie PAM, które ułatwia także wewnętrzne i zewnętrzne audyty. Pokazuje ono na przykład, kto w firmie ma uprawnienia do modyfikowania reguł polityki ochrony danych.

Rozwiązanie PAM jest także zgodne z wprowadzaną przez RODO zasadą Privacy by Design. Przestudiowanie wielu głośnych przypadków kradzieży danych prowadzi do wniosku, że ochrona informacji powinna w pierwszym rzędzie objąć osoby o największych prawach dostępu. PAM jest sposobem na rozwiązanie tego problemu – umożliwia zarządzanie dostępem uprzywilejowanym uwzględniające wdrożenie, utrzymanie i odinstalowanie dowolnej aplikacji, obejmując cały cykl jej życia. Kontroluje także działania poszczególnych użytkowników, zapewniając, że są uprawnione, i dokumentując działanie tych osób.

Wallix Bastion spełnia wymagania RODO

Firma Wallix oferuje rozwiązanie PAM, które odpowiada na wyzwania związane z RODO. Pakiet Wallix Bastion łączy bogatą funkcjonalność PAM z prostotą instalacji i użycia. Implementację i wprowadzanie zmian na bieżąco ułatwia architektura pozbawiona agentów. Inne rozwiązania PAM wymagają instalacji specjalnego programowego agenta w każdym systemie, w którym zarządza się dostępem uprzywilejowanym. Jego użycie spowalnia wdrożenie PAM i może prowadzić do przerwania zarządzania dostępem, gdy rozwiązanie przestanie działać w wyniku kolejnej aktualizacji oprogramowania.

Wallix Bastion można instalować lokalnie, jak i w chmurze. Tworzy pojedynczą bramę dostępu, za pośrednictwem której administratorzy systemowi uwierzytelniają się w trybie single sign-on. Dzięki temu dział IT może zdefiniować politykę ochrony prywatności i wymuszać jej przestrzeganie od administratorów i pracowników w całym środowisku. Wśród kluczowych funkcji oprogramowania Bastion znajdują się:

- **Access Manager** – kontroluje dostęp do kont uprzywilejowanych, tworząc pojedynczy punkt definiowania reguł polityki zarządzania tymi kontami i wymuszania ich przestrzegania. Użytkownik uprzywilejowany prosi o dostęp do systemu za pośrednictwem Access Managera. Ten komponent posiada informacje, do którego systemu użytkownik może uzyskać dostęp i z jakim zakresem uprawnień. Tylko superadmin ma prawo dodawać, modyfikować i usuwać konta o uprzywilejowanym dostępie w Access Managerze.
- **Password Vault** – ten komponent sprawia, że uprzywilejowani użytkownicy nie znają rzeczywistych haseł do krytycznych systemów. Ręczne obejście zabezpieczeń fizycznego urządzenia staje się więc niemożliwe. Bastion przechowuje hasła w bezpiecznym „sejfie" i daje dostęp do systemu uprzywilejowanemu użytkownikowi, który zalogował się za pośrednictwem Access Managera. Password Vault wzmacnia ochronę prywatności zgodną z RODO, gwarantując, że administrator nie zmieni ustawień dotyczących zarządzania lub ochrony danych na lokalnym urządzeniu.
- **Session Manager** – śledzi wszystkie działania z wykorzystaniem uprzywilejowanego konta składające się na sesję. Jest pomocny w opracowywaniu bardzo szczegółowych raportów dla organów ochrony danych, których celem jest udokumentowanie incydentu.

Dystrybutorami rozwiązań firmy Wallix w Polsce są: Veracomp i Vemi.

WALLIX
TRACE, AUDIT & TRUST

Dodatkowe informacje: Paweł Rybczyk, Business Developer CEE&Russia, Wallix, prybczyk@wallix.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ WALLIX.

Zarządzanie tożsamością z Ivanti

Jednym z głównych sposobów zapewniania bezpieczeństwa firmowych zasobów jest zarządzanie uprawnieniami użytkowników. Ivanti oferuje oprogramowanie, które pomaga administratorom w zautomatyzowaniu tego procesu i zapewnia łatwiejszą kontrolę nad ochroną przed niepowołanym dostępem do rozwiązań IT.

W zeszłym roku Ivanti kupiło firmę RES – dostawcę oprogramowania do zarządzania tożsamością (Automation i Identity Director), które zostało włączone do portfolio producenta i zintegrowane z jego pozostałymi rozwiązaniami służącymi do zarządzania infrastrukturą IT i do jej ochrony.

– *Systemy nabyte od firmy RES zapewniają kontrolę nad tym, kogo w ogóle dopuszczamy do środowiska IT klienta, a następnie na bardzo precyzyjne określanie do czego dana osoba może mieć dostęp* – mówi Bogdan Lontkowski, dyrektor regionalny w Ivanti na Polskę, Czechy, Słowację i kraje bałtyckie. – *Dzięki temu oprogramowaniu staliśmy się dostawcą bardzo kompleksowych rozwiązań w zakresie bezpieczeństwa wysokopoziomowego, które zapewnia ochronę nie infrastruktury sieciowej, ale bezpośrednio danych użytkowników.*

Pełna automatyzacja

Większość administratorów musi obecnie stawiać czoła zarządzaniu skomplikowanym, wielowarstwowym środowiskiem, nie mając do dyspozycji wystarczająco licznego personelu. Brak możliwości uproszczenia tego procesu wpływa na wzrost ryzyka popełnienia błędu przez człowieka, a w wielu przypadkach utrudnia uzyskanie zwrotu z inwestycji w drogie rozwiązania IT.

Oprogramowanie Ivanti Automation powered by RES zapewnia automatyzację zadań administracyjnych wykonywanych w skomplikowanym środowisku IT. Dzięki niemu personel IT korzysta z repozytorium ponad 300 zdefiniowanych i przetestowanych procesów, które mogą być wykonane zarówno w odniesieniu do firmowej infrastruktury, jak też w środowisku chmurowym (Amazon i Azure).

Główne cechy oprogramowania Ivanti Identity Director powered by RES

KONTROLA DOSTĘPU – zarządzanie regułami polityki dostępu bazujące na atrybutach identyfikacyjnych i kontekście przeprowadzanej operacji

AUTOMATYZACJA – dostęp do usług IT przydzielany jest automatycznie po pozytywnie przeprowadzonym procesie autentykacji

SAMOOBSŁUGA – użytkownicy mogą wnioskować o dostęp do usług za pomocą samoobsługowego portalu lub aplikacji mobilnej

ELASTYCZNE ZARZĄDZANIE – uproszczenie zarządzania skomplikowanym środowiskiem IT

ZGODNOŚĆ Z REGULACJAMI – ograniczenie ryzyka wycieku danych i zapewnienie zgodności z regulacjami branżowymi lub prawnymi (w tym RODO)

Wszystkie działania i modyfikacje definicji automatyzowanych procesów są odnotowywane. Takie podejście zapewnia dodatkową ochronę oraz ułatwia spełnienie restrykcyjnych wymagań prawnych, w tym RODO. Administratorzy mają również dostęp do historycznych raportów oraz narzędzi umożliwiających analizę ustawień konfiguracyjnych.

Konsolidacja uprawnień i kontrola

Chmura oraz popularność urządzeń przenośnych znacząco wpłynęły na sposób dostarczania usług IT w przedsiębiorstwach. Zapewniły wiele korzyści użytkownikom, ale jednocześnie skomplikowały zarządzanie uprawnieniami do korzystania z udostępnianych centralnie firmowych zasobów. Jeśli nie ma możliwości stworzenia ogólnych reguł polityki dostępu, istnieje ryzyko, że dane posiadane przez przedsiębiorstwo trafią do osób niepowołanych. Z drugiej jednak strony proces kontroli dostępu nie może być zbyt restrykcyjny, aby nie wpływał na produktywność użytkowników.

Automatyzację identyfikowania tożsamości użytkowników oraz przydzielania im dostępu do zasobów IT gwarantuje oprogramowanie **Ivanti Identity Director powered by RES**. Zapewnia ono centralną bazę danych uprawnień poszczególnych osób do korzystania z aplikacji i usług oraz integruje się modułami logowania w rozwiązaniach, z których korzysta dana firma. Pracownicy mają także dostęp do samoobsługowego portalu oraz aplikacji mobilnej, w których mogą np. wnioskować o dostęp do danych zasobów, zmieniać lub resetować zapomniane hasło itp. Dzięki temu minimalizowane jest ryzyko powstawania zjawiska „shadow IT", czyli nieautoryzowanego korzystania z chmurowych usług bez zgody, a nawet wiedzy działu IT.

Dodatkowe informacje:
Bogdan Lontkowski, dyrektor regionalny na Polskę, Czechy, Słowację i kraje bałtyckie, Ivanti, bogdan.lontkowski@ivanti.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ IVANTI.

Thycotic – jak nie stracić kluczy do swojego królestwa?

Najczęstszym celem ataków hakerów jest zdobycie danych logowania do kont uprzywilejowanych i administratorów domen. Fakt korzystania z nich często pozostaje niezauważany przez wiele miesięcy. W tym czasie przestępca, jako „zaufany" użytkownik, ma dostęp do najbardziej wrażliwych, niejawnych firmowych danych.

Administratorzy IT często korzystają z domyślnych nazw użytkownika i haseł, a co gorsza dane logowania do kont uprzywilejowanych przechowują w arkuszach kalkulacyjnych, co ułatwia pozyskanie tych poufnych informacji, np. w wyniku ataku na firmowy serwer plików. Pracownicy często przekazują sobie dane do logowania do kont strategicznych z punktu widzenia bezpieczeństwa korporacyjnych zasobów, lekceważąc podstawowe zasady dotyczące systematycznej zmiany haseł i stosowania wieloskładnikowego uwierzytelniania.

Thycotic to dostawca rozwiązań nowej generacji, które minimalizują ryzyko powodzenia cyberataku przez zabezpieczanie haseł do kont uprzywilejowanych oraz ochronę urządzeń końcowych i kontrolę dostępu do aplikacji w systemach Windows i Linux. Obniżają także szansę skutecznego wykorzystania złośliwego kodu, który wycelowany jest w urządzenia końcowe i serwery, ograniczając możliwość wykonania kolejnych kroków przez hakera oraz zapobiegając instalacji narzędzi do zdalnego dostępu. Oprogramowanie to pomaga również unieważnić nieprawidłowo przypisane zwykłym użytkownikom uprawnienia administracyjne, jednocześnie zwiększa uprawnienia odpowiednim użytkownikom, gdy wymagane jest to przez zaufane aplikacje.

Marta Zborowska
Sales Director,
Connect Distribution

Kontrolowanie dostępu do uprzywilejowanych kont w codziennej pracy może być bardzo kłopotliwe i czasochłonne. A ma ogromne znaczenie, bowiem z czasem hasła do kluczowych zasobów „rozchodzą się" po firmie, w wyniku czego osoby na stanowiskach młodszych administratorów, a nawet zwykli użytkownicy, uzyskują niebezpiecznie wysokie uprawnienia dostępu, co jest zagrożeniem dla całego przedsiębiorstwa.

Podstawę oferty firmy Thycotic stanowią rozwiązania do ochrony haseł. Oprogramowanie **Secret Server** dostępne jest jako licencja lokalna lub w chmurze. Tworzy główną warstwę zabezpieczeń zarządzaną przez administratora i służy do obrony przed cyberatakami skierowanymi na konta uprzywilejowane.

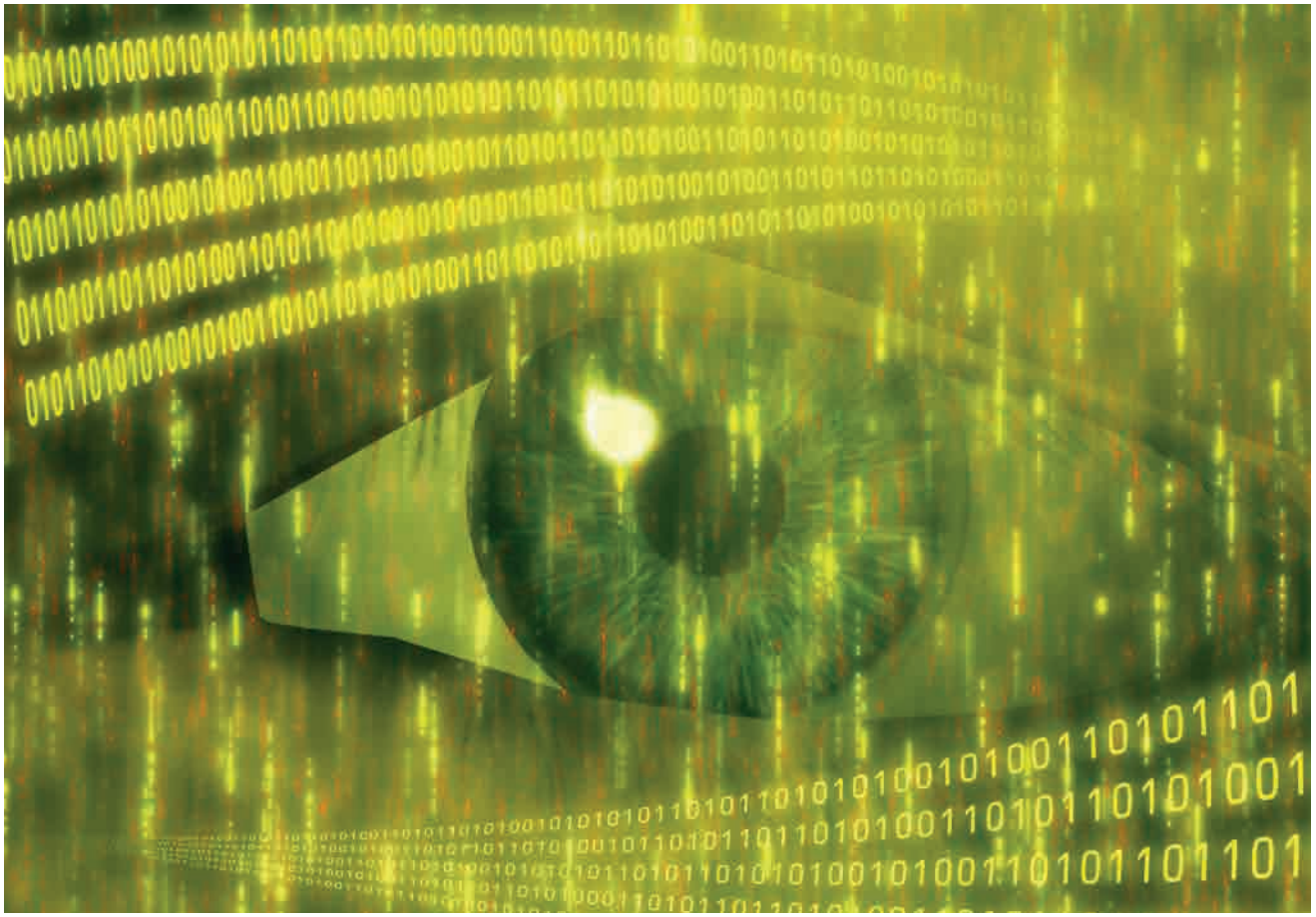
Privileged Behavior Analytics pomaga administratorom IT i osobom odpowiedzialnym za bezpieczeństwo firmowych zasobów szybko wykrywać naruszenia ochrony, zanim spowodują szkody i analizować proces zakładania uprzywilejowanych kont dostępowych w całym przedsiębiorstwie. Rozwiązanie to może być integrowane z oprogramowaniem Secret Server, dzięki czemu dodaje do niego kolejną warstwę zabezpieczającą. Z kolei **Password Reset Server** to narzędzie do prostego, samoobsługowego zarządzania hasłami, które odciąża dział IT od czasochłonnych i nieefektywnych procesów oraz wymusza wzmocnienie kontroli haseł użytkowników.

Druga grupa produktów zapewnia ochronę urządzeń końcowych i ułatwia sprawowanie kontroli nad dostępem do nich. Jej podstawę stanowi rozwiązanie **Privilege Manager** do zarządzania aplikacjami dla systemów Windows i macOS, łączące funkcje zarządzania uprawnieniami użytkowników oraz białą listę aplikacji. Oprogramowanie **Group Management Server** umożliwia wskazanym przez administratorów pracownikom spoza działu IT bezpieczne zarządzanie grupami Active Directory, bez przypisywania im kont uprzywilejowanych. Z kolei **Security Analysis Solution for Windows** identyfikuje błędy konfiguracji rozwiązań ochronnych za pomocą protokołu SCAP (Security Content Automation Protocol), a następnie automatycznie je koryguje. Natomiast **Unix Protection** umożliwia administratorom Secret Server korzystanie z dwóch dodatkowych funkcji: białej listy uniksowych komend oraz zarządzania prywatnymi i publicznymi kluczami SSH.

W odróżnieniu od podobnych rozwiązań, produkty Thycotic są szybkie we wdrożeniu, proste w obsłudze, skalowalne, a ponadto sprzedawane w bardzo atrakcyjnej cenie. Ich autoryzowanym dystrybutorem w Polsce jest Connect Distribution.

Dodatkowe informacje: Marta Zborowska, Sales Director, Connect Distribution, m.zborowska@connectdistribution.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI THYCOTIC I CONNECT DISTRIBUTION.



Ilustracje AdobeStock

Monitoring wizyjny, kontrola dostępu i brak przestojów

Dla integratora, który zjadł zęby na budowaniu sieci oraz wdrażaniu aplikacji i systemów, dołączenie do oferty monitoringu wizyjnego, fizycznej kontroli dostępu i zasilania gwarantowanego nie powinno stanowić problemu.

Tomasz Janoś

Profesjonalne systemy monitoringu, wykorzystujące komunikację IP, to rozwiązania o coraz większych możliwościach, składające się z wielu komponentów: kamer, oprogramowania, sieci komputerowej, pamięci masowej, monitorów. Każdemu klientowi można zaoferować rozwiązanie dostosowane do jego indywidualnych potrzeb. Także w zakresie kontroli dostępu integratorzy mają dziś duży wybór narzędzi. Bezpieczeństwo fizyczne polega również na zapewnieniu ciągłości działania firmowych systemów, a kluczową rolę pełnią w tym rozwiązania zasilania gwarantowanego i klimatyzacji precyzyjnej.

Kamery IP to dla integratora po prostu kolejna grupa urządzeń końcowych. Dość specyficzna, bo wymagająca nowych kwalifikacji, chociażby z zakresu optyki. Nie będzie jednak problemem zdobycie u dostawców informacji o tym, jak określać obszar pokrycia monitoringiem, dobierać obiektywy i obliczać różne parametry, np. całkowitą przestrzeń dyskową potrzebną do zapisu obrazu zgodnego z polityką przechowywania danych u klienta. Na tym rynku przewagę może dać integracja systemów monitoringu, kontroli dostępu oraz innych rozwiązań w zakresie bezpieczeństwa fizycznego.

Jak w każdym sektorze branży IT, tak i w monitoringu IP trzeba zmierzyć się z błędnym przekonaniem klientów, że najważniejszy jest koszt zakupu. Tymczasem cena systemu dozorowego

powinna być sprawą drugorzędną. Zdarza się, że system monitoringu jest instalowany tylko dlatego, że ubezpieczyciel wymaga tego przy zawieraniu umowy. Gdy później zdarzy się incydent, najtańsze kamery nic nie pokażą. A poszkodowani klienci, którzy chcieli maksymalnie zaoszczędzić, nabywając po kilkadziesiąt złotych kamery „no-name", zwracają się do integratorów z prośbą o pomoc w znalezieniu i wdrożeniu profesjonalnego rozwiązania do monitoringu.

Wybór tanich rozwiązań wynika także z niewiedzy. Często klient postanawia umieścić kamery gdzie tylko się da, sądząc, że w ten sposób zapewni sobie lepszy monitoring. Jeżeli dojdzie do wniosku, że potrzebuje 30 kamer, to – mając określony budżet – będzie musiał kupić urządzenia tańsze.

– *Nie wie, że lepszym rozwiązaniem będzie w tym wypadku nabycie 15 kamer dwa razy droższych. Wyda tyle samo, a efekt osiągnie znacznie lepszy* – tłumaczy Maciej Cenkier, Surveillance Product Manager w Konsorcjum FEN.

Do błędnych decyzji zakupowych może prowadzić też pogląd wyrażany przez klientów (ale nierzadko i przez instalatorów), że w kamerach najważniejsza jest rozdzielczość. Przekonanie, że im więcej megapikseli, tym lepiej, niekoniecznie sprawdza się w praktyce. Przy większym zagęszczeniu pikseli do kamery wpada mniej światła i lepszy efekt może dać wysokiej jakości kamera o mniejszej rozdzielczości, z odpowiednio dobrym przetwornikiem.

– *Kamera 2- lub 3-megapikselowa z większą światłoczułością zapewni lepszy obraz w dzień niż 8-megapikselowa i dłużej podtrzyma podgląd w pogarszających się warunkach oświetleniowych, bez przełączania się w tryb czarno-biały* – mówi przedstawiciel Konsorcjum FEN.

System monitoringu wizyjnego potrzebuje pamięci masowej, w której będzie przechowywany obraz rejestrowany przez kamery. Można klientowi zaoferować serwer NAS, do którego producenci dołączają oprogramowanie do monitorowania, najczęściej z kilkoma darmowymi licencjami na kamery (kolejne są płatne). Choć nabycie NAS to dla klienta większy wydatek niż kupno rozwiązania przeznaczonego wyłącznie do monitoringu IP, duże znaczenie ma fakt, że otrzyma funkcjonalną pamięć masową, która będzie spełniać wiele innych zadań w jego firmie.

Klientowi chcącemu stworzyć profesjonalny system monitoringu integrator powinien zaproponować sprzęt przeznaczony do takich zastosowań a nie standardowe monitory ogólnego użytku.

– *Ponieważ monitoring polega najczęściej na pracy w trybie 24/7, standardowe monitory będą ulegać częstszym awariom niż urządzenia zaprojektowane do ciągłego działania* - mówi Elżbieta Jędryka, Business Development Manager w Alstorze. – *Poza tym specjalistyczne monitory są dostosowane do wyświetlania obrazu wysokiej jakości i rozdzielczości, więc lepiej nadają się na przykład do wyświetlania obrazu z wielu kamer jednocześnie.*

Kontrola dostępu także musi być chroniona

Zaawansowane rozwiązania do ochrony danych nie pomogą, gdy nie zostaną wdrożone odpowiednie zabezpieczenia fizyczne. Inaczej przestępcy łatwiej będzie wejść do serwerowni i wykraść dysk z danymi, niż zaplanować wyrafinowany atak przez Internet. Najczęściej w kontroli wstępu do pomieszczeń i na zakładowy teren stosuje się systemy ›

Trendy w monitoringu wizyjnym

ANALIZA WIDEO

Wykorzystanie inteligencji w rozwiązaniach monitoringu wizyjnego polega na analizie obrazu i związanych z nim informacji, co może mieć mnóstwo zastosowań. Wśród tych wykorzystywanych w biznesie można wymienić na przykład badanie ruchu i zachowania klientów w sklepach w celu zwiększenia sprzedaży. Z kolei rozpoznawanie twarzy, niebezpiecznych przedmiotów, detekcja dymu i ognia to funkcje wykorzystywane w systemach bezpieczeństwa.

WYŻSZA ROZDZIELCZOŚĆ

Na rynku są dostępne kamery o rozdzielczości nawet 30 Mpix (7K), rejestrujące bardzo szczegółowy obraz w dużym polu widzenia. Wielkie rozdzielczości wymagają technik skutecznie ograniczających wykorzystanie pasma i pamięci (kompresja H.264).

WIĘKSZA SZYBKOŚĆ KLATKOWA

Wraz ze spadkiem cen sprzętu rośnie oczekiwanie, że będzie on dostarczał obraz złożony z większej liczby klatek na sekundę. W większości kamer do monitoringu IP standardem jest 30 kl./s, ale są też urządzenia rejestrujące obraz z szybkością 120 kl./s. Niektóre stosowane w monitoringu IP aplikacje wymagają dużych szybkości klatkowych, należy do nich m.in. rozpoznawanie tablic rejestracyjnych.

KAMERY DOOKÓLNE

Modele hemisferyczne (180 albo 360 stopni) zaczynają powoli wypierać szybkoobrotowe kamery PTZ, które pokazują fragment całego obrazu, na który są w danym momencie skierowane. Kamera dookólna jest wyposażona w wiele soczewek, z których obraz – dzięki zaawansowanemu oprogramowaniu – jest automatycznie przetwarzany na pełny widok.

KAMERY O DUŻEJ CZUŁOŚCI

Dzięki postępowi w zakresie światłoczułości kamery IP stały się bardzo funkcjonalnymi urządzeniami, z których można korzystać także w nocy. Dzięki wykorzystaniu sensorów IR i termowizji do wykrywania ruchu i obiektów nie jest w ogóle potrzebne światło widzialne. Gdy zastosuje się funkcję dodawania koloru do obrazu w podczerwieni staje się on bardzo podobny do uzyskiwanego w świetle widzialnym.

KAMERY 3-D

Zapewniają dokładniejszy, oparty na głębi obraz, lepiej określają rozmiar, kształt i odległość do monitorowanych obiektów. Znajdują zastosowanie przede wszystkim w analityce wideo, sprawdzają się np. w precyzyjnym zliczaniu ludzi lub rozpoznawaniu niebezpiecznych zachowań.

z kartami, czytnikami i kontrolerami. Ponieważ w sprzedaży jest wiele tego typu rozwiązań, aby osiągnąć oczekiwany poziom bezpieczeństwa, integrator musi wybrać właściwą technikę.

Zdecydowanie nie ma sensu wybór producenta rozwiązania, który dla wszystkich klientów stosuje ten sam klucz cyfrowy. Mniej bezpieczny będzie też system, w którym na wszystkich kartach przechowywany jest ten sam klucz. Czytniki kart powinny być dobrze zabezpieczone przed przejęciem klucza przez intruza. Skuteczniejsze będzie rozwiązanie, w którym klucze są przechowywane nie w zewnętrznym czytniku kart, ale w centralnym kontrolerze, do którego dostęp wymaga specjalnego uwierzytelnienia.

W miejscach, w których powinna być zastosowana zwiększona kontrola dostępu, stosuje się wieloskładnikowe uwierzytelnianie, na które składa się element, który użytkownik posiada (np. karta), element, który zna (PIN lub hasło), oraz taki, który jest charakterystyczny dla jego osoby (biometria). Użycie kombinacji wymienionych metod uwierzytelniania znacznie ogranicza ryzyko, że próbująca uzyskać dostęp osoba nie jest tą, za którą się podaje. W tym przypadku mniejszym problemem staje się zgubiona, skradziona lub sklonowana karta. Najtańsze tego typu rozwiązania, w których drugim po karcie elementem jest hasło lub PIN, wymagają użycia czytników z wbudowaną klawiaturą. Najlepiej, jeśli hasło będzie okresowo zmieniane – im częściej, tym lepiej.

Wygodę w systemach kontroli dostępu, zarówno pracownikom, jak i osobom odpowiedzialnym za administrowanie nimi, powinno dać zastosowanie biometrii. Wielofunkcyjne terminale, zapewniające biometryczną identyfikację osób, a także tradycyjny sposób kontroli dostępu za pomocą kart czy kodów, dają większe pole manewru we wdrożeniach i zwiększają bezpieczeństwo, umożliwiając zastosowanie dwóch wybranych metod łącznie (np. PIN-u i wzorca odcisku palca lub geometrii twarzy). Niestety, ze względu na relatywnie wysoki koszt klienci rzadko wybierają rozwiązania biometryczne, choć są niezwykle skuteczne i zapewniają wysoki poziom bezpieczeństwa.

Z kolei rozwiązania bazujące na rozpoznawaniu twarzy, ponieważ nie oferują jeszcze bardzo dużej dokładności, mogą być wykorzystywane wyłącznie jako drugi czynnik uwierzytelniający. Biometria od lat postrzegana jest jak docelowy system kontroli dostępu. Na razie, ze względu na cenę, złożoność, a także pewne problemy z użyciem systemów nie zyskują takiej popularności, jakiej się spodziewano. Warto także wiedzieć, że dane biometryczne są uznawane za osobowe, więc podlegają wyjątkowej, ujętej w przepisach ochronie.

Coraz częściej przedsiębiorstwa wybierają nowoczesne systemy kontroli dostępu bazujące na protokole IP. Tego rodzaju ochrona może być ściślej zintegrowana z systemem informatycznym firmy niż rozwiązania monitoringu IP. Ten sam system, który powoduje otwarcie zamka po zbliżeniu karty do czytnika, może służyć do logowania się pracownika na komputerze, przyznawać uprawnienia nowo zatrudnionym i odbierać je rozstającym się z firmą. W takim ujęciu integracja ogranicza ryzyko szkód wyrządzanych przez niezadowolonych byłych pracowników, którym zapomniano odebrać prawa dostępu. Fizyczny system kontroli dostępu przestaje więc pełnić wyłącznie rolę „odźwiernego"– bywa także połączony np. z funkcjami HR, takimi jak kontrola czasu pracy, płace itp.

Bezpieczeństwo fizyczne jako brak przestojów

Zasilanie gwarantowane i klimatyzacja to kolejny obszar bezpieczeństwa fizycznego związany z zachowaniem ciągłości działania systemów informatycznych (a także wielu innych). Nie ma znaczenia skala biznesu. Dla małej firmy komputery, serwery i sieć są tak samo ważne jak centrum danych dla korporacji. Straty wynikłe z uszkodzenia sprzętu są dotkliwe, a przestój oznacza przerwę ›

Zdaniem integratora

Adam Pacocha, prezes Falcon 24, członek zarządu Luna & Sokół Security

Wobec konieczności optymalizacji kosztów wykorzystanie wideoanalityki w monitoringu rozwiązuje najbardziej palący problem związany z czasem pracy i kompetencjami agentów ochrony. Kamery IP w połączeniu z analizą wideo zapewniają dużą wydajność detekcji przez 24 godziny na dobę, 365 dni w roku. Przeniesienie zadań i odpowiedzialności z ludzi na urządzenia i postawienie agenta w nowej roli – osoby zarządzającej systemem zabezpieczeń, a nie bezpośrednio czuwającej nad bezpieczeństwem obiektu – to duży krok w kierunku zwiększenia jakości ochrony. Zaawansowane algorytmy zaszyte w systemie analizują scenę w czasie rzeczywistym i w razie incydentu przesyłają do stacji monitorowania alert wraz z załączonym obrazem. Dzięki analizie tysięcy godzin zarejestrowanych obrazów, pochodzących z różnych okresów i miejsc, oraz zwiększonej czułości systemu można w praktyce doprowadzić do zupełnego braku fałszywych alarmów. Oprogramowanie zapewnia też dokładną parametryzację wykrytego obiektu, w tym określenie jego wielkości oraz szybkości przemieszczania się.

Maciej Cenkier
Surveillance Product Manager, Konsorcjum FEN

Dla integratorów oferujących systemy monitoringu wizyjnego ważna jest wiedza o ofercie rynkowej, umiejętność montowania kamer we właściwych miejscach oraz pełnego wykorzystania możliwości sprzętu i oprogramowania. Jest kilka sposobów zdobycia tej wiedzy. Niektórym partnerom wystarczy przeszkolenie z działania i doboru rozwiązań. Potem, wyposażeni w gotowe narzędzia i kalkulatory, radzą już sobie sami. Dla wielu, zwłaszcza początkujących, lepszym wyjściem jest skorzystanie z pomocy dystrybutora podczas kilku wdrożeń. Dystrybutor przeszkoli klienta końcowego, a przy okazji partnera, który zdobywa w ten sposób praktyczne doświadczenie.

EVER
POWER SYSTEMS

GWARANTOWANA NAGRODA

Każdy zakup premiowany nagrodą

Nie zwlekaj
i wybierz coś dla siebie.

SPRAWDŹ INNE NAGRODY

Promocja trwa do 30.06.2018 r. lub wyczerpania produktu promocyjnego.

w sprzedaży albo produkcji i utratę związanych z tym przychodów, a przy tym trudną do oszacowania utratę reputacji.

UPS-y chronią nie tylko przed zanikami zasilania, ale także przed jego złą jakością. Może ona spowodować nie mniejsze szkody niż przerwa w dopływie energii, a przestoje nawet dłuższe (gdy urządzenia ulegną awarii np. wskutek przepięcia).

– *Rośnie liczba klientów, którzy wiedzą, że UPS to nie tylko podtrzymanie zasilania, ale również, w przypadku produktów online, bardzo dobre zabezpieczenie wrażliwych odbiorów oraz skuteczny filtr napięcia* – zauważa Sławomir Franczak, kierownik ds. rozwoju biznesu UPS w Legrandzie.

Na polskim rynku systemów zasilania awaryjnego panuje bardzo silna konkurencja. Klient ma szeroki wybór marek i dostawców. Według Marka Bigaja, prezesa Evera, wybierając produkty, należy zwracać większą uwagę na wiarygodność dostawcy, jego historię rynkową i oferowany zestaw usług posprzedażowych.

Natomiast z doświadczeń polskiego oddziału firmy Socomec wynika, że klienci są coraz bardziej świadomi faktu, że nowoczesne zasilacze UPS powinny się charakteryzować wysoką niezawodnością (MTBF) oraz sprawnością (najlepiej potwierdzoną certyfikatem niezależnej jednostki badawczej). Dzięki wysokiej sprawności mniejsze są straty cieplne, a tym samym niższe koszty eksploatacji. Ważny jest jak najwyższy współczynnik mocy wyjściowej (bliski 1), co oznacza więcej mocy czynnej dla użytkownika. Klienci cenią sobie także możliwość zarządzania UPS-ami przez sieć i ich kompaktowe rozmiary. Łatwe powinny być: obsługa, rozbudowa i serwisowanie w autoryzowanym serwisie producenta (zapewniającym części zamienne, odpowiednio krótki czas naprawy oraz wydłużenie gwarancji).

– *Klienci biznesowi oczekują m.in. wysokiej sprawności zasilaczy UPS, możliwości zarządzania nimi przez sieć, łatwej obsługi i rozbudowy oraz szybko i skutecznie działającego serwisu producenta* – podsumowuje Dorota Suszek, regionalny kierownik sprzedaży w Socomecu.

Energooszczędność jest dla użytkowników istotną wartością dodaną do podstawowych funkcji zasilacza UPS. Przekłada się na całkowity koszt urządzenia, które po pewnym okresie eksploatacji okazuje się tańsze od tego z niską ceną zakupu. Warto informować klientów, którzy potrzebują np. wielu małych zasilaczy do sieci handlowej, że kilkadziesiąt złotych rocznie oszczędności na opłatach za energię przypadających na jedno urządzenie daje w sumie dużą kwotę.

MAREK BIGAJ
prezes zarządu, Ever

Duże firmy, a coraz częściej także średnie, wybierając system zasilania gwarantowanego, stawiają przede wszystkim na kompleksowość oferty, w tym solidny serwis, oraz zoptymalizowane koszty utrzymania systemu. Przez kompleksowość rozumieją dostosowanie rozwiązania do specyficznych potrzeb, audyty z pomiarami parametrów sieci i charakterystyką obciążeń, po dostawę, instalację i uruchomienie rozwiązania, szkolenie w zakresie obsługi oraz rzetelną opiekę posprzedażną, m.in. okresowe przeglądy serwisowe sprzętu.

W dziedzinie zasilania gwarantowanego można zaobserwować stopniowe rezygnowanie z dużych zasilaczy UPS na korzyść modułowej, skalowalnej konstrukcji, dzięki której klient może wybrać dokładnie taką moc, jakiej potrzebuje na danym etapie inwestycji, i stopniowo zwiększać ją, zgodnie z zapotrzebowaniem biznesowym. W takim modelu łatwiejsze staje się także zapewnienie redundancji, gdyż system działa nawet w przypadku awarii któregoś modułu.

Do zapewnienia ciągłości działania systemu informatycznego potrzeba także odpowiednio chłodzonej infrastruktury. Serwery nie będą bezpieczne, jeśli za odprowadzanie ciepła będzie odpowiadać ogólny system klimatyzacji budynku. Integrator może zabezpieczyć system IT klienta nie tylko dostarczając mu profesjonalny system chłodzenia, ale także pomagając w takim urządzeniu serwerowni, by zwiększyć jej efektywność energetyczną i jak najlepiej wykorzystać możliwości klimatyzacji precyzyjnej.

Ważne długotrwałe relacje

Dla większości firm IT jasne jest, że relacje z klientami nigdy nie powinny przebiegać według schematu „sprzedaj i zapomnij". Muszą bazować na zaufaniu, a zachowa się je, jeśli dostarczane rozwiązania będą najlepiej spełniały potrzeby nabywcy. Szczegółową wiedzę o potrzebach i ich zaspokajaniu ma właśnie reseller oraz integrator, i to na nim – a nie dystrybutorach czy producentach – ciąży odpowiedzialność za właściwy dobór rozwiązań. Jest to szczególnie ważne w przypadku zapewniania bezpieczeństwa i ciągłości działania systemów użytkownika.

Zasilanie gwarantowane opiera się na zaawansowanych urządzeniach, które same mogą ulec awarii, wymagać aktualizacji oprogramowania czy rozwiązania problemów technicznych. Działania integratora powinny obejmować – oprócz technicznego opracowywania i dostosowywania projektów oraz uruchamiania sprzętu u klienta – także wsparcie posprzedażowe. Jest to niezmiernie ważne dla trwałości relacji. Jakość tego wsparcia będzie z kolei w dużym stopniu zależeć od relacji integratora z dostawcą. Warto zatem oferować rozwiązania takich producentów, którzy zapewnią właściwą i szybką pomoc w razie awarii.

Wsparcie w zakresie UPS-ów to tylko jeden z elementów obsługi klienta, polegający na dostarczaniu mu kompletnego systemu IT – serwerów, pamięci, szaf, okablowania itp. Wraz z rozwojem firmy klienta zwiększać się będą jego potrzeby dotyczące zasilania gwarantowanego. To stwarza możliwość rozbudowy i wymiany zasilaczy UPS, m.in. dodawania modułów do istniejącego systemu.

Jeśli rozwój biznesu klienta nie jest intensywny, jako powód do rozmowy o dalszych inwestycjach można wykorzystać fakt, że urządzenia mają określony cykl życia i wymagają modernizacji. Na przykład z czasem baterie w UPS-ach się zużywają, a użytkownicy powinni być systematycznie informowani o konieczności ich wymiany. Integrator może wykorzystać tę okazję do rozmowy o strategicznych decyzjach klienta dotyczących rozwoju firmowego systemu informatycznego.

Monitoring bez komputera z EIZO

Alstor ma w ofercie idealne rozwiązanie do projektów wideonadzoru, w których ważna jest jakość obrazu, ale nie ma potrzeby lub możliwości tworzenia pełnej infrastruktury informatycznej. Są to monitory EIZO DuraVision z wbudowanym dekoderem IP, które nie wymagają połączenia z komputerem i mogą wyświetlać sygnał z 16 różnych kamer IP jednocześnie.

Bazując na produktach DuraVision, Alstor z partnerami może stworzyć rozwiązania dostosowane nawet do bardzo niestandardowych wymagań klienta. Jednym z modeli monitorów EIZO z dekoderem jest 46-calowy **DuraVision FDF4627W-IP**, który może pracować w trybie 24/7. Jest zgodny ze standardami firm Panasonic i Axis, protokołem ONVIF Profile S, istnieje też możliwość podłączenia go do kamer z wykorzystaniem protokołu RTSP. Z kolei **DuraVision FDF2304W-IP** to model 23-calowy, doskonale sprawdzający się tam, gdzie jest mniej miejsca: przy bramach wjazdowych, w małych portierniach czy recepcjach.

Oba monitory mają opatentowane przez EIZO funkcje poprawiające czytelność obrazu. Jedna z nich (Smart Insight) jest zapożyczona z monitorów dla graczy – automatycznie wykrywa słabo widoczne obszary i dopasowuje poziom jasności każdego piksela tak, aby wyświetlanie odbywało się z realistyczną głębią. Przydatna jest również funkcja Smart Resolution, analizująca wyświetlaną grafikę i poprawiająca ją w celu zminimalizowania szumu i wyostrzenia rozmytych partii obrazu. Oprócz tego monitory IP z serii DuraVision korzystają z funkcji Overdrive, która zmniejsza czas reakcji matrycy do zaledwie 8 ms, co ogranicza smużenie i rozmycie, zapewniając odtwarzanym filmom płynność i ostrość.

Warto też zwrócić uwagę na monitor **DuraVision FDF2306W**, w którym zastosowano unikalną technologię Visibility Optimizer. Zapewnia ona zestaw funkcji poprawiających jakość obrazu: Defog (zwiększa czytelność obrazów zniekształconych przez warunki atmosferyczne), Low-Light Correction (wykrywa ciemne obszary i dostosowuje jasność każdego piksela) i Outline Enhancer (analizuje obraz i koryguje go tak, by zredukować szumy i go wyostrzyć). Dzięki zastosowaniu funkcji Visibility Optimizer model ten doskonale nadaje się do wyświetlania obrazu z kamer o dalekim zasięgu.

W portfolio EIZO znajdują się również monitory **DuraVision FDS1903** i **FDS1703** (rozdzielczość 1280 x 1024) wyposażone w wejścia analogowe: D-sub mini 15-pin do połączenia z komputerem oraz composite (BNC) do połączenia z kamerami CCTV. Mogą wyświetlać obraz przesyłany w sygnale NTSC, PAL oraz SECAM w dwóch trybach – Underscan i Normal. W trybie Underscan widoczny jest cały obraz, w trybie Normal widać ok. 95 proc. obrazu, bez zbędnych szumów z sygnału TV występujących czasami przy krawędziach ekranu. Model FDS1903 wyposażono też w funkcję UpView, która nie dopuszcza do utraty nasycenia kolorów przy obserwacji ekranu pod kątem. Jest to szczególnie przydatne wtedy, gdy montowany jest powyżej linii wzroku użytkownika i obraz ogląda się od dołu.

Doskonałym uzupełnieniem sprzętu do dozoru wizyjnego są monitory EIZO z biurowej serii FlexScan, oferowane z wyświetlaczami o przekątnych od 15 do 31,5 cala. Wykorzystują technologię hybrydową, która ogranicza poziom jasności i migotanie obrazu, nie pogarszając przy tym jego stabilności. Najpopularniejsze modele z tej serii to 24-calowy **EV2456** oraz 27-calowy **EV2730**.

Oba monitory wyposażono w matrycę IPS i niezwykle cienkie ramki, które u góry i po bokach mają zaledwie 1 mm szerokości. Ponadto z przodu obudowy znajdują się elektrostatyczne przełączniki ułatwiające obsługę menu OSD. Urządzenia mają całkowicie płaską powierzchnię, dlatego świetnie sprawdzają się w rozwiązaniach wieloekranowych.

Użytkownikom, którzy potrzebują większej przestrzeni roboczej, EIZO oferuje 31,5-calowy model **FlexScan EV3237**. To monitor wyposażony w najwyższej klasy panel IPS o rozdzielczości 3840 x 2160 (4K). Na jego ekranie można wyświetlać dużą ilość danych jednocześnie, dlatego z powodzeniem zastępuje on kilka mniejszych urządzeń.

Wszystkie monitory DuraVision są objęte 2-letnią (modele z dekoderem) lub 3-letnią gwarancją producenta. Monitory FlexScan mają 5-letnią gwarancję. Dystrybutor zapewnia też pełną opiekę serwisową oraz pulę sprzętu EIZO dostępnego do testów.

Dodatkowe informacje: Elżbieta Jędryka, Business Development Manager, Alstor, e.jedryka@alstor.com.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI EIZO I ALSTOR.

Wirtualne wsparcie *zasilaczy Socomec Masterys*

Najnowsze zasilacze UPS firmy Socomec obok niezawodności sprawdzonej technologii, wykorzystywanej od lat w urządzeniach z rodziny Masterys, zapewniają też rozszerzone wsparcie dla instalatorów. Dzięki temu gwarantowany jest znacząco skrócony czas wdrożenia oraz wyeliminowane ryzyko popełnienia błędu.

W styczniu bieżącego roku do oferty firmy Socomec trafiły innowacyjne i łatwe w instalacji zasilacze awaryjne Masterys GP4 oraz Masterys BC+. Dzięki zintegrowaniu inteligentnych algorytmów w infrastrukturze elektrycznej tych urządzeń, ich użytkownicy mają zapewnione ograniczenie zużycia energii, co przekłada się na mniejszy koszt eksploatacji, a także gwarancję wysokiej sprawności działania zasilaczy tej marki oraz ich niezawodności.

JAKUB OLICHWIER
inżynier ds. współpracy z biurami projektów i technicznego wsparcia sprzedaży, Socomec

W pełni cyfrowe urządzenia Masterys czwartej generacji są gotowe na wyzwania związane z trendem Industry 4.0. Dzięki wprowadzeniu inteligentnych algorytmów do dzisiejszych systemów elektrycznych możemy zapewnić ich prostszą i bezpieczniejszą obsługę, która gwarantuje prawidłową i niezawodną instalację sprzętu zasilającego, a jednocześnie oszczędność czasu i kosztów pracy inżynierów. Takie podejście gwarantuje całkowity spokój naszym klientom i użytkownikom końcowym. Oczywiste dla nas jest także, że niezawodność to kluczowa cecha każdego rozwiązania UPS przeznaczonego do ochrony systemów IT, zarządzania ciągłością ich działań oraz oferowanych usług. Dlatego prezentujemy naszym klientom realistyczne, przekraczające standardy rynkowe wartości współczynnika MTBF urządzeń Masterys.

Wdrożenie ze wsparciem

Instalacja każdego zasilacza UPS u klienta oraz jego odbiór techniczny ma fundamentalne znaczenie dla zapewnienia ciągłości pracy całego środowiska oraz optymalizacji wydajności systemu zasilania awaryjnego. Dlatego Socomec opracował przełomowy sposób wdrażania zasilaczy awaryjnych, w którym wykorzystuje się m.in. koncepcję rzeczywistości rozszerzonej.

Socomec stworzył aplikację eWIRE – pierwsze na świecie rozwiązanie pomocne w instalacji UPS-ów. Upraszcza pracę wdrożeniowców, co wpływa na zwiększenie niezawodności systemów zasilania oraz daje pewność, że zostaną przeprowadzone wszystkie niezbędne czynności związane z wdrożeniem i weryfikacją poprawności pracy urządzeń. Dzięki zastosowaniu rzeczywistości rozszerzonej, eWIRE rozpoznaje zasilacz przeznaczony do zamontowania za pomocą kamery smartfona instalatora. Następnie aplikacja automatycznie pobiera wszystkie informacje dotyczące tego UPS-a, aby służyć radą podczas jego montażu. Prezentowane są m.in. wyraźne, wszechstronne i szczegółowe opisy poszczególnych etapów prac – od fizycznego pozycjonowania zasilacza przez prowadzenie kabli i podłączanie baterii do weryfikacji ochrony elektrycznej.

Po zakończeniu prac instalacyjnych eWIRE prosi o przeprowadzenie serii czynności kontrolnych i bilansów, w tym pomiarów elektrycznych. Następnie szczegółowy raport jest przesyłany do centrum serwisowego Socomec w celu sprawdzenia oraz stwierdzenia gotowości do przeprowadzenia odbioru technicznego.

Zasilacze objęte usługami

Rozwiązania Masterys, stanowiące część kompleksowej oferty firmy Socomec, zostały zaprojektowane tak, aby można było dopasować je do budżetu każdej firmy. Przy ich tworzeniu uwzględniono też fakt, że często będą stosowane w projektach modernizacji istniejących instalacji zasilania awaryjnego.

Funkcja ciągłego monitorowania parametrów zasilaczy przez sieć umożliwia wykrywanie nieprawidłowości w ich pracy i zapobieganie potencjalnym usterkom. Dzięki niej partnerzy z łatwością mogą świadczyć usługi konserwacji predykcyjnej, prewencyjnej i korekcyjnej.

Konstrukcja urządzeń Masterys zapewnia także nawet pięciokrotne skrócenie czasu ewentualnej naprawy (w porównaniu ze starszymi monolitycznymi zasilaczami UPS).

socomec
Innovative Power Solutions

Dodatkowe informacje: JAKUB OLICHWIER, INŻYNIER DS. WSPÓŁPRACY Z BIURAMI PROJEKTÓW I TECHNICZNEGO WSPARCIA SPRZEDAŻY, SOCOMEC, JAKUB.OLICHWIER@SOCOMEC.COM

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SOCOMEC.

UPS *MASTERYS*

Zaawansowana konstrukcja i nieograniczone możliwości

MASTERYS GP4 – MASTERYS BC+
W pełni cyfrowy zasilacz UPS 4. generacji
od 60 do 160 kVA

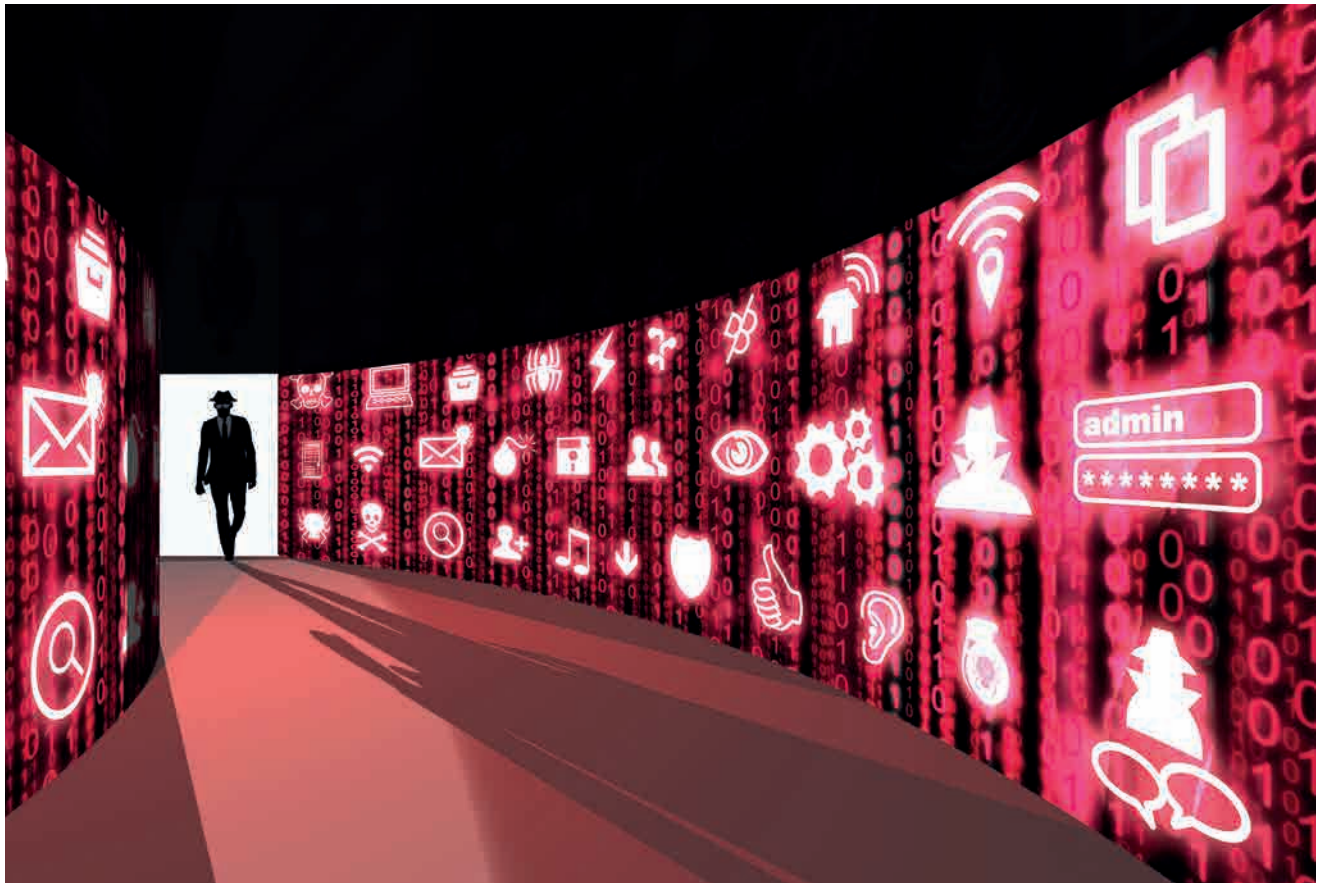
Połączenie intuicyjnej konstrukcji, inteligencji i elegancji zapewnia nowe możliwości

- Wyjątkowa aplikacja mobilna „eWIRE", intuicyjny przewodnik upraszczający instalację
- Zintegrowana technologia gotowa do transformacji cyfrowej
- Doskonała certyfikowana niezawodność
- Rozwiązanie dopasowane do użytkownika i zgodne ze standardami

www.socomec.pl/masterys-range

socomec
Innovative Power Solutions

PUB 1101 02 17



Ilustracja AdobeStock

Zabezpieczenia wpisane w firmowe procesy

Przewagę na rynku zyskają przedsiębiorstwa potrafiące przekonać klienta, że dbają o bezpieczeństwo w całym cyklu tworzenia, wdrażania i użytkowania rozwiązań. Jednym ze sposobów może być niezależny audyt.

Andrzej Gontarz

Zapewnianie cyberbezpieczeństwa należy do najtrudniejszych dziedzin w zarządzaniu firmą. Z kilku co najmniej powodów. Po pierwsze, rzadko wiadomo, kto ma za to odpowiadać. Obecnie jest to zazwyczaj szef IT. Coraz częściej słychać jednak głosy, że ochroną zasobów przedsiębiorstwa powinna się zajmować wydzielona komórka, niezależna od pracowników pionu informatyki. Nie są oni bowiem w stanie poświęcić wystarczającej uwagi kwestiom bezpieczeństwa, gdyż pracują pod presją terminów i wciąż nowych oczekiwań działów biznesowych. Pojawiają się też pomysły, zgodnie z którymi cyberbezpieczeństwo i ochrona fizyczna powinny być umieszczone wspólnie „pod parasolem" jednego ogólnego działu bezpieczeństwa. Mówi się też o tym, że odpowiedzialność za ochronę firmowej infrastruktury IT powinien ponosić wyznaczony członek zarządu.

Ponadto toczą się dyskusje na temat tego, czy nakłady ponoszone na zapewnienie bezpieczeństwa to inwestycje czy koszty. Nie wiadomo przy tym, jak obliczyć, ile trzeba wydać, aby zagwarantować firmie właściwy poziom ochrony bez zbyt dużych nakładów. Problem wynika po części z niezrozumienia specyfiki współczesnych zagrożeń przez osoby kierujące przedsiębiorstwem. Często także przewrażliwienie na punkcie cyberzagrożeń i wyolbrzymianie ich skali, w gronie osób odpowiedzialnych za systemy IT, prowadzi do problemów z racjonalnym wyborem rozwiązań uwzględniających interesy całej firmy.

Wreszcie trudności w kontrolowaniu cyberbezpieczeństwa wynikają też z natury współczesnych zagrożeń. Zmieniają się one bardzo szybko, wraz z rozwojem cyfrowych technologii. Te, które pojawią się w przyszłości, nie muszą być wcale podobne do tych, z którymi borykamy się dzisiaj. W dodatku coraz wyższy jest stopień złożoności ataków i poziomu zaawansowania zastosowanych do ich przeprowadzenia rozwiązań. Metody przestępców są coraz bardziej wyspecjalizowane, ukierunkowane na konkretne, dobrze wcześniej rozpoznane cele. W roli nośnika złośliwego kodu wykorzystywane są już także usługi chmurowe.

Od samego początku

W wyniku upowszechniania się kolejnych technologii, np. blockchain, Internetu rzeczy, sztucznej inteligencji czy sieci 5G, coraz trudniejsze staje się zapewnienie ochrony firmowym zasobom IT. A zatem zapotrzebowanie na usługi i produkty z zakresu cyberbezpieczeństwa będzie stale rosło. Integratorzy powinni uświadamiać klientów, że o ochronie firmowych zasobów trzeba myśleć stale, a nie od projektu do projektu.

– *Zapewnianie bezpieczeństwa musi być od samego początku integralną częścią realizowanych w przedsiębiorstwie procesów. Musi być od razu „zaszyte" w funkcjonujące w firmie rozwiązania* – mówi Michał Kurek, partner w dziale usług doradczych, szef zespołu ds. cyberbezpieczeństwa w KPMG.

Kwestie związane z ochroną trzeba brać pod uwagę już na etapie projektowania systemu, aplikacji czy programu. Rozporządzenie o ochronie danych osobowych (RODO) mówi o tym wprost, wprowadzając zasady: privacy by default oraz privacy by design. Takie podejście, zdaniem Michała Kurka, powinno dotyczyć całego obszaru cyberbezpieczeństwa w przedsiębiorstwach.

W praktyce oznacza to m.in. zmianę podejścia do produkcji oprogramowania. O kwestie ochrony danych należy zadbać już na etapie projektowania każdej aplikacji. Ze względu na presję czasu i wszechobecne dążenie do optymalizacji kosztów jest to dzisiaj element zazwyczaj pomijany, co może przynieść opłakane skutki.

– *Koszt naprawy błędu jest większy w każdej kolejnej fazie tworzenia oprogramowania. Usunięcie wady odkrytej podczas eksploatacji może być nawet stukrotnie droższe niż na etapie testowania aplikacji* – zwraca uwagę Michał Kurek. Jego zdaniem w ekstremalnych przypadkach trzeba nawet stworzyć cały program od nowa.

Istnieją standardy, które pomagają zachować odpowiednie podejście do kwestii bezpieczeństwa w całym procesie przygotowywania aplikacji. Jednym z nich jest opracowanie Software Assurance Maturity Model, przygotowane i udostępnione publicznie przez organizację OWASP. Zaleca ono m.in. analizę kodu oprogramowania w trakcie jego tworzenia. Jego sprawdzanie może następować automatycznie lub być prowadzone przez odpowiednio przygotowanych testerów. Również inne mechanizmy kontrolne pozwalają zapobiec przepuszczeniu błędu – zidentyfikować pojawiające się luki i sprawdzić możliwości skuteczniejszej ochrony oprogramowania. To bardzo ważne ze względu na dynamikę zmian technicznych i biznesowych, z której wynika presja na producentów, by jak najszybciej dostarczali na rynek tanie produkty informatyczne.

Nowe wyzwania

Zintegrowane podejście do cyberbezpieczeństwa stawia nowe wyzwania również przed integratorami. Zaatakowane firmy notują coraz więcej realnych strat i szkód. Trudno się więc dziwić, że intensywnie szukają sposobów przeciwdziałania nasilającym się zagrożeniom. Nie poprzestają już na stosowaniu wewnętrznych procedur i polityki bezpieczeństwa. Domagają się ochrony również od dostawców systemów i aplikacji – producentów, integratorów i sprzedawców.

– *Coraz większe wymagania w zakresie bezpieczeństwa stawiane są ich dostawcom. Ten trend będzie narastał. W zapytaniach ofertowych będzie się pojawiać coraz więcej pytań o środki ochrony stosowane w proponowanych rozwiązaniach* – twierdzi Patryk Gęborys, wicedyrektor w Zespole Bezpieczeństwa Biznesu PwC.

Klienci chcą mieć też w coraz większym zakresie prawo do audytu. Już teraz wielu zastrzega sobie prawo do weryfikacji deklarowanego poziomu bezpieczeństwa w zamawianych aplikacjach lub u dostawcy usług informatycznych. To może być kłopot dla firm, które obsługują wielu klientów.

– *Wyjściem z sytuacji jest przeprowadzenie niezależnego audytu. Raport z jego wynikami można okazywać wszystkim firmom, które są zainteresowane współpracą. Integratorzy lub usługodawcy będą odwoływać się do niego w negocjacjach z każdym klientem* – wyjaśnia Patryk Gęborys.

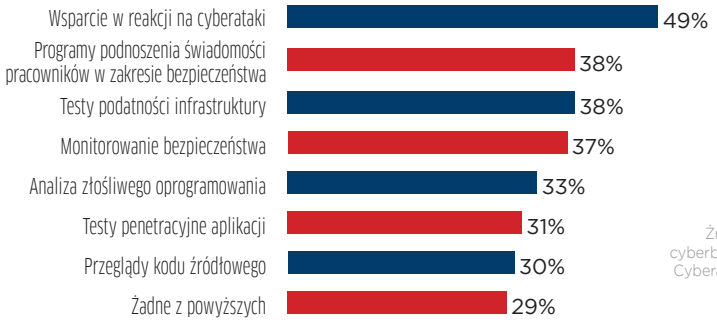
Orzeczenie wydane przez niezależnego audytora pomoże firmie informatycznej w walce o klienta – zaprezentuje ją jako pewnego, godnego zaufania kontrahenta. Dlatego integratorzy, którzy chcą sobie zapewnić przewagę ›

Zdaniem integratora

❑ Jakub Jagielak, dyrektor rozwoju sprzedaży rozwiązań ochronnych, Atende

Firmy mają do czynienia z nasileniem różnego rodzaju cyberataków. Grożą im straty materialne, w tym kary, i prawne konsekwencje skompromitowania systemu bezpieczeństwa oraz utraty newralgicznych danych. Ogromnym problemem jest brak odpowiedniej liczby doświadczonych i wykwalifikowanych pracowników. Na to nakładają się problemy z coraz bardziej zróżnicowaną, trudną do zarządzania infrastrukturą IT, w której stosowane są rozwiązania wielu dostawców. Kolejne wyzwania niesie korzystanie przez pracowników z coraz większej liczby niezabezpieczonych aplikacji i niezaktualizowanego oprogramowania. W zakresie rozwiązań technicznych z jednej strony nasila się automatyzacja ataków, z drugiej – automatyzacja obrony przed nimi. Widać także wzrost zapotrzebowania na systemy EDR (Edge Detection and Response) służące do kontroli bezpieczeństwa na brzegu sieci. Kluczowe staje się wyciąganie wniosków z cyberataków, by zabezpieczyć firmę na przyszłość.

Outsourcing cyberbezpieczeństwa – funkcje i procesy realizowane przez dostawców



Źródło: Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym, KPMG 2018

Planowane inwestycje w różne obszary zabezpieczeń

Źródło: Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym, KPMG 2018

Między certyfikacją a regulacją

W Unii Europejskiej planowane jest wprowadzenie powszechnego systemu certyfikacji wyrobów i usług zapewniających cyberbezpieczeństwo. Ma to umożliwić lepszą orientację w zakresie sposobów wykorzystywania nowych technologii, bowiem coraz trudniej regulować ten obszar. Pojawiające się wciąż nowe zagrożenia powodują, że nie sposób wprowadzić sztywnych, szczegółowych przepisów. Niełatwo nawet stworzyć rejestr zagrożeń, których wystąpienie jest przewidywane w najbliższej przyszłości. Jakie będą zasady funkcjonowania systemu certyfikacji i kiedy wejdzie w życie – jeszcze nie wiadomo.

W Polsce natomiast trwają prace nad projektem ustawy o krajowym systemie cyberbezpieczeństwa. Pod koniec kwietnia został on przyjęty przez rząd. Ustawa obejmie operatorów usług kluczowych i dostawców usług cyfrowych. Za usługi kluczowe zostały uznane usługi o szczególnym znaczeniu dla zapewnienia stabilności funkcjonowania państwa i społeczeństwa, związane m.in. z dostawami wody, gazu, prądu, opieką medyczną, finansami, transportem itp. Operatorzy tych usług będą wyłaniani w drodze decyzji administracyjnej. Z kolei do dostawców usług cyfrowych zostały zaliczone: elektroniczne platformy zakupowe, usługi chmurowe i wyszukiwarki internetowe. Największe znaczenie dla wypełnienia ustawowych zobowiązań będzie miała analiza ryzyka. Na jej podstawie każdy podmiot będzie podejmował decyzje o wyborze adekwatnych środków i sposobów ochrony. W ustawie znajdzie się tylko spis obowiązków podstawowych, m.in. obowiązek zgłaszania incydentów.

konkurencyjną na rynku bezpieczeństwa, powinni zadbać o możliwość posługiwania się wynikami audytu. Istnieją różnego rodzaju normy i standardy, które mogą stanowić podstawę weryfikacji poziomu ochrony oferowanego przez dostawcę, na przykład normy ISO z grupy 27 000 lub standardy typu SOC 1 i SOC 2.

Warto zatem, by firma poddała się audytowi, mimo że nie ma żadnych formalnych, na przykład prawnych, obowiązków w tym zakresie. Oczywiście wiąże się to z pewnymi kosztami. Dla dostawców obsługujących dużą liczbę klientów bądź oferujących skomplikowane rozwiązania taki wydatek bywa jednak opłacalny. Każde przedsiębiorstwo musi więc zrobić rachunek zysków i strat – to w dużej mierze kwestia strategicznej decyzji biznesowej.

– *Z całą pewnością klienci będą coraz częściej pytać o takie potwierdzenia poziomu zabezpieczeń* – twierdzi Patryk Gęborys.

Uważa on także, że klienci firm IT będą dążyli do coraz bardziej szczegółowych zapisów dotyczących kwestii cyberbezpieczeństwa w podpisywanych umowach, na co powinni się już dzisiaj przygotowywać integratorzy i usługodawcy. Przy czym specyfikacji oczekiwanych funkcji zamawianych aplikacji oraz systemów będzie coraz częściej towarzyszyć lista wymogów dotyczących bezpieczeństwa. Spełnienie ich będzie też coraz uważniej sprawdzane podczas testów akceptacyjnych rozwiązania.

Decyzja po analizie

Integratorzy i resellerzy powinni pamiętać, że w zapewnianiu firmom bezpieczeństwa coraz większego znaczenia będzie nabierać analiza ryzyka, a nie spełnianie jednoznacznych wymagań prawnych. Zdaniem ekspertów ma to wiele dobrych stron. Mimo istniejących już norm, każde przedsiębiorstwo może wypracować sobie własną metodę analizy ryzyka. Zadanie nie jest łatwe, ale przyniesie korzyści w postaci wyboru najbardziej optymalnego sposobu ochrony firmowych zasobów. Otwiera się zatem pole do działania dla integratorów, którzy będą chcieli dodatkowo zarobić na wsparciu klienta w przeprowadzeniu analizy ryzyka. Nie ma bowiem norm ani

>>> Trzy pytania do...

dr Dominika Lubasza, radcy prawnego, wspólnika zarządzającego Kancelarii Radców Prawnych Lubasz i Wspólnicy

CRN Obserwujemy coraz większą potrzebę szybkiego wprowadzania na rynek nowych, innowacyjnych rozwiązań. Nie zawsze wiadomo, jakie są skutki ich działania. Kto zatem ponosi odpowiedzialność za ich stosowanie?
Dominik Lubasz Decyzja o wyborze konkretnego rozwiązania zawsze należy do użytkownika. Zanim rozpocznie wdrożenie, powinien przeanalizować, co może bezpiecznie zastosować. Trudno mu będzie przerzucić odpowiedzialność za naruszenie bezpieczeństwa na producenta, jeśli spełnił on swoje obowiązki, na przykład wykonał wszelkie wymagane testy. Działając w najlepszej wierze, użytkownik ma prawo oczekiwać, że wybrany produkt jest odpowiedni do jego celów. W przypadku ujawnienia luki może wysunąć roszczenia. Każdy przypadek będzie jednak wymagał osobnego, szczegółowego zbadania.

CRN W jakim stopniu integratorzy oraz resellerzy odpowiadają za wprowadzenie do sprzedaży niesprawdzonego rozwiązania?
Dominik Lubasz Każdy odpowiada za swoje przewinienia. Jeżeli, na przykład, integrator nie podał prawdziwych parametrów wdrażanego czy sprzedawanego rozwiązania, zataił jakąś informację lub poinformował klienta nieprecyzyjnie, poniesie odpowiedzialność z tego tytułu. Występuje również odpowiedzialność kontraktowa, wynikająca z postanowień umowy. W interesie firm informatycznych jest więc precyzyjne określanie w podpisywanych umowach zakresu własnej odpowiedzialności.

CRN Jakie pozakontraktowe możliwości zabezpieczenia własnych interesów w przypadku nowych technologii mają integratorzy?
Dominik Lubasz Powinni przede wszystkim prowadzić otwartą politykę informacyjną. Z nowymi, nieprzebadanymi do końca technologiami jest podobnie jak z nowymi lekami – niektóre skutki ich używania mogą wystąpić dopiero po pewnym czasie. Integratorzy powinni jasno i wprost mówić, jakie ryzyko może wiązać się z zastosowaniem nowych rozwiązań. Jeżeli dostawca ma jakiekolwiek obawy, lepiej, żeby je ujawnił, nawet jeśli mogą okazać się nieuzasadnione, niż zataił. Podobnie jak w ostrzeżeniach przed niepożądanymi skutkami dołączanymi do leków, jest szansa, że taka informacja zwolni integratora z odpowiedzialności. Jeżeli przedstawił skutki, jakie może pociągnąć zastosowanie nieprzetestowanego rozwiązania, użytkownik podejmie decyzję o wdrożeniu na własną odpowiedzialność. Musi jednak uzyskać wiedzę o ryzyku, którą integrator ma obowiązek mu dostarczyć.

standardów uniwersalnych, które można stosować w każdej firmie. Inne reguły będą obowiązywały podczas analizy ryzyka w dużej firmie energetycznej, a inne u producenta żywności w sektorze MŚP.

Wbrew pozorom analizy ryzyka nie zaczęto stosować w przedsiębiorstwach za sprawą RODO, chociaż unijne rozporządzenie rzeczywiście mocno na nią stawia. W gruncie rzeczy nie wprowadza ono pod tym względem tak rewolucyjnych zmian, jak się powszechnie uważa.

– *Analizy ryzyka były robione przez firmy. I nadal będą robione, bez względu na obowiązujące przepisy* – ocenia Beata Marek, właścicielka firmy Cyberlaw.

Specyfika współczesnych zagrożeń sprawia bowiem, że każdy system informatyczny musi być stale monitorowany i analizowany. A każde przedsiębiorstwo powinno mieć opisane zasoby i procesy przetwarzania danych, ustalone zasady dostępu, procedury backupu itp. Jak to zrobić, nie powie żadna ustawa.

– *To oznacza pracę ciągłą i różną w różnych przedsiębiorstwach. Nie da się stworzyć jednego aktu prawnego, który by to wszystko regulował* – mówi Beata Marek. – *Każdy musi i tak dokonać analizy ryzyka na własny użytek i znaleźć odpowiedni dla siebie sposób jego minimalizacji.*

Według niej nacisk trzeba położyć nie na budowę „muru", lecz na analizowanie podatności systemu IT na ataki oraz procesów zachodzących na jego końcówkach, na routerach i serwerach. A ponieważ informacja jest dla firmy istotną wartością, należy zabezpieczać dane na każdym etapie przetwarzania i przesyłania.

Specjaliści coraz bardziej poszukiwani

Coraz większego znaczenia nabiera umiejętność wyboru konkretnego rozwiązania w danej sytuacji. A większym problemem niż brak szczegółowych regulacji dotyczących bezpieczeństwa wydaje się dzisiaj brak wykwalifikowanych kadr. Firmy mają coraz większe trudności z pozyskaniem specjalistów z tej dziedziny. To szansa dla podmiotów z branży IT, które wyspecjalizują się w konkretnej dziedzinie z zakresu ochrony i będą świadczyć usługi. Duże firmy zapewne zaczną budować własne zespoły, ale na rynku MŚP zapotrzebowanie na outsourcing będzie spore.

Pomocne w zwalczaniu współczesnych zagrożeń mogą okazać się nowe, innowacyjne rozwiązania. Autorzy raportu „Cisco 2018 Annual Cybersecurity Report" twierdzą, że w dziedzinie cyberbezpieczeństwa coraz bardziej będzie się liczyć automatyzacja, uczenie maszynowe oraz sztuczna inteligencja. Wyspecjalizowanie się w tworzeniu i oferowaniu produktów i usług bazujących na wschodzących technologiach daje integratorom szansę zbudowania przewagi konkurencyjnej.

Skoro bowiem na rynku są problemy ze zdobyciem fachowców z dziedziny cyberbezpieczeństwa, trudno liczyć, że integratorzy będą w innej sytuacji. Ale jeżeli zaproponują narzędzia, które dzięki automatyzacji lub w efekcie wykorzystania określonych algorytmów odciążą zespoły ludzkie, będą mogli liczyć na sukces biznesowy.

Ilustracja AdobeStock

RODO: decyduje praktyczne podejście

Nie istnieją systemy informatyczne zgodne z RODO, bo nowe prawo nie zawiera w sobie żadnych „zero-jedynkowych" zapisów.

Andrzej Gontarz

W polskim prawie nie ma obecnie osobnych regulacji dotyczących cyberbezpieczeństwa. Prace nad ustawą o krajowym systemie cyberbezpieczeństwa wciąż trwają, więc firmy i instytucje bazują na regulacjach zawartych w różnych przepisach branżowych, takich jak np. prawo bankowe. Jednak nawet, gdy w końcu uchwalone zostaną akty prawne, które traktują kwestie bezpieczeństwa danych przekrojowo, będą miały bardzo ogólny charakter. W tym kierunku idą prace zarówno nad wspomnianą ustawą o krajowym systemie cyberbezpieczeństwa, jak też nad ustawą wprowadzającą Rozporządzenie o Ochronie Danych Osobowych do polskiego systemu prawnego. Oba projekty przyjmują za podstawę działania analizę ryzyka, której wyniki mają decydować o wyborze odpowiednich rozwiązań zabezpieczających.

Z tego względu nie jest łatwo ustosunkować się do szeregu podnoszonych przez przedsiębiorców kwestii. Należy do nich m.in. pytanie o to, jak należy podchodzić do wdrażania systemów informatycznych, aby sprostać w zakresie bezpieczeństwa wymogom obowiązującego prawa? Kolejny problem to kwestia odpowiedzialności dostawców i integratorów za zapewnienie właściwego poziomu bezpieczeństwa wdrażanych rozwiązań. Trzeba też wiedzieć, według jakich przesłanek dokonywać analizy ryzyka i doboru środków zabezpieczających, żeby spełniać nałożone prawem obowiązki.

Te i podobne pytania nabierają szczególnego znaczenia w kontekście potencjalnych odszkodowań i kar grożących za niewłaściwą realizację ustawowych wymogów. Wprawdzie część dostawców rozwiązań informatycznych zapewnia klientów, że ich system jest zgodny z RODO, ale takie deklaracje w świetle prawa mogą okazać się niewystarczające.

– *Nie ma czegoś takiego jak „zgodność z RODO". Może być jedynie system IT zapewniający realizację wymogów RODO. A to dwie różne rzeczy* – mówi dr Paweł Litwiński, adwokat, wspólnik w kancelarii prawnej Barta Litwiński.

Zwraca przy tym uwagę, że RODO nie wprowadza w tym obszarze żadnych „zero-jedynkowych" rozwiązań. Wyznacza wartości skrajne, określając jedynie sposób podejścia do zagadnienia ochrony danych osobowych. Jak to zrobić w praktyce, każda firma musi zdecydować sama. Dlatego nie można przesądzać o zgodności narzędzia informatycznego z RODO, bo w określonym zakresie będzie się sprawdzał jeden, a w innym przypadku drugi system.

DR PAWEŁ LITWIŃSKI
adwokat, wspólnik w kancelarii radców prawnych i adwokatów Barta Litwiński

Wymogi zawarte w RODO mają charakter zobowiązań publicznoprawnych. Obowiązują bez względu na porozumienie między stronami kontraktu. Nie można w drodze umowy wyłączyć lub ograniczyć odpowiedzialności usługodawcy za naruszenie prawa. Nawet, gdyby klient świadomie zgodził się na przykład za niższą cenę, na niższy poziom zabezpieczeń, to w przypadku naruszenia bezpieczeństwa danych nie będzie to zwalniało usługodawcy od odpowiedzialności za wyciek. W umowie można jedynie ustalić zakres i poziom odpowiedzialności odszkodowawczej.

Liczy się funkcjonalność

Trudność przy wyborze odpowiedniego rozwiązania może stanowić fakt, że nie ma żadnej uniwersalnej checklisty, za pomocą której można by sprawdzić przydatność poszczególnych rozwiązań.

– *RODO nie daje recepty, jak powinny być chronione dane. Wybór odpowiedniego sposobu działania, to problem praktyczny, a nie prawny. Zastosowane rozwiązania mają być skuteczne* – podkreśla Paweł Litwiński.

Zatem w sensie technicznym zgodność lub niezgodność systemu czy rozwiązania z RODO nie istnieje. Można o niej mówić jedynie w sensie usługowym, funkcjonalnym. Przykładowo można sprawdzać, czy system zapewnia wymagane przez RODO przestrzeganie praw osób, których dane dotyczą, a więc prawa do bycia zapomnianym, do przenoszenia danych, do ograniczenia przetwarzania danych itp. Z prawnego punktu widzenia obojętne, jakich użyje się w tym celu narzędzi i technik. Liczy się efekt, który za ich pomocą można osiągnąć. On dopiero podlega ocenie prawnej.

Zabezpieczenie w kontrakcie

Jak powinny w takiej sytuacji zachować się firmy wdrażające systemy informatyczne lub świadczące usługi przetwarzania danych? Jak mogą chronić swoje interesy w związku z wejściem w życie unijnego rozporządzenia?

– *Odpowiedzialność resellera lub usługodawcy można ukształtować kontraktowo. Zakres i poziom odpowiedzialności firmy informatycznej najlepiej określić w umowie* – radzi mecenas Paweł Litwiński.

Zapisy powinny być sformułowane w sposób jasny i dokładny, nie budzący wątpliwości. Integrator musi także zadbać, aby z umowy nie wynikała jego nieograniczona odpowiedzialność. Nawet jeśli będą kary, nie oznacza to, że usługodawca musi pokryć całą zasądzoną kwotę. Umowa powinna jednoznacznie i precyzyjnie określać, za co i do jakiej wysokości odszkodowania odpowiada firma informatyczna.

Można ustalić, do jakiej konkretnie kwoty będzie odpowiadał integrator za szkody, gdyby się okazało, że wdrożony przez niego system nie jest w stanie zrealizować wymaganej przez RODO funkcji i z tego powodu użytkownik został ukarany.

– *Klient zapewne by chciał, aby umowa zapewniała mu zwrot całej kary, którą ewentualnie będzie musiał zapłacić. Jednak dostawca usługi lub rozwiązania nie musi się zgodzić na takie zapisy. Zakres jego odpowiedzialności powinien mieć odzwierciedlenie w możliwościach biznesowych jego firmy* – zwraca uwagę Paweł Litwiński.

Spisanie dokładnej umowy ma dla właścicieli firm informatycznych kluczowe znaczenie, gdyż zasadą jest, że osoba świadcząca usługę pod własną marką ponosi odpowiedzialność z tytułu skutków jej wykonywania. Jeżeli, na przykład, udostępniany w chmurze program nie zrealizuje żądania usunięcia danych, firma, która go oferuje, będzie odpowiadać za konsekwencje powstałej sytuacji tak samo jak jej klient, który wykorzystuje system do przetwarzania posiadanych danych.

Na własną odpowiedzialność

Ostateczna decyzja o wyborze usługodawcy należy oczywiście do klienta. To klient, będąc administratorem danych osobowych, odpowiada za ich bezpieczeństwo bez względu na to, komu powierzy je do przetwarzania. Do niego należy więc też ocena, czy oferowane rozwiązanie, w tej konkretnie konfiguracji i przy tych konkretnie użytych technologiach, jest adekwatne do oszacowanego przez niego ryzyka i wynikających z niego potrzeb. Do niego należy sprawdzenie, czy przetwarzane za pomocą danego narzędzia dane będą bezpieczne oraz używane w sposób wymagany przez prawo.

Problem polega na tym, że nie ma żadnej powszechnie obowiązującej listy wyznaczników, na podstawie których można by dokonać oceny i wyboru systemu. Takie listy mogą dopiero pojawić się w przyszłości. Projektowane polskie przepisy towarzyszące RODO nakładają bowiem na organ ochrony danych osobowych obowiązek opublikowania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Mają być sporządzane z uwzględnieniem specyfiki danego rodzaju działalności i podlegać okresowej aktualizacji.

Ułatwieniem będą z pewnością certyfikaty, których przyznawanie jest przewidziane w nowych przepisach. Posiadanie certyfikatu będzie wskazówką dla klienta, że dostawca oferuje system zapewniający realizację wymogów RODO. Nie uchroni jednak przed karą za niewłaściwe przetwarzanie danych osobowych, bo każdy będzie za nie odpowiadał sam. Każdy, na własne ryzyko i odpowiedzialność, musi zadbać o właściwe zabezpieczenie i zgodne z prawem wykorzystanie danych osobowych. Bez względu na system informatyczny, z którego korzysta.

Indeks firm

CRN COMPUTER RESELLER NEWS POLSKA
WYDANIE SPECJALNE, maj 2018
ISSN 1640-9183

REDAKCJA:
02-674 Warszawa, ul. Marynarska 15
tel. (22) 360-38-00, redakcja@crn.pl,
www.CRN.pl

Tomasz Gołębiowski (redaktor naczelny)
tomasz.gołebiowski@crn.pl,
tel. (22) 44-88-991
Krzysztof Jakubik (redaktor prowadzący)
krzysztof.jakubik@crn.pl,
tel. (22) 244-29-23
Dorota Smusz (sekretarz redakcji)
dorota.smusz@crn.pl,
tel. (22) 44-88-933
Andrzej Gontarz,
andrzej.gontarz@crn.pl
Tomasz Janoś,
tomasz.janos@crn.pl
Wojciech Urbanek,
wojciech.urbanek@crn.pl

KIEROWNIK PROJEKTU VADEMECUM:
Jacek Goszczycki,
jacek.goszczycki@burdamedia.pl

ŁAMANIE I GRAFIKA:
Aneta Mikulska, Marcin Górski

ILUSTRACJA NA OKŁADCE:
AdobeStock
FOTOGRAFIE:
archiwum
KOREKTA: Lidia Sadowska-Szlaga

KIEROWNIK PRODUKCJI:
Tomasz Gajda,
tomasz.gajda@burdamedia.pl

KOORDYNATOR PRODUKCJI:
Jan Kutyna,
jkutyna@burdamedia.pl

PRENUMERATA: Maciej Grzybowski,
prenumerata@crn.pl

WYDAWCA:
Burda Publishing Polska Sp. z o.o.
02-674 Warszawa, Marynarska 15

ZARZĄD:
Chief Executive Officer: Alexander Sorg
General Director Burda International Poland:
Justyna Namięta

Chief Commercial Officer: Michał Helman
Strategy&Sales Support Director:
Małgorzata Teodorowicz
Sales Director:
Małgorzata Nocuń-Zygmuntowicz
Deputy Sales Director:
Katarzyna Nowakowska
Director of Monetization Digital Burda Media:
Katarzyna Cieślik
Chief Digital Officer:
Anna Podkowińska-Tretyn

Brand Manager CRN Polska:
Ewa Korzańska
ewa.korzanska@burdamedia.pl

REKLAMA:
Sekretariat Biura Reklamy
22 360 36 03, fax 22 360 39 80
biuro.reklamy@burdamedia.pl

Sales Team Manager:
Agata Myśluk
agata.mysluk@burdamedia.pl

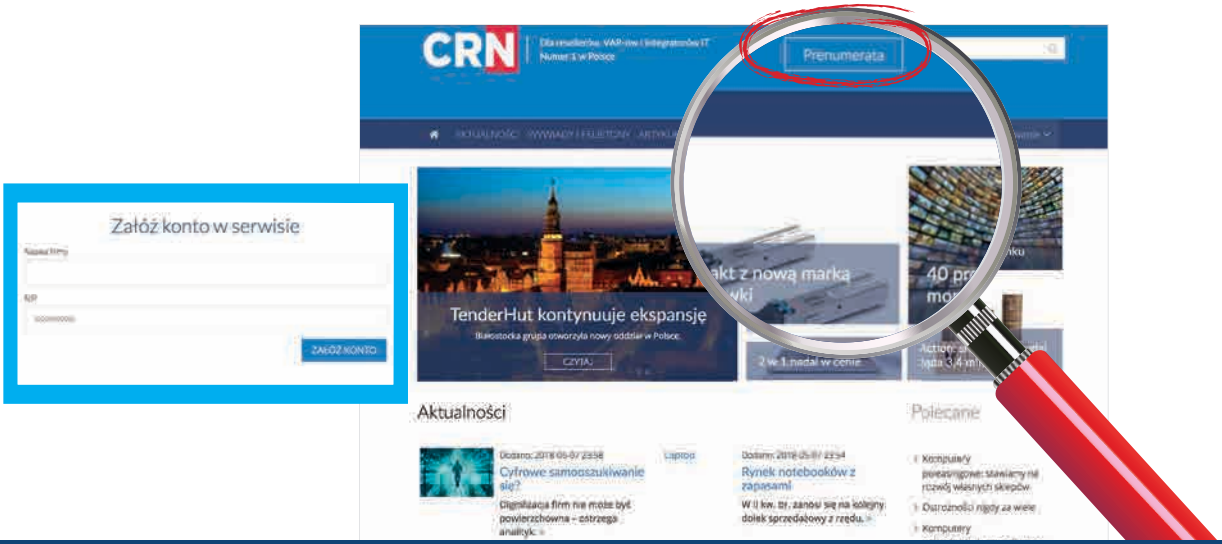
PROJEKTY SPECJALNE:
Senior Project Manager:
Jacek Goszczycki
jacek.goszczycki@burdamedia.pl

PRENUMERATA
BEZPŁATNEGO MAGAZYNU

WYŁĄCZNIE DLA FIRM Z BRANŻY IT

Załóż konto
na stronie CRN.pl
wypełniając odpowiedni formularz

Prenumerata jest aktualna przez 12 miesięcy.
Pod koniec tego okresu wysyłane jest przypomnienie o możliwości jej przedłużenia.



Więcej informacji: tel.: 22 36 03 992, prenumerata@crn.pl

NAJLEPIEJ POINFORMOWANE PISMO W BRANŻY IT!

This is NEXT-GEN Cybersecurity

XG FIREWALL

Stop nieznanym zagrożeniom.

- **Funkcja Synchronized App Control** automatycznie identyfikuje wszystkie nieznane aplikacje
- **Wbudowany Sandbox z mechanizmem Machine Learning,** ATP, podwójnym silnikiem AV, Web & App Control i modułem Anti-Phishing
- **Automatyczna odpowiedź na incydenty - technologia Synchronized Security**

Najwyżej oceniany przez niezależnych ekspertów

NSS Labs ocenił Sophos XG Firewall jako jeden z najlepiej działających firewalli w branży. Przekonaj się sam!

www.sophos.pl/xgfirewall

SOPHOS
Cybersecurity made simple.