VADEMECUM
VAR-ÓW i INTEGRATORÓW

CRN
WYDANIE SPECJALNE
Wrzesień 2023
ISSN 1640-9183

Dane w przedsiębiorstwie

ZARZĄDZANIE I OCHRONA

CRN

Rusza pierwszy w kanale sprzedaży IT program certyfikacji producentów rozwiązań informatycznych!

Certyfikat Channel Master będą mogli uzyskać producenci, którzy prowadzą swoją działalność za pośrednictwem partnerów handlowych, zapewniając im przy tym dostęp do szerokiego wachlarza narzędzi i usług.

CRN Certyfikat Channel Master 2024

Cel programu

Celem programu jest rekomendowanie integratorom IT tych dostawców produktów i usług, którzy kładą szczególny nacisk na ekosystem partnerski. Rolą programu Channel Master jest ponadto zwiększanie świadomości odnośnie do wagi, jaką w dalszym rozwoju całego rynku IT ma dobrze rozwinięty ekosystem partnerski, z korzyścią dla dostawców, integratorów i użytkowników technologii.

Podstawa programu certyfikacji

Procedura certyfikacji została poprzedzona konsultacjami branżowymi z udziałem integratorów IT.
W rezultacie w procedurze certyfikacji będzie weryfikowane 10 kategorii (narzędzi i usług), uszeregowanych i ocenianych zgodnie z oczekiwaniami ekosystemu partnerskiego.

Beneficjenci programu

Certyfikat mogą uzyskać producenci, którzy pomyślnie przejdą procedurę certyfikacyjną opisaną w „Regulaminie programu certyfikacji Channel Master". Uzyskanie praw do tytułu Channel Master stanowi potwierdzenie pełnego zaangażowania producenta w rozwój ekosystemu partnerskiego na polskim rynku IT.

Certyfikaty Channel Master 2024 zostaną wręczone 7 grudnia br. podczas wyjątkowej uroczystości w warszawskim Hotelu Polonia Palace!

Szczegółowych informacji udzielają:
Agata Myśluk, 694 455 426, agata.mysluk@crn.pl • Jacek Goszczycki, 601 935 513, jacek.goszczycki@crn.pl

10 **Lawina danych napędza innowacje**
W obliczu znalezienia się w lawinie danych firmy nie mogą pozostać w bezruchu, lecz powinny podejmować konkretne działania.

Fot. Adobe Stock

16 **Obecnie wszystko i wszyscy są podejrzani**
Zaufanie do kogokolwiek czy czegokolwiek w kontekście cyberbezpieczeństwa powinno stać się... zerowe.

42 **Od kontroli do imitacji**
Wielorakość potrzebnych form ochrony poufnych danych daje integratorom wiele możliwości działania.

24 **Rozproszone dane w hybrydowej chmurze**
Do obsługi nowych aplikacji oraz sposobów przetwarzania danych potrzebne będą zarówno wielkie, hiperskalowe centra danych, jak i te małe, brzegowe.

Spis treści:

Psychologia i biznes: największi wrogowie backupu

Ludzie dzielą się na dwie grupy – tych, którzy robią backup danych i tych, którzy... będą robili. W tym zresztą przypadku powiedzenie „mądry Polak po szkodzie" można z powodzeniem rozszerzyć na obywateli całego świata. Alternatywna mądrość głosi, że dane dzielą się na dwie grupy – zabezpieczone oraz (jeszcze) nie utracone. A skoro przysłowia są mądrością narodu, dlaczego tak wiele firm oraz większość użytkowników indywidualnych odkłada na później lub unika podjęcia choćby podstawowych kroków w celu ochrony swoich najcenniejszych (zaraz po tych finansowych) zasobów?

Dla psychologów odpowiedź na tę zagadkę jest dość prosta, choć wielowątkowa. Nasz mózg ma pewną ewolucyjną „wadę", która polega na tym, że skupia się głównie na zadaniach umożliwiających przetrwanie. Robienie czegoś, z czego zazwyczaj nigdy nie skorzystamy (a nie służy to przyjemności), wydaje się nie mieć sensu. Oczywiście, argument ten można próbować skontrować argumentem, że zabezpieczanie danych przed utratą to działania na rzecz swego rodzaju „biznesowego przetrwania". Zgoda, ale żeby dojść do takiego wniosku potrzebna już jest zdroworozsądkowa racjonalizacja, z którą wielu osobom nie jest po drodze.

Trzeba bowiem przyznać, że w kontekście ryzyka utraty danych oraz backupu stosowanego jako remedium racjonalizacja pobłądziła. Nierzadko można usłyszeć takie argumenty: mnie to nie dotyczy (wiadomo!), mam dobry sprzęt (i nigdy przypadkowo niczego nie skasowałem!), nie mam ważnych danych (to się okaże dopiero po ich utracie...), mój dostawca usługi dba o wykonywanie kopii (przeczytaj umowę...). Dla dopełnienia tej argumentacji, w trakcie swoich podróży już dwa razy spotkałem wyznawców obcych nam kulturowo religii, którzy twierdzili, że nie robią backupu, bo jeśli utracą dane, to znaczy, że... taka była wola siły wyższej.

Do negacji zagrożenia dochodzi brak bezpośrednich, natychmiastowych konsekwencji związanych z rezygnacją z robienia backupu. Nie pomaga też powszechna prokrastynacja: dziś jestem zajęty, a do jutra nic się nie wydarzy, zresztą muszę kupić bardziej pojemny dysk. I tak dalej, a major Edward Murphy tylko pośmiertnie się uśmiecha zza – nomen omen – chmur.

W aspekcie biznesowym też nie jest lekko. Nie ma co ukrywać: backup to koszty. Trzeba zapewnić przestrzeń na nośnikach, kupić odpowiednie oprogramowanie lub sprzęt, wyszkolić pracowników do realizacji tego procesu oraz weryfikacji poprawności jego przebiegu. Rzadko pomaga oferowany przez niektórych dostawców systemów backupu argument, że kopie można wykorzystać też w innym celu, chociażby do prowadzenia prac analitycznych na zgromadzonych w nich danych.

> Honor branży mogą uratować **integratorzy.**

Tymczasem przez całe dekady funkcjonowania branży IT nie było tak dużego wyboru narzędzi do zabezpieczania danych, z jakim mamy do czynienia od kilku lat. Duża konkurencja w tym obszarze spowodowała, że możliwe jest zaspokojenie najbardziej nietypowych potrzeb klientów. Honor naszej branży mogą uratować jedynie integratorzy, którzy dzięki swojemu doświadczeniu gotowi są do przeprowadzenia wywiadu z klientem, stworzenia strategii backupu, zaproponowania rozwiązań w maksymalnym stopniu automatyzujących ten proces oraz przypominania o konsekwencjach utraty danych (finansowych, wizerunkowych i prawnych). Finalnie, sami mogą wziąć na siebie odpowiedzialność za obsługę wykonywania kopii – trudno bowiem o bardziej modelowy przykład tego, co można objąć usługą outsourcingu. Skoro jest z nią związanych tyle psychologicznych barier, niech problemem zajmie się ktoś inny...

Krzysztof Jakubik
redaktor prowadzący

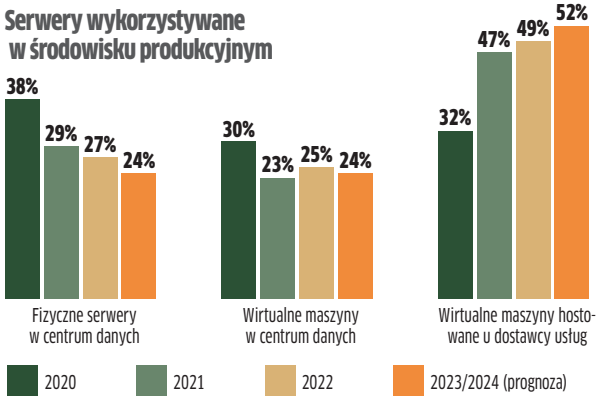
Fot. Adrian Stykowski

Tegoroczne trendy w ochronie danych

Pod koniec 2022 r. na zlecenie Veeam niezależna firma badawcza przeprowadziła wśród 4200 menedżerów i wdrożeniowców z obszaru IT ankietę na temat czynników wpływających na ochronę danych oraz związanych z nią wyzwań i strategii. W gronie tym znalazło się również 200 respondentów z Europy Wschodniej. Z analizy zgromadzonych informacji wynika, że przedsiębiorstwa z naszego regionu świata planują w tym roku zwiększenie budżetu na ochronę danych o 5,6 proc. Pełną treść raportu można pobrać ze strony vee.am/DPR23.

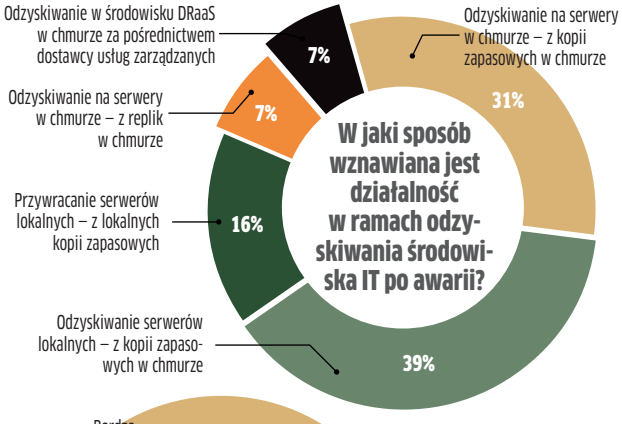
W tym samym czasie przeprowadzone zostało (również na zlecenie Veeam) kolejne interesujące badanie, tym razem dotyczące strategii wykorzystania usług chmurowych (IaaS, PaaS oraz SaaS) do zastosowań produkcyjnych oraz zabezpieczania danych. Wzięło w nim udział 1700 menedżerów, a dokument z treścią raportu z tego badania dostępny jest na stronie vee.am/CPT23.

Serwery wykorzystywane w środowisku produkcyjnym



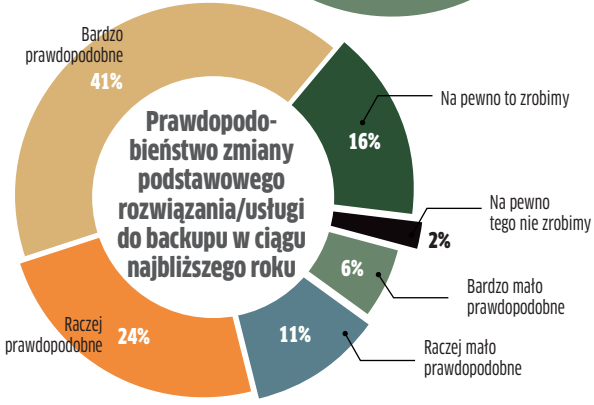
Cechy charakterystyczne dla korporacyjnego rozwiązania do backupu

W jaki sposób wznawiana jest działalność w ramach odzyskiwania środowiska IT po awarii?



Powody uzasadniające skorzystanie z usługi backupu online (BaaS) zamiast tradycyjnego sprzętu i oprogramowania do backupu

Prawdopodobieństwo zmiany podstawowego rozwiązania/usługi do backupu w ciągu najbliższego roku



Źródło: „2023 Data Protection Trends", „Cloud Protection Trends for 2023", Veeam

W pamięciach masowych zmienia się wszystko

„Zmienia się sposób podejścia do tworzenia infrastruktury obsługującej środowisko IT w przedsiębiorstwach. Już od dawna nie istnieją uniwersalne produkty, które są w stanie zaspokoić potrzeby wszystkich” – mówi **Jan Jiskra, Storage Sales Manager (Central Eastern Europe & Central Asia) w Lenovo ISG.**

CRN Jaką rolę w czasach postępującej cyfrowej transformacji firm odgrywają klasyczne macierze dyskowe, które znamy od lat?

Jan Jiskra W związku z tą transformacją zmienia się wszystko, także architektura centrów danych. Pamięci masowe nie są już wyłącznie odizolowanymi silosami, a stały się częścią układanki całego obrazka, jakim jest centrum danych. To przekłada się także na procesy zakupowe realizowane przez klientów. Z tego powodu coraz częściej nie rozmawia się o pamięciach masowych, ale w szerszym kontekście – o zarządzaniu danymi, a w tym procesie macierze dyskowe stanowią tylko część wszystkich zagadnień, które należy uwzględnić.

Co było bezpośrednią przyczyną takiej zmiany?

Dane to obecnie jeden z najbardziej wartościowych zasobów biznesowych. Większość firm oraz instytucji koncentruje wokół nich strategie swojego rozwoju. Dlatego zaciera się granica między fizycznymi macierzami a różnego typu oprogramowaniem do zarządzania danymi i zabezpieczania ich. Na tej granicy obecnie znajdują się oferowane przez wielu dostawców narzędzia klasy software defined storage i to one powodują, że obecnie kryteria związane z wyborem właściwej macierzy nie są już aż tak kluczowe jak kiedyś. Nadal widzimy klientów, którzy w określonych przypadkach kupują pojedyncze macierze, ale generalnie następuje przejście do bardziej projektowego podejścia, wynikającego z potrzeb generowanych przez aplikacje. W oczywisty sposób zyskują na tym producenci, którzy są w stanie zaoferować pełną infrastrukturę end-to-end, obejmującą także brzeg sieci i rozwiązania chmurowe.

> W branży pamięci masowych o wiele rzadziej występuje zjawisko **„vendor lock-in” niż dwie dekady temu.**

Czy to oznacza, że przyszłość klasycznych macierzy dyskowych nie jest pewna? Czy do ich zniknięcia z rynku mogą doprowadzić dyski SSD, w których stale rośnie gęstość zapisu, a przez to możliwe jest zapewnienie dużych pojemności na bardzo szybkich nośnikach, instalowanych bezpośrednio w serwerach?

Nie sądzę, aby klasyczne systemy dyskowe wkrótce miały zniknąć. Nadal są potrzebne do przechowywania dużych repozytoriów danych. Może zmienić się jedynie charakter kupujących je klientów – do tej pory nierzadko były to także firmy inwestujące w macierze dyskowe na własne potrzeby, ale szala tej wagi coraz bardziej prze-

chyla się na rzecz dużych centrów danych, działających na wyłączność dla poszczególnych przedsiębiorstw, jak też komercyjnych usługodawców. Natomiast generalnie zmienia się sposób podejścia do tworzenia infrastruktury obsługującej środowisko IT w przedsiębiorstwach. Już od dawna nie istnieją uniwersalne produkty, które są w stanie zaspokoić potrzeby wszystkich.

Jakie są tego konsekwencje?

W efekcie mamy tak duże zróżnicowanie dostępnych na rynku rozwiązań, że klient może dobrać dla siebie te właściwe. Niektóre firmy mogą preferować system on-premise, inne będą korzystać ze środowiska chmury hybrydowej, ale są też klienci, dla których serwer z dyskami NVMe będzie wystarczający do przechowywania danych. Zawsze zależy to od potrzeb klienta i jego środowiska aplikacji, a także wymagań w zakresie wysokiej dostępności, skalowalności i wielu innych aspektów.

Jakie wyzwania związane z zakupami pamięci masowych stoją obecnie przed klientami? Przez wiele lat najtrudniejsze było zapewnienie odpowiedniej wydajności, ale dzięki pamięciom flash i protokołowi NVMe wydaje się, że problem ten – przynajmniej na pewien czas – został rozwiązany...

Rzeczywiście, dzięki coraz większej popularności nośników NVMe oraz nowej generacji przełączników Fibre Channel część problemów z wydajnością, rozumianą jako gwarancja szybkiego dostarczenia danych z nośnika do kontrolera macierzy, zostało częściowo rozwiązanych. Częściowo, ponieważ w wielu firmach okazała się konieczna modernizacja infrastruktury sieciowej – ta może okazać się wąskim gardłem, szczególnie jeśli tworzące ją urządzenia nie są zgodne z protokołem NVMe-over-Fabrics. Natomiast nowe rodzaje obciążeń w środowiskach IT mogą spowodować pojawienie się nowych rodzajów wyzwań.

Jakiego typu?

Mam na myśli mechanizmy sztucznej inteligencji i uczenia maszynowego, które wymagają nie tylko bardzo szybkiego przetwarzania danych przez procesory kart graficznych, ale też błyskawicznego dostępu do danych archiwalnych, będących „paliwem" dla uczących się silników. Poza tym, w firmach przetwarzanych jest coraz więcej naprawdę różnorodnych danych. W jednej macierzy bywają przechowywane maszyny wirtualne, kontenery, środowiska mikrousług, bazy danych, pliki, w tym backup ze stacji roboczych i serwerów, materiały wideo z systemów cyfrowego nadzoru itd. Dlatego wybór odpowiedniej macierzy, zapewniającej satysfakcjonującą wydajność zarówno przy operacjach losowych, jak również szybkiego zapisu i odczytu sekwencyjnego, nadal nie jest prosty i wymaga doświadczenia w rozpoznawaniu potrzeb klientów, którego powinni oni oczekiwać od integratorów. ➤

Fot. archiwum

A jakiego typu błędy podczas wyboru pamięci masowych i ich wdrażania popełniane są najczęściej?

Celem klientów jest jak najszybsze wprowadzenie w życie ich usług, aby mogli prowadzić biznes. Dlatego za problem uznają każdą sytuację, która może przyczynić się do opóźnień. Rzadko, ale zdarza się, że w wyniku braku zrozumienia podstawowych kwestii związanych z przechowywaniem danych cały projekt wdrożenia jest niewłaściwy, bo wybrano zbyt wolne nośniki lub infrastrukturę sieciową, albo zdecydowano się na takie rozwiązanie, w którym brakuje wewnętrznych mechanizmów zabezpieczania danych. Zdarza się też brak znajomości najlepszych praktyk, szczególnie w kontekście próby przewidzenia jak będą zmieniały się wymagania co do wspomnianej już wydajności, ale też objętości danych – należy zapewnić sobie jak największą elastyczność w kwestii skalowalności środowiska. Jeśli klient nie posiada wystarczającej wiedzy w tym zakresie, a jego wymagania są specyficzne, powinien skontaktować się z partnerem, który specjalizuje się głównie w tematyce związanej z zarządzaniem danymi. Aby uniknąć niepowodzeń w fazie wdrażania, ważne jest też budowanie i utrzymywanie przez klienta kultury oraz zasad DevOps, a także dostosowywanie operacji do rozwoju aplikacji i potrzeb biznesowych.

Na rynku pamięci masowych rozwija się nowy trend związany z zarządzaniem nimi w chmurze. Czy jest to chwilowa moda i z czasem, chociażby ze względów bezpieczeństwa, praktyki takie zostaną zaniechane, czy też w ten sposób klaruje się model zarządzania całą infrastrukturą IT w przyszłości?

Nie ma już ścisłych granic między chmurą a środowiskiem lokalnym. Większość klientów buduje hybrydową architekturę chmurową, aby wykorzystać to, co najlepsze z obu światów. Łączą model konsumpcyjny w chmurze i szybkie wdrażanie z bezpieczeństwem infrastruktury znajdującej się za firewallem. Środowisko aplikacji gotowych do pracy w chmurze odgrywa tutaj ważną rolę w zapewnianiu płynnej integracji.

JAN JISKRA
pracuje w branży IT od ponad 25 lat. Przez większość tego czasu koncentrował się na rozwiązaniach pamięci masowych i zarządzaniu danymi. Do Lenovo, gdzie pełni funkcję dyrektora sprzedaży pamięci masowych na rynkach Europy Środkowo-Wschodniej i Centralnej Azji, trafił cztery lata temu. Wcześniej pracował na różnych stanowiskach technicznych, sprzedażowych i kierowniczych w międzynarodowych firmach, takich jak Sun Microsystems, HPE czy NetApp.

Jeszcze dwadzieścia lat temu producenci pamięci masowych, zazwyczaj celowo, doprowadzali do sytuacji typu „vendor lock-in", w której różnymi sztuczkami technicznymi, finansowymi lub odpowiednią konstrukcją umowy utrzymaniowej uzależniali od siebie klienta. Później, głównie dzięki wysiłkom organizacji SNIA, większość z tych praktyk została zaniechana, a środowisko pamięci masowych stało się bardziej otwarte i interoperacyjne. Ostatnio coraz częściej można zauważyć jednak, że co prawda systemy te nadal są otwarte i „rozmawiają" ze sobą, ale niektóre bardziej zaawansowane funkcje są dostępne tylko w ramach korzystania z rozwiązań tego samego producenta. Czy w ten sposób „na miękko" następuje powrót starych praktyk?

To kwestia wielowątkowa i należy spojrzeć na nią z różnych punktów widzenia. Generalnie potwierdzam, w branży pamięci masowych o wiele rzadziej występuje zjawisko „vendor lock-in" niż dwie dekady temu. Ponadto klienci są obecnie bardzo przeczuleni na tym punkcie i unikają wybierania rozwiązań, które współpracują wyłącznie z innymi produktami danego dostawcy. Akurat segment pamięci masowych jest jednym z najbardziej otwartych w branży IT. W tym przypadku większość technologii sprzętowych i programowych jest uniwersalnych, a konkurenci korzystają z tych samych platform procesorowych, pamięci, interfejsów twardych dysków i łączności sieciowej. To akurat trzeba branży pamięci masowych zaliczyć na plus.

Czyli problem został wyeliminowany na zawsze?

To zależy jak na to spojrzeć, bo rzeczywiście istnieją korzyści płynące z posiadania infrastruktury od jednego producenta. To gwarantuje, że współpraca takich rozwiązań ze sobą została wystarczająco przetestowana oraz łatwiejsza jest ich integracja. Ich dostawca może stworzyć narzędzia, dzięki którym prostsze będzie zarządzanie, chociażby za sprawą ujednoliconego interfejsu,

co oznacza brak konieczności dodatkowych szkoleń dla administratorów. Jeśli dana firma jest przy tym producentem serwerów, może stworzyć narzędzia do wspólnego zarządzania całym środowiskiem. Natomiast taki poziom integracji niekoniecznie musi oznaczać „vendor lock-in". Zresztą identyczne mechanizmy można zaobserwować nie tylko w przypadku pamięci masowych, ale także w innych dziedzinach, szczególnie przy systemach bezpieczeństwa.

À propos, ostatnio coraz częściej w oprogramowaniu macierzy dyskowych można znaleźć różnorodne funkcje ochrony danych, zarówno przed utratą, jak też przed cyberatakami. To duża rewolucja w porównaniu z podstawowym zadaniem pamięci masowych. Czy rzeczywiście użytkownicy korzystają z takich funkcji?

Jak najbardziej, w ostatnim czasie ich obecność stała się jednym z kluczowych kryteriów wyboru dla klientów. Zadaniem macierzy dyskowej jest bezpieczne przechowywanie danych i zapewnienie ich jak największej dostępności. Wcześniej cel ten był osiągany tylko poprzez łączenie dysków w strukturę RAID, aby zabezpieczyć się na wypadek awarii napędu, zaś wysoka dostępność poprzez odpowiednie zaprojektowanie poszczególnych komponentów i przetestowanie ich współpracy. Jednak cyfrowy świat wokół nas staje się coraz bardziej niebezpieczny, co w kontekście faktu, że dane są najważniejszym zasobem we wszystkich branżach, zmusiło wszystkich zainteresowanych do podjęcia dodatkowych działań. W dobie powszechnych ataków ransomware mechanizmy ochronne powinny być wbudowywane absolutnie wszędzie, aby chronić przed powodzeniem takiego ataku, a gdy do niego dojdzie, umożliwiać jak najszybsze przywrócenie środowiska do pracy. Stąd coraz więcej mechanizmów weryfikacji danych, blokad przed masowym zaszyfrowaniem, wykonywania kopii, replikacji do zewnętrznych repozytoriów itd.

Skoro już mówimy o wydajności, w tej dziedzinie dzięki protokołowi NVMe usunięte zostało wąskie gardło powodowane przez interfejsy SAS i SATA. Niemal równolegle na znaczeniu błyskawicznie straciła organizacja Storage Performance Council, której strona internetowa z wynikami testów wydajnościowych macierzy dyskowych była mekką dla wszystkich zainteresowanych tematem i jedynym wiarygodnym źródłem takich informacji. Dlaczego tak się stało i jak w dzisiejszych czasach skutecznie porównywać wydajność konkurencyjnych macierzy? A może, w dobie dysków NVMe, porównywanie wydajności już nie ma sensu?

Rzeczywiście, pamiętam jak wyniki testów SPC były głównym kryterium zakupowym, ale nie zawsze słusznie. Wydajność pamięci masowych od zawsze była skomplikowaną dziedziną do analizy. Testy SPC to była bardzo prosta symulacja teoretycznego obciążenia, charakterystycznego głównie dla baz danych. Tymczasem rola pamięci masowych w firmach uległa zmianie. Obecnie obsługują one bardzo wiele środowisk – jedno urządzenie może przechowywać bazy danych, maszyny wirtualne, pliki itd. Dostępnych jest wiele wpływających efektywnie na wydajność funkcji, jak kompresja, deduplikacja czy wspomniane już mechanizmy antyransomware. Do tego dochodzi integracja z chmurą i wymiana danych przez internet. W takich okolicznościach stworzenie testu, który rzetelnie i uczciwie oceniłby wydajność macierzy w celu porównania jej z konkurencją, jest praktycznie niemożliwe. Testy wydajnościowe mogą prowadzić klienci zainteresowani danym rozwiązaniem, w ramach projektów proof of concept. W naszym przypadku oferujemy możliwość wykonania testów konkretnych aplikacji w naszych centrach obsługi, co pozwala zasymulować rzeczywistą wydajność, jaką uzyskają w swoim środowisku.

Mechanizmy ochronne powinny być wbudowywane absolutnie wszędzie.

Jak w kontekście tej rewolucji, związanej z zastosowaniem nośników flash w profesjonalnych rozwiązaniach, wygląda sytuacja mechanicznych twardych dysków?

Tam, gdzie jest potrzebny sekwencyjny dostęp do danych, twarde dyski sprawdzają się bardzo dobrze pod względem wydajności, a ich cena za jednostkę pojemności wciąż jest znacznie niższa. Nieustannie rośnie też ich pojemność. Natomiast oczywiście liczba ich zastosowań będzie spadać, podobnie jak już praktycznie zostały wyparte z komputerów osobistych. W tej dziedzinie wiele będzie się zmieniało w najbliższym czasie ze względu na obecność nowych technologii produkcji kości pamięci flash, jak QLC, które zapewniają bardzo dużą pojemność za niską cenę. Nie są one tak trwałe jak poprzednie, ale prace nad tym trwają, poza tym nieustannie rozwijane są kontrolery dysków SSD, dzięki którym ryzyko utraty danych jest praktycznie eliminowane.

Lenovo oferuje rozwiązania pamięci masowej również w modelu subskrypcyjnym TruScale Infinite Storage. Nie jest on jednak dostępny w Polsce, czyżby nasi klienci nie byli zainteresowani tego typu ofertą?

Polski rynek jest postrzegany jako bardzo atrakcyjny dla tego typu usług – konkurencyjny i duży. Na pewno jako jeden z najciekawszych w całym regionie CEE. Dlatego z pewnością ta usługa będzie oferowana w waszym kraju, ale w tej chwili jeszcze nie jest dostępna we wszystkich państwach, ponieważ cały czas dopracowujemy warunki jej świadczenia. Ten model oferowania rozwiązań IT stanowi kluczowy element naszej strategii, zresztą obejmujemy nim także inne produkty, na przykład dla środowiska SAP. To jest jeden z czynników wynikających z dużych zmian związanych z przekształceniami na rynku IT, zmieniającą się rolą dostawców, partnerów i usługodawców. Tu dobrym przykładem są operatorzy chmurowi, których określamy jako next-generation cloud service providers. Mimo że teoretycznie są to nasi klienci, bo w ich infrastrukturze działają nasze rozwiązania, traktujemy ich jako partnerów. Wszystko wskazuje na to, że wolumenowo to będą najwięksi odbiorcy rozwiązań infrastruktury centrów danych. Dlatego te partnerstwa są dla nas tak ważne – współpracujemy z większością głównych CSP w Europie, także w Polsce.

Rozmawiał
Krzysztof Jakubik

Lawina danych napędza innowacje

Jeśli znajdziesz się w lawinie, nie zatrzymuj się, stale się poruszaj – doradzają eksperci survivalowi. Nie inaczej jest w przypadku lawiny danych. W jej obliczu firmy nie mogą pozostać w bezruchu, lecz powinny podejmować konkretne działania.

Wojciech Urbanek

Chociaż ilość przetwarzanych i gromadzonych przez firmy danych rośnie, w tym roku na konta dostawców zewnętrznych dyskowych pamięci masowych prawdopodobnie wpłynie mniej pieniędzy niż rok wcześniej. Według prognoz IDC ma to być 32,47 mld dol., co oznacza spadek o 1,4 proc. w ujęciu rocznym. Na osłabienie popytu w tym segmencie rynku wpłynęły przede wszystkim dwa czynniki: spowolnienie gospodarcze oraz wojna w Ukrainie. Wszystko wskazuje na to, że jest to chwilowa zadyszka, bowiem IDC przewiduje, iż globalne przychody ze sprzedaży zewnętrznych dyskowych pamięci masowych w 2024 r. wzrosną do poziomu 34,27 mld dol. Klienci biznesowi nie mogą w nieskończoność odkładać inwestycji związanych z modernizacją infrastruktury IT, zwłaszcza w kontekście znaczenia danych we współczesnej gospodarce.

Często słyszy się, że rynek pamięci masowych dla użytkowników korporacyjnych jest zabetonowany, aczkolwiek ostatnimi czasy ten beton zaczyna się kruszyć. Dzieje się tak nie tyle za sprawą nowych graczy, lecz konkurencyjnych technologii, takich jak software defined storage (SDS), systemy hiperkonwergentne czy architektura komponowalna. Poza tym dużą chrapkę na ten segment rynku mają dostawcy usług chmurowych. Liderzy rynkowi trzymają rękę na pulsie, bacznie śledząc konkurencję, a jednocześnie rozwijając swoje oferty. Nowe modele urządzeń już nie tylko składują i przetwarzają dane, ale oferują szerokie możliwości w zakresie ochrony informacji, w tym również przed atakami typu ransomware.

Warto też odnotować śmiałe ruchy nowej fali dostawców, takich jak Qumulo, Vast Data, czy WekaIO. Tym, co łączy wymienione firmy, jest wspólna dewiza – koniec z kompromisami pomiędzy wydajnością a pojemnością przetwarzanych danych, co

Fot. Adobe Stock

Zdaniem specjalisty

Łukasz Grzesiak, dyrektor BU Cloud, Arrow Electronics

Ostatnie kilka lat na rynku pamięci masowych upłynęło pod znakiem dominacji technologii flash. W pierwszych latach były to dyski SSD SAS, a obecnie szybko wzrasta znaczenie nośników NVMe. Użytkownicy biznesowi bardzo często pytają o takie funkcje jak deduplikacja czy kompresja. W cyfrowym świecie powstaje mnóstwo danych, dlatego klienci poszukują rozwiązań, które zapewnią nie tylko bezpieczne, ale również efektywne ich przechowywanie. Duże znaczenie mają też możliwości systemów w zakresie analizy informacji – kto z nich korzysta, kiedy, gdzie znajdują się dane, a także elastyczność zarządzania nimi i okres, w jakim producent wspiera dane rozwiązanie.

Grzegorz Korus, Senior System Engineer Servers & Storage, AB

Pod względem sprzedaży trend wzrostowy systemów all-flash utrzymuje się od wielu lat. Polska nie jest tu wyjątkiem. Udział all-flash w rynku macierzy SAN niezmiennie rośnie, a obecnie stanowi przeważającą jego część, zarówno jeśli weźmiemy pod uwagę liczbę sprzedawanych macierzy, jak i użytkową pojemność. Nie bez znaczenia jest fakt, iż macierze all-flash często mają mechanizmy deduplikacji i kompresji. Nabywcy systemów pamięci masowych mają różne wymagania i preferencje, lecz istnieje kilka wspólnych, o które często pytają. Należą do nich: wydajność, skalowalność, niezawodność, zarządzanie, zgodność i interoperacyjność oraz ochrona danych.

po części oznacza pożegnanie się z dyskami mechanicznymi.

Macierze dyskowe bez wodotrysków

Teoretycznie przyrost oraz rozproszenie danych powinny skłonić dostawców rozwiązań do wprowadzania innowacji, a odbiorców do wzrostu zainteresowania dostępnymi na rynku nowinkami. W praktyce bywa z tym różnie. O ile nie można narzekać na tych pierwszych, użytkownicy często bywają konserwatywni. Gal Naor, CEO i założyciel StorOne, przyznaje, że dla większości firm jedynym sposobem na poradzenie sobie z przyrostem danych jest zakup następnej macierzy. Nie myślą o wprowadzeniu nowego oprogramowania pozwalającego uporać się z problemami związanymi z wydajnością czy tworzeniem silosów w centrach danych. Jednak wśród dużych firm pojawia się nowy sposób myślenia, na co zwraca uwagę Ryan Farris, wiceprezes Qumulo.

– Ilość danych nieustrukturyzowanych podwaja się co 18–20 miesięcy, a nasi najwięksi klienci nie chcą rozmawiać o dokładaniu urządzeń – zaznacza Ryan Farris.

Z kolei rodzimi użytkownicy dążą do tego, aby zaoszczędzić jak najwięcej powierzchni dyskowej, dlatego często pytają o takie funkcje jak kompresja czy deduplikacja danych.

– Niektórzy producenci gwarantują odpowiedni współczynnik deduplikacji, a jeśli nie zostanie on osiągnięty, dokładają do urządzenia bezpłatnie dodatkowe dyski. Klienci w ostatnim czasie wykazują duże zainteresowanie replikacją synchroniczną oraz asynchroniczną na inną macierz lub do chmury publicznej – mówi Tomasz Spyra, CEO Rafcomu.

W dobie ataków ransomware duże znaczenie mają zabezpieczenia oferowane przez dostawców macierzy dyskowych. Nie lekceważą oni potrzeb użytkowników i wprowadzają ochronę on-line przed atakami bądź możliwość stworzenia odseparowanej trzeci kopii danych. Obie funkcje odgrywają kluczową rolę w przypadku współużytkowania danych, a więc systemów obsługujących pliki oraz obiekty. Część producentów rozwija rozwiązania poprzez kreowanie nowych funkcji i usług, często określanych jako „wodotryski".

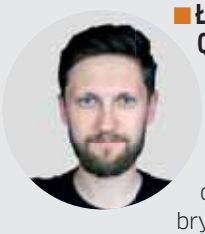
– Dla klientów ważne jest bezpieczne przechowywanie danych, wydajność oraz wysoka bezprzerwowa dostępność. Nie ma potrzeby wprowadzania dodatkowych rozwiązań, gdyż mogłyby one obniżyć poziom bezpieczeństwa i wydajności, a także zakłócić działanie kluczowych funkcji. Najlepiej w gestii macierzy pozostawić zadania, do których realizacji zostały stworzone, a całą resztę powierzyć oprogramowaniu aplikacyjnemu – tłumaczy Piotr Drąg, Storage Category & Data Services Business Development Manager w HPE.

SAN pod znakiem flash?

Na rynku dobrze radzą sobie macierze all-flash, których sprzedaż według IDC zwiększyła się o 4,4 proc. w ujęciu rocznym. Pod względem wartościowym do tej grupy produktów należy już 50,4 proc. całego rynku zewnętrznych macierzy dyskowych, który wzrósł zaledwie o jeden procent. Nie mniej interesująco wyglądają dane Gartnera dotyczące dostarczonej pojemności pamięci all-flash. W pierwszym kwartale bieżącego roku stanowiła ona 31 proc. całkowitej ➤

Przemysław Biel, Sales Channel Manager Poland, Synology

Co jakiś czas pojawiają się głosy o końcu dysków mechanicznych. W mojej opinii te nośniki pozostaną z nami jeszcze przez chwilę, przy czym ich zastosowanie może się zmieniać wraz z upływem czasu. W nieodległej przyszłości będą wykorzystywane wszędzie tam, gdzie istnieje zapotrzebowanie na dużą pojemność, przy jednoczesnym zachowaniu niskich kosztów magazynowania danych. Wraz z takimi funkcjami nowoczesnych systemów NAS, jak obsługa W.O.R.M. czy niemodyfikowalnych migawek, dyski obrotowe mogą być świetnym miejscem na archiwizację danych i ochronę przed atakami ransomware.



Łukasz Milic, Business Development Representative, QNAP

Dla wielu klientów, którzy poszukują rozwiązań do przechowywania danych, chmura publiczna jawi się jako potencjalna odpowiedź na ich potrzeby. Jednak zwykle używana jest jako przestrzeń dodatkowa wobec firmowych NAS-ów. Model hybrydowy zapewnia dużą przestrzeń lokalną, gdzie nie ma opóźnień, a także zapasową, zdalną lokalizację danych w chmurze. Nie zmienia to faktu, iż chmura publiczna jest problematyczna dla wielu klientów ze względu na niejasne mechanizmy naliczania opłat oraz opóźnienia wynikające ze słabszych łączy. Jeśli chodzi o wybór dostawcy, preferencje klientów są oczywiście zróżnicowane. Najważniejsze jest to, aby dane były przechowywane w ramach Europejskiego Obszaru Gospodarczego i zgodnie z wymogami RODO.

powierzchni dyskowej sprzedanej w tym okresie, zaś rok wcześniej tylko 16,8 proc.

Wśród dostawców all-flash niekwestionowanym liderem jest Dell (790 mln dol.), a drugą pozycję zajmuje NetApp z dość dużą stratą wobec lidera (415 mld dol.). Przy czym dystans między nimi się powiększa. Dell zwiększył wartość sprzedaży aż o 17 proc. w ujęciu rocznym, takim samym wzrostem może pochwalić się HPE. NetApp zaliczył dość spektakularny spadek, jego udział w globalnym rynku systemów all-flash w ciągu roku skurczył się z 22 proc. do 16 proc.

– *Popyt na macierze SAN generują głównie aplikacje transakcyjne wymagające minimalnych opóźnień. Firmy poszukujące produktów w tym segmencie preferują rozwiązania cechujące się wysoką wydajnością i szerokimi możliwości w zakresie redukcji objętości danych* – mówi Radosław Piedziuk, Unstructured Data Solutions Sales Manager w Dell Technologies.

W czerwcu jeden z producentów macierzy all-flash przedstawił dość śmiałą prognozę, iż od 2028 r. nie będą już sprzedawane nowe dyski mechaniczne, które całkowicie zostaną zastąpione pamięciami all-flash. O ile w przypadku nośników dla komputerów to bardzo prawdopodobny scenariusz, o tyle w przypadku macierzy dyskowych i serwerów stosowanych w centrach danych sytuacja jest dużo bardziej złożona. Za wykorzystaniem HDD przemawiają przede wszystkim dwa argumenty: niższa cena oraz dłuższa żywotność. Jednak postęp technologiczny, a także brak ruchomych części, sprawiają, że nośniki flash mają mniejszą awaryjność niż „twardziele", co pozwala zrekompensować jedną z największych wad SSD, czyli ograniczoną liczbę operacji zapisu.

Niemniej cena nadal pozostaje silnym atutem HDD. W rozwiązaniach dla centrów danych najpopularniejsze są bardzo pojemne dyski nearline (7400 obr./min., 3,5 cala), których cena za 1 GB wynosi 0,019 dol., podczas gdy dla nośnika flash NAND przeznaczonego do pracy w serwerowniach jest to 0,2 USD za 1 GB. Jak widać różnica jest dziesięciokrotna, aczkolwiek technologia QLC (4 bity na komórkę) oraz ciągły wzrost liczby warstw (rekordzista SK Hynix latem rozpoczął produkcję 238-warstwowej pamięci 4D NAND flash), sprawiają, że ceny SSD powinny dość szybko topnieć. Z drugiej strony producenci HDD nie zasypiają gruszek w popiele, koncentrując działania na optymalizowaniu pod kątem zwiększania ich pojemności, co najlepiej pokazują takie technologie jak SMR, czy pojawiająca się na horyzoncie HAMR.

Do macierzy all-flash należy już ponad połowa rynku.

– *Prognozy dotyczące dalszych losów HDD zweryfikuje rynek, jako punkt przecięcia popytu zgłaszanego przez klientów i możliwości po stronie podaży. Istotnymi czynnikami, które wpłyną na ten trend, będzie rynek aplikacji oraz możliwości obsługi danych przez nowe narzędzia* – przyznaje Radosław Piedziuk.

NAS zmierza w kierunku scale out

Działy biznesowe coraz częściej zgłaszają zapotrzebowanie na systemy pozwalające przechowywać miliony plików o pojemności liczonej w petabajtach. To dopiero początek tego zjawiska, ale Internet Rzeczy czy generatywna sztuczna inteligencja będą w najbliższych latach napędzać popyt na wielkie repozytoria danych.

Szczególnie ciekawe perspektywy rysują się ponadto przed serwerami NAS typu scale out, umożliwiającymi dołączenie do serwera NAS kolejnych urządzeń i objęcie tej grupy wspólnym systemem plików.

– *Liczba danych nieustrukturyzowanych rośnie w tempie wykładniczym. Najlepiej magazynować je na rozproszonych systemach NAS. Firmy coraz częściej wykorzystują nie tylko klasyczne systemy plikowe bazujące na protokołach SMB czy NFS, ale także macierze obiektowe używające do komunikacji protokołu S3* – zauważa Piotr Drąg.

Architektura scale out stanowi odpowiedź na potrzeby analityki, przepisów obligujących do długoterminowej archiwizacji dokumentacji w wersji elektronicznej czy mediów tworzących materiały w coraz wyższych rozdzielczościach. Trudno tutaj spodziewać się dominacji rozwiązań naszpikowanych nośnikami SSD, choć dostawcy systemów scale out takowe oferują.

– *Wiele macierzy dyskowych używa twardych dysków do archiwizacji danych bądź ich zabezpieczenia. W takich scenariuszach pojemność często liczy się nie w terabajtach, lecz w petabajtach. Dlatego bardzo istotny jest tutaj koszt składowania zasobów. Przy obecnych cenach wciąż bardziej opłacalne jest użycie dysków mechanicznych, tym bardziej, że w systemach archiwizacyjnych wydajność nie jest najważniejszym kryterium wyboru* – wyjaśnia Tomasz Spyra.

Nadal dużą popularnością cieszą się klasyczne serwery NAS scale up oferowane między innymi przez QNAP i Synology. Klienci tych firm wciąż preferują dyski mechaniczne, a najbardziej istotna staje się dla nich kwestia możliwości rozbudowy urządzeń o dodatkowe nośniki. Obaj vendorzy bardzo poważnie podchodzą do kwestii związanych ze skalowaniem systemów. Synology planuje rozpocząć w trzecim kwartale sprzedaż systemów NAS scale out, zaś QNAP zacieśnia współpracę z Seagate'em, która ma zaowocować urządzeniami obsługującymi przestrzeń dyskową rzędu kilku petabajtów. ■

Zdaniem integratora

Jacek Marynowski, prezes, Storage IT

Jak na razie systemy NAS typu scale up zaspokajają potrzeby obsługiwanych przez nas firm, ale docelowo to rozwiązania scale out będą miały istotny udział w naszej sprzedaży. Klienci najczęściej pytają o bezpieczeństwo przechowywania danych i możliwość szybkiego przywrócenia pracy w wypadku awarii czy cyberataku. Ważne są też dla nich opcje SLA dla wybieranych urządzeń. Natomiast zauważamy zainteresowanie zakupem urządzeń w modelu usługowym. W mojej ocenie firmy i podmioty sektora publicznego nie są jeszcze gotowe na płacenie za tego typu usługi. Jednak w dość bliskiej perspektywie czasowej może to być istotny trend. Niestety, tego typu usługi będą mogli zaoferować jedynie duzi gracze.

Dyski Western Digital

gotowe na wyzwania

W bogatej ofercie Western Digital można znaleźć nośniki przystosowane do pracy w wielu różnych rozwiązaniach IT – zarówno w profesjonalnych stacjach roboczych, jak i serwerach, urządzeniach NAS, a także w rejestratorach monitoringu wideo.

Wybór odpowiednich twardych dysków na potrzeby różnych rozwiązań jest kluczowy w kontekście optymalnej wydajności, niezawodności oraz ciągłości dostępu do danych. Już od ponad 10 lat na rynku dostępne są modele mechanicznych napędów oraz pamięci flash, które zostały specjalnie zaprojektowane pod kątem charakterystyki gromadzonych w nich danych. Wzięto w nich pod uwagę takie kryteria, jak proporcja liczby operacji zapisu do operacji odczytu, ilość przetwarzanych danych w ciągu doby, czy też częstotliwość dostępu do nich.

Czerwono w serwerach NAS...

Serwery NAS są wykorzystywane do przechowywania dużej ilości ważnych firmowych plików i obrazów maszyn wirtualnych oraz udostępniania ich w sieci. Zazwyczaj jest to macierz RAID, w której zainstalowanych jest kilka lub kilkanaście nośników. Jeśli są to mechaniczne twarde dyski, powinny być zoptymalizowane pod kątem ciągłej pracy pod dużym obciążeniem oraz odporne na charakterystyczne dla wielodyskowych macierzy RAID wibracje.

Do instalacji w serwerach NAS zaprojektowane zostały 3,5-calowe dyski z rodziny **WD Red**. Jednym z ich kluczowych wyróżników jest wbudowany zestaw zaawansowanych funkcji NASware, które mają na celu poprawę wydajności, niezawodności i zgodności z różnymi systemami NAS dostępnymi na rynku, a także gwarantują poprawny przebieg procesu aktualizacji firmware'u napędu.

Dyski WD Red są dostępne w trzech podrodzinach. Podstawowe modele o tej samej nazwie przeznaczone są do użytku w niewielkich serwerach NAS (do 4 napędów) o małym obciążeniu. Zapewniają one od 2 do 6 TB pojemności, prędkość obrotową 5400 rpm oraz cache 256 MB. Objęte są trzyletnią gwarancją, a ich wytrzymałość mechaniczna obliczona jest na zapis/odczyt 180 TB danych rocznie. Dyski z podrodziny **WD Red Plus** mają podobne parametry, ale dostępne są w większych pojemnościach (do 14 TB) i są przystosowane do pracy w systemach NAS zawierających do 8 napędów.

Do najbardziej zaawansowanych zastosowań dostępne są dyski **WD Red Pro** o pojemności od 2 do 22 TB, prędkości obrotowej 7200 rpm i pamięci cache 256 MB. Są przystosowane do pracy w macierzach zawierających maksymalnie 24 nośniki i umożliwiają zapis/odczyt do 300 TB danych rocznie. Mają też rozszerzoną do 5 lat gwarancję.

Ofertę mechanicznych twardych dysków dla serwerów NAS uzupełniają przystosowane do całodobowej pracy pamięci SSD z rodziny **WD Red SA500**. Dostępne są w 2,5-calowej obudowie z interfejsem SATA (pojemność od 500 GB do 4 TB) oraz w postaci modułu M.2 2280 o pojemności od 500 GB do 2 TB.

...a purpurowo w systemach monitoringu

Systemy cyfrowego monitoringu i nadzoru, szczególnie te używane w miejscach o dużym natężeniu ruchu, generują duże ilości danych w krótkim czasie. Aby zagwarantować ciągłość zapisu oraz minimalizować opóźnienia, gdy zajdzie konieczność równoległego odczytu danych, niezbędne jest zastosowanie dysków zoptymalizowanych do obsługi wielu strumieni danych jednocześnie, co sprawia, że są bardziej wydajne w środowiskach CCTV.

Do instalacji w systemach cyfrowego monitoringu przystosowane są 3,5-calowe dyski **WD Purple**. Zapewniają od 500 GB do 14 TB pojemności, 64-512 MB pamięci cache i roczny zapis/odczyt do 180 TB danych. Modele z podrodziny **WD Purple Pro** są dostępne w szerszym zakresie pojemności (8–22 TB) oraz dzięki wzmocnionej konstrukcji umożliwiają zapis/odczyt do 550 TB danych rocznie. Są także wyposażone w funkcję Western Digital Device Analytics (WDDA) zapewniającą zarządzanie stanem dysku w kompatybilnych rejestratorach wideo.

W dyskach WD Purple zastosowano mechanizm AllFrame, który redukuje zjawisko utraty klatek, poprawia jakość odtwarzania wideo i pozwala nie tylko na jednoczesne nagrywanie nawet 64 strumieni wideo w rozdzielczości HD, ale także na analizowanie do 32 strumieni na dysk w jednym systemie.

Western Digital ma również w portfolio karty pamięci microSDHC **WD Purple SC QD101** o pojemności od 32 GB do 1 TB. Zastosowano w nich specjalne układy 3D NAND o zwiększonej trwałości, co gwarantuje niezawodną pracę tych kart po włożeniu bezpośrednio do kamer cyfrowego nadzoru bądź rejestratorów wideo.

Dystrybutorami dysków WD w Polsce są: AB, Action, Also, Elko, Incom i Tech Data.

Western Digital

Dodatkowe informacje:
Marcin Pączko, Enterprise & Devices Country Manager East Europe & CIS, Western Digital
marcin.paczko@wdc.com

Trwałość niejedno ma imię

Użytkownicy dysków SSD powinni zapoznać się z nowymi parametrami związanymi z trwałością komórek pamięci flash, aby uniknąć nieporozumień podczas wybierania odpowiedniego nośnika do różnych zastosowań.

Nowy dysk SSD firmy Kingston – DC600M – jest przeznaczony do instalacji w serwerach o zróżnicowanym poziomie obciążenia. Dzięki parametrowi DWPD wynoszącemu 1 przy 5-letniej gwarancji (1,66 przy 3-letniej gwarancji) nośnik ten idealnie nadaje się do pracy w klasycznych serwerowniach, centrach danych oraz u dostawców usług chmurowych.

Komórki pamięci w stosowanych w dyskach SSD układach flash NAND zużywają się przy każdej operacji zapisu (odczyt jest „za darmo"). Można to porównać z pisaniem po kartce papieru ołówkiem i ciągłym wycieraniu tekstu gumką. Każdy szanujący się producent podaje w specyfikacji swoich dysków parametry, które pozwalają oszacować, ile danych będzie można zapisać na nośniku w trakcie obowiązującej gwarancji.

Sam proces zapisu w pamięciach flash jest skomplikowany z technicznego punktu widzenia: komórka musi być pusta, więc wcześniej czasem trzeba ją oczyścić. Gdy w komórce jest zapisanych mniej danych niż może ona pomieścić, dochodzi do marnowania cennej przestrzeni. Dlatego konieczna jest optymalizacja tego procesu, o co dba wbudowany w dysk SSD kontroler, którego praca polega na umiejętnym równomiernym rozproszeniu danych w komórkach kości pamięci.

Ile danych można zapisać?

Wśród dostawców dysków SSD przyjęły się dwa parametry, które określają ich trwałość. **Total Bytes Written (TBW)** to łączna ilość danych podawana w terabajtach lub petabajtach, którą można zapisać na dysku bez narażania ich na utratę. Dzieląc wartość tego parametru przez pojemność dysku otrzymuje się liczbę cykli zapisu dla każdej z komórek pamięci. W dyskach klasy konsumenckiej wartość ta wynosi około 600, zaś w dyskach o wzmocnionej trwałości – od 1000 do 1200. W nośnikach przeznaczonych do instalacji w serwerach wartość ta przekracza 1800.

– *Wartość oscylująca wokół tysiąca cykli zapisu wygląda na niewielką, ale w praktyce klienci bardzo rzadko dokonują zapisu takiej ilości danych. Jedynie w bardzo specyficznych sytuacjach może dojść do nadmiernej eksploatacji dysku SSD. Przy normalnym użyciu taki problem praktycznie nigdy się nie zdarza* – mówi Robert Sepeta, Business Development Manager w Kingston Technology.

Istnieje też drugi parametr, który obrazuje trwałość nośników SSD – można go zresztą wyliczyć na bazie TBW, korzystając z powszechnie dostępnych wzorów. Chodzi o **Drive Writes Per Day (DWPD)**, czyli współczynnik określający, ile razy dziennie można dokonać zapisu pełnej pojemności dysku w trakcie trwania okresu gwarancyjnego. Dla dysków konsumenckich wartość ta oscyluje wokół 0,3, dla dysków serwerowych – 1. Tylko w przypadku nośników przeznaczonych do zastosowania w środowiskach o wyjątkowo dużym obciążeniu (np. w systemach transakcyjnych) czasami stosowane są dyski o parametrze DWPD wynoszącym 3.

Co wybrać?

Dobór odpowiedniego dysku SSD powinien być bezpośrednio uzależniony od charakteru przetwarzanych przez klienta danych, z naciskiem na częstotliwość zapisu i ich objętość. Znając te wartości należy oszacować parametry TBW oraz DWPD, a następnie porównać z nośnikami dostępnymi na rynku.

– *Często okazuje się, że nawet w przypadku zaawansowanych profesjonalnych zastosowań osiągany parametr DWPD wynosi jedynie 0,1 lub mniej. Może to skusić klienta do wyboru dysku konsumenckiego, przestrzegam jednak przed popełnieniem tego błędu. Trwałość to jeden aspekt, ważna jest też konstrukcja kontrolera dysku SSD, który w przypadku nośników przystosowanych do pracy w serwerach i zaawansowanych rozwiązaniach jest szybszy i wyposażony w dodatkowe algorytmy minimalizujące ryzyko wystąpienia błędu w zapisywanych danych* – podkreśla Robert Sepeta.

Na koniec warto wspomnieć o jeszcze jednym fakcie, dość mało znanym wśród użytkowników. Otóż również twarde dyski mają określoną maksymalną objętość zapisywanych danych, która częściowo wynika z ograniczonej wytrzymałości mechanicznej. Standardowo w dyskach do pecetów można zapisać „tylko" 55 TB/rok, zaś w przypadku modeli do zastosowań serwerowych wartość ta wynosi kilkaset terabajtów rocznie. Oznacza to, że w przypadku dysku 10 TB pełnego skasowania i ponownego zapisania można dokonać co kilka dni i przez dziesiątki lat dla klientów było to zupełnie wystarczające. Tymczasem dysponując nowoczesnymi dyskami SSD klasy enterprise, taką operację można wykonywać codziennie.

Autoryzowanymi dystrybutorami produktów Kingstona w Polsce są: AB, Action, Also, Asbis, Ingram Micro i Tech Data.

Dodatkowe informacje:
Robert Sepeta,
Business Development Manager, Kingston Technology
rsepeta@kingston.eu

InfiniBox – macierz o olbrzymiej skalowalności

Zaawansowane funkcje optymalizacji i autonomicznego zarządzania danymi, obecne w stworzonym przez firmę Infinidat rozwiązaniu InfiniBox, umożliwiają przechowywanie dużej ilości informacji w jednym miejscu, minimalizując jednocześnie ryzyko awarii i utraty danych.

Firma Infinidat zdobyła uznanie użytkowników oraz wiele nagród dzięki innowacyjnemu podejściu do składowania informacji. Stworzyła unikalne, wydajne, niezawodne, skalowalne i bezpieczne rozwiązanie klasy korporacyjnej do przechowywania ogromnych ilości danych oraz efektywnego i prostego zarządzania nimi.

Obecnie w ofercie Infinidat znajdują się macierze dyskowe **InfiniBox** (w tym wersja all-flash – SSA), a także nowatorskie rozwiązanie **InfiniGuard** do backupu i przywracania środowisk do pracy po awarii. Macierze InfiniBox zapewniają fizyczną pojemność od 250 TB do 6,9 PB (dzięki technikom optymalizacji możliwe jest przechowywanie danych o objętości do 17,28 PB) oraz do 368 TB pamięci flash cache. Ich wydajność sięga 2 mln operacji wejścia-wyjścia na sekundę (IOPS), zaś przepustowość – 25 GB/s (w przypadku macierzy SSA jest to 38 GB/s oraz wewnętrzne opóźnienie poniżej 1 milisekundy). Taka wydajność jest zapewniona we wszystkich produktach zarówno dla obsługi plików i bloków.

Logiczna skalowalność tych macierzy jest tak duża, że zaspokaja potrzeby większości przedsiębiorstw na rynku. Maksymalna wielkość jednego pliku to 1 petabajt. Istnieje bardzo wysoki limit co do liczby woluminów oraz rozmiaru systemu plików – rozwiązanie może przechowywać do 17 mld plików, 100 tys. kopii migawkowych oraz 4 tys. systemów plików.

Siła w oprogramowaniu

Konkurencyjnym wyróżnikiem rozwiązania InfiniBox jest stworzony w modelu software-defined storage system operacyjny **InfuzeOS** o unikalnej funkcjonalności. Nawet gdy pojemność macierzy rozbudowana jest do wielu petabajtów, gwarantuje ona bardzo wysoką skalowalność, dostępność, wydajność oraz odporność na cyfrowe zagrożenia. Funkcje są dostępne poprzez przyjazny dla użytkownika, czytelny interfejs, wyposażony w mechanizmy umożliwiające zautomatyzowaną obsługę, bez konieczności prowadzenia zaawansowanych działań administracyjnych.

Wysoka wydajność macierzy InfiniBox została zapewniona dzięki opatentowanej przez Infinidat funkcji **Neural Cache**. Wbudowane inteligentne mechanizmy uczenia maszynowego analizują wzorce dostępu do danych, a następnie wykorzystują zdobytą wiedzę do buforowania ich w pamięci cache. W ten sposób optymalizowany jest współczynnik trafień – dzięki skuteczności funkcji Neural Cache wynosi on ponad 90 proc.

W system InfuzeOS wbudowany jest też mechanizm **Active/Active Data Mobility (AADM)** umożliwiający bezproblemową synchroniczną replikację danych pomiędzy macierzami Infinidat. Rozwiązanie to jest szczególnie przydatne w sytuacji, gdy konieczne jest równoważenie obciążenia macierzy, wdrożenie do infrastruktury nowych rozwiązań lub konserwacja sprzętu. Dostępna jest też replikacja asynchroniczna, która zapewnia wiele poziomów skalowalności, elastyczność obsługi oraz ochronę infrastruktury przechowywania danych, a także ciągłość jej pracy.

Kolejnym interesującym rozwiązaniem w systemie InfuzeOS jest opatentowany mechanizm **InfiniRAID**. Proces zabezpieczania danych przed utratą w wyniku awarii dysków jest w nim realizowany w unikalny sposób, bazujący na równoważeniu obciążenia pomiędzy dyskami. W InfiniRAID oddzielono strukturę danych od warstwy fizycznej i wykorzystano tysiące wirtualnych grup RAID zawierających redundantne bloki informacji. Są one rozprowadzane na wszystkich dyskach, co zapobiega powstawaniu hotspotów oraz gwarantuje stuprocentowe szybkie odzyskiwanie danych z każdego uszkodzonego dysku.

Istotnym wyróżnikiem jest też funkcja **InfiniSafe**, gwarantująca bezpieczeństwo danych i odporność na cyfrowe ataki. Jest realizowana między innymi poprzez logiczną separację danych, lokalne oraz zdalne niemodyfikowalne kopie migawkowe, gwarantowane, niemal natychmiastowe przywracanie środowisk i inne mechanizmy. Wszystko to bez wpływu na wydajność macierzy. W maju 2023 r. udostępniona została funkcja **InfiniSafe Cyber Detection**, która zapewnia skanowanie woluminów, plików, bloków, maszyn wirtualnych oraz kopii migawkowych w poszukiwaniu złośliwego kodu, w tym ransomware.

INFINIDAT

Dodatkowe informacje:
Noa Beit-On,
Regional Sales Manager, Central & Eastern Europe, Infinidat
nbeiton@infinidat.com

MATERIAŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ INFINIDAT.

Obecnie wszystko i wszyscy są podejrzani

Następuje zmiana paradygmatu, w wyniku której zaufanie do kogokolwiek czy czegokolwiek w kontekście cyberbezpieczeństwa powinno stać się... zerowe. Także w odniesieniu do sztucznej inteligencji.

Tomasz Janoś

Zazwyczaj do ogromnych strat powodowanych przez wewnętrzne zagrożenia dochodzi dlatego, że ich źródłem jest ktoś, kogo obdarzono jakimś rodzajem zaufania. Mogą być to zarówno niefrasobliwi pracownicy, którzy nawet nie wiedzą, że narażają firmę na ryzyko, jak i świadomi swoich złośliwych celów cyberprzestępcy. Istniejące w obrębie firmy zagrożenie może stwarzać każdy, kto ma dostęp do wrażliwych danych lub procesów: pracownicy, konsultanci, dostawcy, a zdarza się, że i klienci.

Jednym z najczęstszych scenariuszy jest nieumyślne doprowadzenie przez pracownika do wycieku firmowych informacji. Przykładowo, może do tego dojść przez pozostawienie laptopa bez nadzoru w miejscu publicznym. Podobnie pomyłka w wysyłce mejla może spowodować, że poufne informacje trafią do nieuprawnionych odbiorców. Innym rodzajem wewnętrznego zagrożenia są zwalniani pracownicy, którzy dążą do zemsty albo uzyskania osobistych korzyści. Wreszcie, cyberprzestępcy mogą wykorzystać uważane za zaufane konta i aplikacje zewnętrznych podmiotów, aby ukraść dane lub dokonać sabotażu w systemach informatycznych.

> Samo wdrożenie ZTNA **to za mało.**

Wobec tak wielu różnych zagrożeń wewnętrznych dużego znaczenia nabiera posiadanie solidnych zabezpieczeń, szkolenie pracowników w zakresie świadomości zagrożeń oraz wprowadzenie rygorystycznej polityki w celu minimalizacji ryzyka i ochrony wrażliwych danych. A przede wszystkim, zmiana paradygmatu, w wyniku której zaufanie do kogokolwiek czy czegokolwiek w kontekście cyberbezpieczeństwa po prostu zniknie.

Zero Trust – nie ufaj, sprawdzaj

O mechanizmie Zero Trust zrobiło się szczególnie głośno podczas pandemii, w trakcie której pojawiła się pilna potrzeba zabezpieczania komputerów zdalnych pracowników. Pandemia się skończyła, ale nie znikła konieczność tego rodzaju ochrony firmowej sieci, której wyraźne dotychczas granice zaczęły się zacierać. ZTNA stał się niezbędny przede wszystkim ze względu na ewolucję w sposobie pracy i rozwój rozwiązań IT.

Chociaż skutki pandemii odcisnęły swoje lokalne piętno, dominującym czynnikiem jest wiele globalnych, nasilających się zmian. Wojciech Wąsik, Chief Digital & Information Security Officer w Transition Technologies PSC, wyróżnia trzy.

Pierwszą jest **popularyzacja pracy zdalnej**. W różnych jej formach, począwszy od wykorzystania wielu urządzeń w różnych lokalizacjach geograficznych i porach dnia, przez model BYOD i trend zatrudniania pracowników rozsianych po całym świecie, aż do freelancerskiego modelu pozyskiwania siły roboczej (gig economy). Istnieje jeden wspólny mianownik dla każdego z tych przypadków: potrzeba całodobowego zapewnienia szybkiego dostępu do usług i narzędzi na wielu urządzeniach. Klasyczny VPN radzi sobie znacznie gorzej w tak zmiennym i charakteryzującym się dużą elastycznością środowisku.

– *Główną przewagą ZTNA jest koncentracja na tożsamości, a nie na sieci, jak też granularna definicja reguł dostępu do aplikacji oraz izolacja sieci od usług, w ramach której sieć pozostaje „ukryta" przed jej użytkownikami. Te czynniki pozwalają skupić się znacznie bardziej na modelu biznesowym, a nie na technikaliach związanych z infrastrukturą. Oczywiście one nie znikają, ale zostają silniej odseparowane od użytkownika końcowego* – tłumaczy Wojciech Wąsik.

Drugą kluczową zmianą jest **rosnąca popularność chmury**. Nawet jeśli nie wszędzie ten proces przebiega w takim samym tempie, to faktem jest, że przybywa firm zarówno częściowo korzystających z chmury, jak i tych, które całkowicie przełączyły się na podejście cloud-first i często nie posiadają własnej infrastruktury. ZTNA natywnie działa w środowisku chmurowym, dlatego zastosowanie takiego podejścia ma szczególne znaczenie w kontekście uruchamiania nowych usług chmurowych, integracji pomiędzy nimi oraz zabezpieczania dostępu do nich. Co więcej, zważywszy na to, że ZTNA nie wymaga skalowania infrastruktury, umożliwia również łatwiejsze skalowanie samych firm korzystających głównie z usług chmurowych (upraszcza dodawanie użytkowników, urządzeń końcowych, tworzenie nowych grup, zarządzanie aplikacjami

i usługami oraz wdrażanie reguł polityki bezpieczeństwa).

– *W takiej konfiguracji zasoby w infrastrukturze on-premise stanowią jedno ze źródeł usług i danych, a nie centralny punkt komunikacji z firmą* – zauważa specjalista Transition Technologies PSC.

Trzecia zasadnicza zmiana dotyczy **bezpieczeństwa**. Podejście polegające jedynie na uszczelnianiu granicy sieci od lat nie jest postrzegane jako dostatecznie bezpieczne. Jednym z problemów jest udzielenie dostępu do sieci dla użytkownika, którego urządzenie jest skompromitowane, co stanowi realne i trudne do wykrycia zagrożenie dla przedsiębiorstwa. Paradygmat separacji dostępu do sieci i do aplikacji stanowiący fundament ZTNA oraz wielopunktowa weryfikacja (poświadczenia, stan urządzenia, uprawnienia, zachowanie) stanowi o klasę lepsze zabezpieczenie przed atakami, w tym typu ransomware.

– *Co więcej, ZTNA domyślnie stosuje zasadę najmniejszych uprawnień oraz znacząco ułatwia utrzymanie polityki, konfiguracji czy certyfikatów, co eliminuje wiele słabych punktów klasycznego podejścia bazującego na VPN* – podsumowuje Wojciech Wąsik.

Warto wspomnieć, że ZTNA to jedna z pięciu kluczowych funkcji SASE (Secure Access Service Edge), czyli „bezpiecznego dostępu do usług brzegowych". Pozostałe to: sieć rozległa SD-WAN (Software-Defined WAN), brama SGW (Secure Web Gateway, broker CASB (Cloud Access Security Broker) oraz zapora nowej generacji NGFW (Next-Gen Firewall). Ponieważ ➤

Dlaczego szyfrowanie jest takie ważne?

Szyfrowanie to proces przekształcania danych w kod, który tylko upoważnione strony mogą odczytać i uzyskać dostęp do informacji. Dlatego szyfrowanie chroni dane przed nieautoryzowanym dostępem, modyfikacją czy kradzieżą, bez względu na to, czy są one przechowywane na urządzeniu, przesyłane przez sieć czy przetwarzane przez aplikację. Pomaga również w spełnianiu wymogów prawa, w tym regulacji dotyczących ochrony danych, takich jak RODO czy HIPAA, które wymagają zapewnienia prywatności i bezpieczeństwa danych osobowych. Czym powinny cechować się efektywne narzędzia do szyfrowania? Różne ankiety i badania, takie jak przeprowadzone przez Ponemon Institute „Global Encryption Trends Study Survey", pokazują jakie cechy firmowych systemów do szyfrowania danych są uważane przez ich użytkowników za najbardziej istotne.

Szyfrowanie może chronić dane nie tylko w ramach obiegu informacji, ale także już po wycofaniu z użytku ich nośników. Alternatywną metodą dla kogoś, kto pozbywa się dysków, są usługi bezpiecznego niszczenia danych. W tym obszarze stosowane są dwa podejścia. Jednym jest skuteczne niszczenie nośników, a drugim specjalistyczne kasowanie danych. Ten drugi przypadek daje możliwość ponownego wprowadzenia sprzętu na rynek. To do klienta należy wybór – czy programowo usunąć dane (co może być lepsze dla środowiska naturalnego), czy raczej postawić na fizyczne ich zniszczenie (jeśli ma to zapewnić większy spokój zlecającemu).

1 Wydajność – firmy cenią sobie dużą wydajność i małe opóźnienia systemu do szyfrowania danych. Nie powinno to dziwić, jeśli szyfrowanie ma być kluczowe w ochronie dużej ilości danych.

2 Egzekwowanie reguł polityki bezpieczeństwa – wybrana metoda szyfrowania powinna współgrać z polityką bezpieczeństwa danej firmy. W przeciwnym razie może dochodzić do zakłóceń, a rozwiązywanie niezgodności, w tym w zarządzaniu kluczami, będzie wymagać dodatkowego czasu i pieniędzy.

3 Wsparcie dla wdrażania on-premise i w chmurze – firmy muszą obecnie zabezpieczać dane używane zarówno w aplikacjach chmurowych, jak i lokalnych. Dlatego niezbędne staje się znalezienie rozwiązania do szyfrowania, które można zastosować w hybrydowych środowiskach.

4 Zarządzanie kluczami – bezpieczne zarządzanie kluczami kryptograficznymi to podstawa w ochronie wrażliwych i poufnych danych. Szyfrowanie nie ma sensu, jeśli klucze nie są odpowiednio chronione przed nieuprawnionym dostępem.

5 Możliwość integracji z innymi narzędziami bezpieczeństwa – łatwa integracja oszczędza czas, pieniądze i wysiłek, które w przeciwnym razie trzeba byłoby poświęcić na próby dopasowania rozwiązania do szyfrowania do kluczowych narzędzi bezpieczeństwa, jak SIEM i zarządzanie tożsamością.

Fot. Adobe Stock

zwiększa się zainteresowanie możliwością uzyskania bezpiecznego zdalnego dostępu do aplikacji, bez względu na to skąd one są uruchamiane i gdzie znajduje się użytkownik, rośnie liczba dostawców oferujących SASE na rynku, a więc i możliwości ich partnerów w docieraniu do klientów.

Wielowarstwowa ochrona i monitorowanie

W miarę rozwoju pracy zdalnej i hybrydowych środowisk wielochmurowych, kluczowa staje się wspomniana strategia Zero Trust, która ogranicza dostęp i wymaga kontekstowego uwierzytelniania. Także klasyfikacja danych, mechanizmy ich retencji oraz szyfrowanie (włącznie z pełnym szyfrowaniem homomorficznym), zwiększają widzialność i chronią przed naruszeniami.

Wyciekom danych będzie zapobiegać wprost wdrożenie mechanizmów kontroli DLP (Data Loss Prevention) – na poziomie sieci, w urządzeniach końcowych oraz poczcie elektronicznej. Kontrola dostępu do sieci w postaci systemu NAC (Network Access Control) dodatkowo ograniczy nieautoryzowane połączenia. Wewnętrzne zagrożenia ograniczy również poprzedzone klasyfikacją danych wprowadzenie dostępu do zasobów na podstawie profili.

Wiele warstw zabezpieczeń zapewni wszechstronną ochronę przed potencjalnymi zagrożeniami i podniesie ogólny poziom cyberbezpieczeństwa w firmie. Do lepszego wykrywania i ograniczania naruszeń prowadzi także stworzenie ram wewnętrznych audytów, oceny ryzyka oraz zachowania zgodności z regulacjami. W zapewnianiu bezpieczeństwa danym przedsiębiorstwa muszą przyjąć nowoczesne strategie, obejmujące zarządzanie dostępem uprzywilejowanym (PAM), zarządzanie aplikacjami na urządzeniach końcowych, podejście Zero Trust, zwiększone bezpieczeństwo chmury, szyfrowanie informacji oraz rozwiązania ochronne typu XDR (Extended Detection and Response).

Z kolei wdrożenie solidnych systemów monitorowania umożliwi wykrywanie podejrzanych działań, a także otrzymywanie w czasie rzeczywistym alertów dotyczących potencjalnych zagrożeń. Dodatkowo, kluczowe dla szybkiej neutralizacji zagrożeń oraz minimalizowania potencjalnych szkód, będzie opracowanie dobrze zdefiniowanego planu reagowania na incydenty.

Ostrożnie ze sztuczną inteligencją

Eksperci z zespołu CERT-EU zwracają uwagę, że coraz częstsze wykorzystanie ogólnie dostępnych, zamkniętych modeli językowych AI, takich jak ChatGPT, niesie ze sobą potencjalne ryzyko dla wrażliwych danych podawanych w zapytaniach użytkowników. Poszukując pomocy lub odpowiedzi mogą oni podczas interakcji z modelem w sposób nieświadomy wprowadzić poufne dane lub możliwe do zidentyfikowania informacje osobiste.

> Wyraźne do tej pory **granice firmowych sieci** zaczęły się zacierać.

Tego typu dane są zazwyczaj przechowywane w celu przetworzenia i wygenerowania odpowiedzi, istnieje ryzyko, że mogą zostać ujawnione, zarówno w przypadku udanego ataku, jak i podczas szkolenia przyszłych iteracji AI. Eksperci przestrzegają, że bez zastosowania odpowiednich środków anonimizacji danych oraz ochrony prywatności, w posiadanie takich informacji mogą wejść nieautoryzowane podmioty, co może prowadzić do kradzieży tożsamości, oszustw finansowych lub szkód reputacyjnych zarówno dla firmy, jak i osób fizycznych.

Także w przypadku cyberataku na infrastrukturę modelu językowego AI istnieje znaczne ryzyko związane z potencjalnym wyciekiem danych. Może on ujawnić wrażliwe i prywatne informacje użytkowników, w tym dane osobowe, poufne rozmowy i własność intelektualną. Skutki takiego wycieku mogą być bardzo poważne, obejmując naruszenie prywatności, utratę zaufania klientów i potencjalne konsekwencje prawne.

Zdaniem specjalistów z CERT-EU ryzyko ujawnienia wrażliwych danych podczas korzystania z dużych modeli językowych (LLM) można znacznie ograniczyć, starannie wybierając sposób wdrożenia AI. Potencjalnym rozwiązaniem może być wykorzystanie lokalnego modelu bazującego na otwartym źródle, hostowanego on-premise i pod bezpośrednią kontrolą wykorzystującej go firmy. Inny sposób to skorzystanie ze zweryfikowanej usługi komercyjnej, oferującej środowisko stworzone z myślą o ochronie prywatności. ■

Zdaniem integratora

Wojciech Wąsik, Chief Digital & Information Security Officer, Transition Technologies PSC

Podejmując decyzję o uruchomieniu skutecznie działającego ZTNA klient powinien po pierwsze odpowiedzieć sobie na pytanie: czy i w jakim zakresie potrzebuję tego rozwiązania. To z kolei wymaga edukacji oraz skonfrontowania swojej percepcji zagrożeń i poziomu ochrony z wiedzą rynkową. Wsparcie doświadczonego partnera, kontakt z dostawcą systemów, udział w konferencjach poświęconych cyberbezpieczeństwu i ZTNA na pewno zaowocuje bardziej dojrzałym podejściem. Po drugie, aby dostosować infrastrukturę do modelu Zero Trust, należy realnie ocenić jakie możliwości organizacyjne i finansowe klient posiada. Wdrożenie systemu jako kolejnej fasady uszczelniającej dostęp do sieci mija się z celem. Fundamentem jest zmiana wewnętrzna – przestajemy zabezpieczać sieć, a skupiamy się na ochronie aplikacji i kontroli dostępu. To często wymaga wielu wewnętrznych dyskusji, warsztatów i konfrontacji punktów widzenia, aby zespoły – zarówno techniczne, jak i kierownicze – zaczęły dostrzegać sens proponowanej zmiany. Po trzecie, elementem uruchomienia ZTNA musi być także zadbanie o odpowiednie kwalifikacje zespołów IT. Ten, często niesłusznie pomijany, aspekt może okazać się szczególnie kłopotliwy, jeśli klient nie zadba o zbudowanie wspólnego celu, szkolenia lub reorganizację zespołów technicznych, tak aby w pełni wspierały potencjał wdrożenia.

Kompleksowa platforma Acronis dla partnerów

Acronis umożliwia partnerom świadczenie w modelu MSP usług kompletnego środowiska cyfrowej ochrony zasobów IT. Mogą one obejmować funkcje backupu rozszerzonego o przywracanie pracy po wystąpieniu awarii, zabezpieczeń antywirusowych i EDR, a także ochronę danych wrażliwych i zarządzanie maszynami.

Przy stale rosnącym krajobrazie cyfrowych zagrożeń dane przedsiębiorstw są coraz bardziej narażone na ataki. Ich zabezpieczanie stało się nieodzownym elementem strategii biznesowej, dlatego coraz więcej firm decyduje się na współpracę z dostawcami usług zarządzanych (MSP). Mogą oni skorzystać z zaawansowanej platformy ochronnej **Acronis Cyber Protect Cloud** wyróżniającej się połączeniem w sobie szeregu narzędzi i funkcji pomagających w zabezpieczaniu danych przedsiębiorstwa oraz zapewniających szybkie i sprawne przeprowadzenie działań naprawczych w przypadku wystąpienia incydentu.

Jednym z kluczowych elementów platformy Acronis Cyber Protect Cloud jest usługa **Advanced Disaster Recovery**. Umożliwia ona kopiowanie do repozytorium Acronis Cloud obrazów systemów operacyjnych Windows i Linux, zainstalowanych aplikacji oraz plików użytkowników. W przypadku awarii dysku komputera, poważnego błędu oprogramowania lub powodzenia ataku cyberprzestępców (np. zaszyfrowania danych przez ransomware), kopia takiego obrazu może być uruchomiona w postaci wirtualnej maszyny bezpośrednio w chmurze Acronis lub na wskazanym przez administratora serwerze. Identyczny mechanizm jest dostępny dla środowisk wirtualnych, obsługiwanych przez wszystkie popularne hypervisory.

Przywrócenie takiego środowiska do pracy bezpośrednio z centrum danych producenta następuje bardzo szybko, co minimalizuje ryzyko przestoju i związanych z nim strat. Administratorzy zaś zyskują dodatkowy czas na przywrócenie komputera do pracy – na podobnym lub innym sprzęcie. Bardzo korzystny dla firm jest też w tym przypadku charakterystyczny dla usług chmurowych abonamentowy model cenowy – nie muszą one inwestować w drogą infrastrukturę DR, która nie przyczynia się do wzrostu zysku przedsiębiorstwa, a jedynie stanowi koszt ubezpieczenia przed stratami.

Bezpieczeństwo to nie tylko backup

Kolejnym kluczowym elementem platformy Acronis Cyber Protect Cloud jest ochrona antywirusowa z funkcjonalnością **EDR (Endpoint Detection and Response)**. Wbudowany już wcześniej w rozwiązania Acronis mechanizm antywirusowy został rozbudowany o EDR, co pozwala na bieżące monitorowanie i analizę wykrytych incydentów bezpieczeństwa oraz szybką reakcję na nie. To oznacza, że klienci końcowi lub partnerzy MSP mogą śledzić aktywność w środowisku IT, analizować podejrzane zachowania oraz podejmować odpowiednie działania w celu zabezpieczenia systemów.

Mechanizm EDR dostępny na platformie Acronis Cyber Protect Cloud zapewnia wiele zaawansowanych funkcji, jak analiza behawioralna, wykrywanie zagrożeń w czasie rzeczywistym, raportowanie incydentów oraz izolacja złośliwego kodu. To umożliwia dostawcom usług zarządzanych skuteczną ochronę swoich klientów przed takimi zagrożeniami jak ransomware czy zaawansowane ataki typu phishing.

Zdalne wsparcie partnerów

Ostatnim elementem, na który warto zwrócić uwagę, jest funkcja zdalnego dostępu do komputerów klientów z systemami Windows/Linux/macOS oraz ich monitorowania **(Remote Desktop and Monitoring)**, oferowana jako część pakietu Advanced Management na platformie Acronis Cyber Protect Cloud. Narzędzie to ułatwia zarządzanie komputerami i udzielanie pomocy technicznej w razie potrzeby. Wykorzystany w nim został zarówno tradycyjny protokół RDP, jak też stworzony przez Acronis protokół NEAR, który cechuje się znacznie wyższym poziomem bezpieczeństwa. Zapewnione jest również wsparcie dla usługi Apple Screen Sharing.

Możliwość oferowania przez platformę Acronis Cyber Protect Cloud takich funkcji jak Disaster Recovery, ochrona antywirusowa z EDR oraz zdalne zarządzanie i monitorowanie, ułatwia partnerom stworzenie bogatej oferty usług skutecznej ochrony danych i infrastruktury klientów. Dla firm MSP Acronis opracował specjalne reguły w ramach swojego programu partnerskiego, dzięki czemu mogą one rozpocząć świadczenie usług dla małych, średnich i dużych klientów, bez względu na ich specyfikę oraz wymagania.

Autoryzowanymi dystrybutorami oprogramowania Acronis w Polsce są: Also, APN Promise, Clico, Dagma, Ingram Micro oraz Systemy Informatyczne ITXON.

Acronis

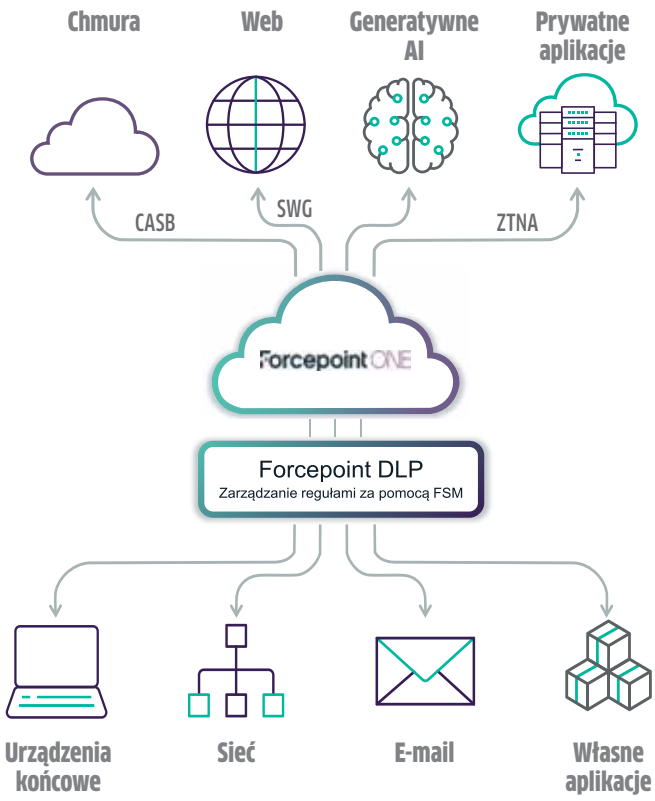
Dodatkowe informacje:
Dariusz Mumot, Senior Solutions Engineer, Acronis
dariusz.mumot@acronis.com

Forcepoint: chronimy dane wszędzie

Data Security Everywhere to przyjęta przez Forcepoint koncepcja, zgodnie z którą narzędzia oferowane przez tego producenta umożliwiają zabezpieczanie każdego rodzaju danych, niezależnie od tego, gdzie się znajdują i w jakich okolicznościach są przetwarzane.

Filarem koncepcji Data Security Everywhere jest zintegrowana platforma Forcepoint ONE klasy SSE (Security Service Edge). Umożliwia ona tworzenie spójnych reguł polityki bezpieczeństwa dla całego środowiska, obejmującego swym zasięgiem dane przetwarzane w siedzibie przedsiębiorstwa, w aplikacjach chmurowych, a także użytkowane przez pracowników zdalnych i w trakcie podróży. Rozwiązanie to ostatnio zostało uznane za lidera w raporcie Forrester Wave (Data Security Platform Q1 2023) oraz jako „Top Player" w raporcie Radicati Group (DLP Market Quadrant 2023).

Dzięki Forcepoint ONE zasady ochrony danych z narzędzia Forcepoint Security Manager (FSM) mogą być w automatyczny i scentralizowany sposób aplikowane do takich rozwiązań jak Cloud Access Service Broker (CASB), Secure Web Gateway (SWG) czy Zero Trust Network Access (ZTNA). Administratorzy uzyskują dostęp do tworzonych centralnie raportów dotyczących wszystkich zaobserwowanych incydentów oraz informacji z przeprowadzonych przez narzędzia Forcepoint analiz i podjętych akcji. FSM stanowi również jedno miejsce do zarządzania incydentami wycieku danych i ich śledzenia.



Podstawowe założenia koncepcji Data Security Everywhere

- Uproszczone zarządzanie regułami polityki bezpieczeństwa
- Bezpieczne dane na każdym urządzeniu i w każdej aplikacji
- Lepsza widzialność środowiska i nieustrukturyzowanych danych
- Ujednolicone mechanizmy kontroli i raportowania
- Obecność mechanizmu Security Service Edge

DLP gotowe do działania

Należące do platformy Forcepoint ONE rozwiązanie Forcepoint Enterprise DLP zapewnia skuteczne wykrywanie wycieków danych dzięki zaimplementowanym ponad 1600 gotowym klasyfikatorom, regułom polityki i szablonom – więcej niż w przypadku jakiegokolwiek innego dostawcy tego typu narzędzi. Są one egzekwowane zarówno w urządzeniach końcowych, jak i usługach chmurowych. Obejmują przede wszystkim takie akcje jak załączanie plików do wiadomości e-mail oraz udostępnianie ich za pomocą popularnych serwisów, pobieranie plików, jak też komunikacja przez czat.

Dzięki zastosowanym mechanizmom uczenia maszynowego możliwe jest skuteczne rozpoznawanie danych nieustrukturyzowanych (ponad 900 typów plików, nawet jeśli została zmieniona nazwa ich rozszerzenia) oraz przetwarzanie języka naturalnego (NLP) w celu zwiększenia dokładności rozpoznawania powszechnych typów danych. Dodatkowo, stworzone przez Forcepoint narzędzie PreciseID Fingerprinting pobiera dane bezpośrednio z ustrukturyzowanych i nieustrukturyzowanych źródeł. Następnie tworzy unikalny cyfrowy podpis, który reprezentuje dane poddane analizie, co pozwala identyfikować, monitorować i chronić wrażliwe informacje.

Dystrybutorem rozwiązań Forcepoint w Polsce jest Ingram Micro.

Forcepoint INGRAM MICRO

Dodatkowe informacje:
Piotr Jasiński, Business Unit Manager, Ingram Micro
piotr.jasinski@ingrammicro.com

Szkolenia G DATA dla partnerów i klientów

G DATA ma w ofercie platformę szkoleniową, z której mogą korzystać użytkownicy końcowi, ale też partnerzy do rozbudowy portfolio swoich usług związanych z bezpieczeństwem.

Celem, którzy postawiła przed sobą firma G DATA jest zwiększanie świadomości obecnych, systematycznie rosnących zagrożeń. Jej cyfrowa platforma edukacyjna, dostępna także w Polsce, zawiera aż 36 opracowanych przez ekspertów materiałów z zakresu świadomości przestrzegania zasad bezpieczeństwa. Ich treść bazuje na realnych przykładach ataków oraz spotykanych zagrożeń i będzie nieustannie aktualizowana, wraz z rozwojem szkodliwej działalności cyberprzestępców.

Platforma Security Awareness Training znajduje zainteresowanie w oczach partnerów, ponieważ dzięki niemu mogą rozszerzyć swoją ofertę szkoleniową. Bardzo skutecznym argumentem sprzedażowym jest też fakt, że szkolenia te stanowią idealne przygotowanie do zdobycia certyfikatu ISO 27001 oraz minimalizują ryzyko nałożenia kar w wyniku naruszenia obowiązku o ochronie danych osobowych. Więcej informacji dostępnych jest na stronie gdata.pl/szkolenia.

Elastyczne podejście do każdego pracownika

Jednym z użytkowników platformy Security Awareness Training jest niemiecka firma Edelrid, która specjalizuje się w produkcji lin wspinaczkowych. Kilka lat temu stała się ofiarą ataku ransomware Locky, a do pracy udało się jej szybko wrócić tylko dzięki aktualnym kopiom zapasowym. Zarząd Edelrid, w ramach budowy całościowej strategii bezpieczeństwa IT, zdecydował się na jeszcze lepsze przygotowanie pracowników na istniejące zagrożenia. Dlatego zostali oni zaproszeni do udziału w szkoleniach z zakresu świadomości bezpieczeństwa.

Materiały treningowe zostały udostępnione wszystkim pracownikom. Dzięki modułowej strukturze przebieg szkoleń został rozłożony w czasie i można było ukończyć je w dowolnym momencie. Zwykli pracownicy ukończyli 18 podstawowych kursów, liderzy działów przeszli przez 31 kursów, zaś pracownicy IT zostali zobowiązani do ukończenia pełnego pakietu z 33 kursami. Ponieważ firma Edelrid nie jest etnicznie jednorodna, dużą korzyścią była możliwość ukończenia szkoleń w ojczystym języku każdego z pracowników.

Po sześciu miesiącach od rozpoczęcia szkoleń zdecydowano się zmniejszyć ich zakres, aby nie przeciążać pracowników pod względem ilości treści do przyswojenia. Obecnie dla każdego pracownika obowiązkowe jest ukończenie ośmiu kursów (pięciu podstawowych i kolejnych w zależności od pełnionego stanowiska).

Wygodniej przez internet

Streamline to szwajcarska firma świadcząca usługi kompleksowego wsparcia klientów w zakresie IT. Jej zarząd podjął strategiczną decyzję i nawiązał współpracę z G DATA w celu zaoferowania klientom szkoleń dotyczących bezpieczeństwa w modelu white-label. Klienci Streamline są oczywiście zabezpieczeni na poziomie technicznym – korzystają z firewalli, narzędzi do ochrony urządzeń końcowych oraz tworzenia kopii zapasowych. Wiadomo jednak, że w kontekście bezpieczeństwa najsłabszym ogniwem jest człowiek, któremu zdarza się ulec ukierunkowanym atakom realizowanym chociażby poprzez wiadomości spear phishing. Dlatego istnieje duże zapotrzebowanie ze strony klientów na kompleksowe działania szkoleniowe.

Odrzucono jednak możliwość realizowania szkoleń w modelu stacjonarnym, nie tylko ze względu na ich intensywność, ale też ryzyko, że nie zawsze wszyscy będą mogli wziąć w nich udział. Dlatego zdecydowano się na rozbudowanie oferty o szkolenia realizowane poprzez platformę, w ramach której możliwe jest stworzenie pakietów dostosowanych do poziomu uczestnika, składających się z krótkich modułów (5–20 minut). Dla firmy Streamline bardzo ważna była też możliwość oznakowania szkoleń własną marką (white-label), dzięki czemu klienci identyfikują usługę z dostawcą, do którego mają zaufanie.

Tematyka szkoleń G DATA Security Awareness Training

- Bezpieczna praca poza biurem
- Zarządanie ryzykiem i hasłami
- Phishing & Malware – demaskowanie ataków i prób wyłudzenia danych
- W jaki sposób informacje są klasyfikowane i dlaczego?
- Social-media i praca w chmurze
- Incydenty zagrażające bezpieczeństwu i kontrola dostępu
- Socjotechnika
- Prawidłowe użytkowanie urządzeń mobilnych w pracy
- RODO i prywatność

G DATA academy

Dodatkowe informacje:
Dział Handlowy G DATA Software,
tel. (94) 37-29-650,
sales@gdata.pl

MATERIAŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ G DATA SOFTWARE.

Funkcje bezpieczeństwa w skanerach

Właściwa ochrona dokumentacji przetwarzanej przez skanery jest kluczowa dla zachowania poufności i zapewnienia zgodności z regulacjami. Dlatego warto postępować w zgodzie z wypracowanymi przez branżę najlepszymi praktykami.

Postępująca cyfryzacja spowodowała, że coraz ważniejsze stało się wdrożenie odpowiednich procedur, aby zapewnić poufność firmowym danym. Jednym z kluczowych w tym kontekście obszarów jest środowisko skanowania dokumentów i ich przetwarzania. Aby zagwarantować ich ochronę, konieczne jest stworzenie odpowiedniej strategii przechowywania i przesyłania dokumentów, z uwzględnieniem wielu środków technicznych, ale też nie zapominając o szkoleniu pracowników.

1. Korzystanie z godnych zaufania, certyfikowanych systemów

Bezpieczne przetwarzanie dokumentacji papierowej powinno się odbywać z użyciem certyfikowanych systemów producenta sprzętu bądź takich, które on autoryzuje. W celu zapewnienia właściwej organizacji zeskanowanych dokumentów oraz warunków ich przechowywania i udostępniania, warto korzystać ze sprawdzonych rozwiązań z odpowiednimi atestami i certyfikatami. Zaleca się wdrażanie systemów bezpiecznego zarządzania dokumentami (DMS). Dobrze zaprojektowany DMS zapewnia kontrolę wersji, dzienniki dostępu oraz dostęp bazujący na rolach.

2. Kontrola dostępu

Aby uchronić firmę przed niekontrolowanymi wyciekami danych, warto wyposażyć ją w skanery uniemożliwiające nieautoryzowane kopiowanie. Ochrona winna odbywać się za pomocą mechanizmów kontroli dostępu, takich jak PFU Ricoh N7100E lub fi-7300NX. Korzystanie z nich jest możliwe wyłącznie po prawidłowym uwierzytelnieniu na panelu urządzenia poprzez wprowadzenie kodu PIN, loginu i hasła, czy zbliżeniu karty NFC do czytnika. W tym scenariuszu użytkownik może przekazywać zeskanowane dokumenty tylko do zdefiniowanych dla niego lokalizacji, więc nie będzie mógł omyłkowo lub celowo przesłać danych do nieautoryzowanej lokalizacji lub folderu innej osoby.

3. Ochrona przed zniszczeniem i utratą informacji

Współczesne skanery to wysokowydajne maszyny, które przetwarzają dokumenty z dużą prędkością, co może prowadzić do zacięć, czy nawet fizycznego uszkodzenia dokumentu w przypadku papieru o gorszej jakości lub pomiętego, czy sklejonego. Jeśli w firmie tego typu dokumenty zdarzają się często, warto zainwestować w skaner wyposażony w odpowiednie mechanizmy ochronne:

- czujniki ultradźwiękowe wykrywające pobranie sklejonych dokumentów;
- czujniki akustyczne wykrywające anomalie, jak zwijanie papieru podczas podawania, co zabezpiecza dokument przed podarciem;
- czujniki detekcji długości wykrywające nałożone na siebie dokumenty, co może spowodować przesunięcie papieru i prowadzić do jego zacięcia oraz utraty informacji;
- czujniki detekcji przekosu wykrywające sytuacje, gdy użytkownik krzywo umieścił dokumenty na podajniku (sprawdzają, czy cały dokument mieści się w efektywnym obszarze skanowania), co zapewnia, że żaden fragment nie zostanie utracony;
- rolki podające dokumenty automatycznie prostują je i zabezpieczają przed nadmiernym przekosem.

4. Bezpieczeństwo danych

Obrazy skanowanych dokumentów znajdują się przez określony czas w pamięci skanera. Urządzenia firmy PFU Ricoh dbają o to, żeby dane te były bezpieczne w czasie skanowania i po jego zakończeniu. Dostęp do skanera może być zabezpieczony hasłem w celu uniknięcia przechwycenia danych, natomiast wszystkie skanowane informacje są przechowywane jedynie w pamięci ulotnej, z której po restarcie urządzenia nie da się odczytać danych. Natomiast skanery wyposażone w twarde dyski mają odpowiednie mechanizmy szyfrowania pamięci, co uniemożliwia przechwycenie znajdujących się na nich informacji.

5. Dopasowanie do potrzeb

Istotnym elementem w kontekście zagwarantowania bezpieczeństwa związanego ze skanowaniem dokumentów jest dbałość o to, aby wybrany sprzęt spełniał przyjęte przez przedsiębiorstwo wymagania w tym zakresie. PFU Ricoh razem z dystrybutorem – firmą Stovaris – mogą na prośbę resellera lub użytkownika końcowego zorganizować szkolenie, podczas którego zaprezentują najlepsze praktyki dotyczące bezpieczeństwa dla rozwiązań do digitalizacji.

PFU A RICOH Company

Stovaris

Dodatkowe informacje:
Daniel Murawski, Product Manager, Stovaris
d.murawski@stovaris.pl

MATERIAŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI PFU A RICOH COMPANY I STOVARIS.

Komunikacja skutecznie zaszyfrowana

Cypherdog to wymyślone i stworzone przez polski zespół rozwiązanie, które umożliwia kompleksowe i skuteczne szyfrowanie komunikacji biznesowej. Jego kluczową cechą jest brak zaangażowanej w proces szyfrowania trzeciej strony – producenta, wystawcy certyfikatów lub dostawcy warstwy komunikacyjnej.

Infrastruktura poczty elektronicznej, podobnie jak większość cyfrowych usług, jest podatna na cyberataki, które mogą skutkować nieuprawnionym dostępem do skrzynki pocztowej i ujawnieniem poufnych informacji. Co więcej, w przypadku nieautoryzowanego użycia skompromitowanej skrzynki e-mail, odbiorcy wiadomości nie są w stanie zweryfikować tożsamości ich rzeczywistego nadawcy. Cypherdog to przystępne cenowo, kompleksowe rozwiązanie chroniące przed obydwoma tymi zagrożeniami. Zapewnia szyfrowanie wiadomości poprzez ukrywanie ich treści przed nieautoryzowanymi osobami. Pozwala też odbiorcy na zweryfikowanie tożsamości prawdziwego nadawcy.

Oprogramowanie Cypherdog pozwala zaszyfrować i odszyfrować dowolny tekst lub plik i wysłać je za pomocą dowolnego medium, w tym pocztą elektroniczną wspieraną przez wtyczki do przeglądarek Firefox, Chrome i Edge dla Gmaila/Google Suite i AddIns w Outlook oraz Thunderbird. Użytkownik może wysyłać oraz odbierać zaszyfrowane pliki i wiadomości za pomocą dowolnego webowego lub natywnego klienta poczty elektronicznej, a też takich usług jak Slack, WeTransfer, Google Drive lub dowolnej innej metody komunikacji. Zawsze ma pewność, że tylko autoryzowany odbiorca będzie miał dostęp do odszyfrowanej treści.

Cypherdog skutecznie chroni przedsiębiorstwa przed szpiegostwem gospodarczym, wyciekami danych, nową generacją ataków ransomware z mechanizmem podwójnego wymuszenia, wyłudzeniami pieniędzy za pomocą fałszywych faktur i innymi rodzajami wykorzystania poczty elektronicznej w działaniach socjotechnicznych. Dzięki temu wspiera firmy przy wdrożeniach ISO 2700x, a także w zapewnianiu zgodności z RODO. Także europejskie ustawodawstwo, takie jak DORA czy NIS2, bezpośrednio wskazuje na szyfrowanie jako rekomendowaną metodę ochrony komunikacji.

Potwierdzone przewagi

Oprogramowanie Cypherdog jest proste w użytkowaniu. W trakcie instalacji aplikacja prosi o hasło do klucza prywatnego użytkownika i pozwala na wykonanie jego kopii zapasowej (w postaci pliku zapisywanego lokalnie lub na urządzeniu USB, zaś w wersji Business kopia wykonywana jest automatycznie na serwerze firmy). Po zakończeniu instalacji można szyfrować wiadomości i załączniki oraz wysyłać je natychmiast za pośrednictwem poczty e-mail.

Cypherdog wyraźnie przewyższa często stosowany standard szyfrowania S/MIME pod wieloma względami. Jego mankamentem jest wykorzystanie łańcucha certyfikatów x509, które są podatne na ryzyko ataków na infrastrukturę klucza publicznego (PKI). W przeciwieństwie do tego, Cypherdog wprowadza przełomową funkcję „magicznego okna", umożliwiającą intuicyjne szyfrowanie i deszyfrowanie tekstu na różnych platformach, jak Slack, Telegram czy Google Docs, co jest niemożliwe przy zastosowaniu S/MIME. Cypherdog usuwa też podatność na ataki na lokalne magazyny certyfikatów, przez co eliminuje ryzyko naruszenia tożsamości i bezpieczeństwa wiadomości.

Wyeliminowane jest też zagrożenie obecne w standardzie PGP, w którym możliwa jest zmiana kluczy publicznych użytkowników, co stwarza ryzyko ataków typu „man in the middle". W Cypherdog nie występuje zjawisko zaufanej sieci, co oznacza, że klucz publiczny jest podpisywany przez system i kontrolowany przez aplikację klienta, bez przekazywania do infrastruktury firm trzecich. Dodatkowo, dłuższy ciąg klucza asymetrycznego w Cypherdog wpływa na wyższy poziom bezpieczeństwa w porównaniu ze standardem PGP.

Przemysław Kucharzewski
General Manager, Cypherdog Security

W ostatnim czasie wprowadziliśmy do oferty wersję Business, która współpracuje z systemami DLP oraz antywirusowymi i xDR, a także pozwala na szyfrowanie i deszyfrowanie plików oraz tekstów z użyciem linii komend, co na przykład umożliwia zautomatyzowanie procesu przy wysyłce zestawień operacji na koncie w instytucjach finansowych czy wyników badań diagnostycznych w placówkach ochrony zdrowia. Obecnie pracujemy nad aplikacjami dla urządzeń mobilnych, które dołączą do dostępnych już klientów dla systemów Windows, macOS i Linux. Wkrótce wprowadzimy także system dystrybucji kluczy publicznych w mechanizmie blockchain, jak też zagwarantujemy odporność na łamanie naszych metod szyfrowania za pomocą komputerów kwantowych.

CYPHER.DOG®

Dodatkowe informacje:
Przemysław Kucharzewski,
General Manager, Cypherdog Security,
przemyslaw.kucharzewski@cypher.dog

Rozproszone dane w hybrydowej chmurze

Do obsługi nowych aplikacji oraz sposobów przetwarzania danych potrzebne będą zarówno wielkie, hiperskalowe centra danych, jak i te małe, brzegowe. Wszystkie połączy chmura, której docelowym modelem jest hybryda.

Tomasz Janoś

Wokół centrów danych integratorzy mogą tworzyć ofertę obejmującą wszystkie aspekty środowiska IT klientów – od wdrażania infrastruktury, poprzez jej zabezpieczanie, aż po zarządzanie. Dzięki dużej rynkowej konkurencji tego typu placówek łatwe i atrakcyjne ekonomicznie stało się też uruchamianie dla klientów zapasowych ośrodków przetwarzania danych albo obejmowanie ich całego środowiska backupem w formie zewnętrznej usługi. Finalnie, dla klientów o najbardziej rozbudowanej infrastrukturze i rygorystycznych wymaganiach warto jest stworzyć bazującą na usługach centrów danych ofertę pod kątem przywracania środowisk IT do pracy po awarii lub katastrofie, jak też tworzenia infrastruktury hybrydowej, łączącej cyfrowe zasoby klienta z chmurą publiczną. To ostatnie wydaje się być najbardziej logicznym sposobem budowania firmowego IT.

Chmura publiczna, gdy pojawiła się w postaci komercyjnej oferty, była przedstawiana jako najlepsze rozwiązanie problemów związanych z przechowywaniem danych, dotyczących głównie skalowalności i wydajności. Jej operatorzy obiecywali, że uruchomienie wszystkich firmowych zasobów informatycznych w ich hiperskalowych centrach danych będzie kosztować mniej niż utrzymywanie chmury prywatnej albo serwerów on-premise. Po latach przedsiębiorstwa mają już znacznie większą wiedzę zarówno o zaletach, jak i wadach chmury publicznej.

Bez wątpienia doskonale sprawdza się ona w przypadku startupów, które jeszcze nie wiedzą, jakie będą mieć potrzeby związane z IT. Dlatego oczekują rozwiązania, które będzie można szybko skalować w górę i w dół. Z kolei przedsiębiorstwa, które już dysponują własnym IT, starają się obecnie bardzo uważnie analizować swoje potrzeby informatyczne, zdając sobie sprawę, że w chmurze publicznej często płaci się „ekstra" za rzeczy, z których się nie korzysta.

I chociaż wiele wskazuje na to, że chmura publiczna nie jest już docelowym miejscem dla całego firmowego IT, to z drugiej strony – co dowiodła sytuacja z pandemii – trudno będzie się bez niej obejść. Logicznym rozwiązaniem staje się architektura chmury hybrydowej, która łączy infrastrukturę chmury publicznej i prywatnej, dzięki czemu przedsiębiorstwa mogą korzystać z najlepszych cech obu środowisk. Z jednej strony zyskują kontrolę i bezpieczeństwo chmury prywatnej dla wrażliwych danych, a z drugiej skalowalność i optymalizację kosztów dla mniej krytycznych zasobów w chmurze publicznej.

> Mamy już większą wiedzę **zarówno o zaletach, jak i wadach** chmury publicznej.

Dzięki połączeniu obu środowisk firmy mogą skalować swoje zasoby w górę lub w dół w miarę potrzeb, unikając nadmiernej alokacji i redukując koszty. Korzystając z rozwiązania hybrydowej chmury mogą sprawić, że kluczowe aplikacje i dane będą zawsze dostępne i chronione, utrzymując większą kontrolę nad wrażliwymi danymi. Takie podejście umożliwia utrzymanie zgodności z regulacjami prawnymi i branżowymi, co jest szczególnie istotne w przypadku podmiotów stale przetwarzających wrażliwe dane, takich jak ochrona zdrowia, finanse czy administracja publiczna.

Brzegowe centra danych w sojuszu z 5G

Od kilku lat edge computing to dla wielu dostawców IT jeden z ważniejszych trendów na rynku. Z jednej strony wpływa na to eksplozja danych tworzonych na brzegu sieci, które monitorowane i analizowane mają ułatwiać klientom osiąganie lepszych wyników biznesowych. Z drugiej strony rośnie oferta przeznaczonego do wdrożeń brzegowych sprzętu i oprogramowania, które mają zmniejszyć opóźnienia aplikacji i zwiększać wydajność infrastruktury, co przekłada się na zwiększenie możliwości przetwarzania informacji (IT) oraz automatyzacji produkcji (OT). Dostawcy

oferują także gotową infrastrukturę dla brzegowych centrów danych.

Ta infrastruktura jest potrzebna, ponieważ w zastosowaniach analityki czasu rzeczywistego, Internetu Rzeczy (IoT), rzeczywistości wirtualnej (VR) i innych nowych technik przetwarzania informacji kluczowym ryzykiem w korzystaniu z usług centrum danych stają się opóźnienia, liczone czasem potrzebnym na podróż danych od ich źródła do odbiorcy. Tworzone są więc brzegowe centra danych, które są rozproszonymi obiektami świadczącymi usługi obliczeniowe i pamięci masowej. Takie obiekty często znajdują się blisko miejsca, w którym dane są generowane, albo jak najbliżej użytkownika. Wraz z rozwojem usług 5G te niewielkie centra danych będą odgrywać coraz większą rolę.

Sieci 5G oraz mechanizmy przetwarzania brzegowego są predestynowane do tego, aby funkcjonować w symbiozie. Chociaż wdrażane osobno także przynoszą duże korzyści, to stosowane razem, uzupełniają się, tworząc rozwiązanie, które pozwala przedsiębiorstwom uruchamiać zupełnie nowe aplikacje. Można spodziewać się, że coraz więcej klientów zacznie myśleć w przypadku wdrożeń Internetu Rzeczy (IoT) o prywatnych sieciach komórkowych 5G. Wzrost zainteresowania takimi sieciami będzie kreował nowe biznesowe szanse zarówno dla doświadczonych integratorów, jak i startupów.

Centrum danych szybkie do wdrożenia

Drugi trend, obok przetwarzania brzegowego, wpływający na wzrost popytu na niewielkie obiekty wynika z tego, że firmy zdają sobie sprawę, jak wiele czasu i pracy wymaga uruchomienie dużego centrum danych. Wybór lokalizacji, problemy budowlane, wyzwania związane z łańcuchem dostaw i wiele innych czynników ogranicza uruchamianie dużych obiektów. Budowa największych centrów danych zajmuje lata, a wielu klientów nie może czekać.

Owszem, są dostawcy, którzy twierdzą, że potrafią zbudować duże centrum danych w ciągu 12–18 miesięcy, ale takie deklaracje zazwyczaj pomijają etapy obejmujące planowanie, wybór lokalizacji, projektowanie i inne prace wstępne przed rozpoczęciem budowy. Jeśli wziąć pod uwagę wszystkie działania, to największe centra mogą potrzebować – od pierwszego konceptu do uruchomienia – nawet pięciu i więcej lat. ➤

Serwery
już nie są energooszczędne

Jeszcze przed niecałą dekadą postęp w projektowaniu i produkcji chipów wpływał na zmniejszenie zużycia energii przez serwery, ale w ostatnich latach granice optymalizacji w tym obszarze zostały osiągnięte. Doprowadziło to do gwałtownego wzrostu zużycia energii przez coraz wydajniejsze serwery, który – jak wynika z danych Standard Performance Evaluation Corporation (SPEC) – wyniósł od 2017 roku do teraz aż 266 proc. (!). Ten gwałtowny skok jest jednym z wielu czynników technicznych i rynkowych, które kierują uwagę zarówno ustawodawców, jak i klientów, na sprawy związane ze świadomością ekologiczną. Napędzają też popyt na rozwiązania infrastruktury centrów danych, które pozwalają łatwiej osiągnąć cele zrównoważonego rozwoju (Environmental, Social, and Governance, ESG).

Popularne standardy
projektowania centrów danych

Projekt centrum danych musi być zgodny z regulacjami prawnymi i standardami. Oprócz międzynarodowych, krajowych oraz lokalnych przepisów, które mają zastosowanie do projektów budowlanych wszystkich typów obiektów, istnieje kilka najważniejszych standardów obowiązujących przy planowaniu takich placówek:

- **Uptime Institute Tier Standard** – norma ta koncentruje się na odporności, redundancji i niezawodności centrum danych, zawiera wytyczne dotyczące faz projektowania, budowy i uruchamiania projektu.
- **ANSI/TIA-942** – norma ta dotyczy fizycznych aspektów funkcjonowania centrów danych, w tym infrastruktury telekomunikacyjnej, lokalizacji, architektury, systemów elektrycznych i mechanicznych, ochrony przeciwpożarowej i bezpieczeństwa.
- **EN 50600** – to pierwsza ogólnoeuropejska i ponadnarodowa norma, która przyjmuje całościowe podejście do planowania, budowy i eksploatacji centrum danych.

Fot. Adobe Stock

Co gorsza, na koszty i harmonogramy budowy takich placówek mają wpływ problemy z łańcuchem dostaw. Długie terminy realizacji, trwające kilka miesięcy, dotyczą chociażby rozwiązań klimatyzacji czy generatorów prądu. Eksperci przewidują, że stanie się to już normą. Dlatego w odpowiedzi na potrzebę szybszego udostępnienia potrzebnej mocy obliczeniowej wzrastać ma zainteresowanie prefabrykowanymi centrami danych, które będą wstępnie montowane w zakładach producenta, a następnie wysyłane do klienta. Mogą one przyczynić się do obniżenia ogólnych kosztów związanych z wdrożeniem infrastruktury, jednocześnie przyspieszając jej projektowanie i budowę.

W modelu prefabrykowanym projekty są zazwyczaj skalowalne, co pozwala na szybką reakcję na nieprzewidziane zapotrzebowanie. Wstępnie zintegrowane rozwiązania mogą obejmować takie podsystemy jak zarządzanie ciepłem, ochrona i dystrybucja energii, oprogramowanie sterujące i zarządzające, a także systemy pomocnicze, jak oświetlenie, ochrona przeciwpożarowa, bezpieczeństwo fizyczne i uzdatnianie wody.

Chłodzenie cieczą bardziej ekologiczne

Przez lata gęstość mocy w szafach serwerowych była względnie stała, ale to już przeszłość. Z badania Global Data Centre Survey 2022 przeprowadzonego przez Uptime Institute wynika, że u ponad jednej trzeciej operatorów centrów danych gęstość szaf w ciągu ostatnich trzech lat szybko wzrosła. Szczególnie dotyczy to większych przedsiębiorstw i centrów danych o dużej skali. Niemal połowa ankietowanych, którzy prowadzą obiekty o mocy 10 MW i więcej, deklarowała posiadanie szaf z urządzeniami o mocy powyżej 20 kW, zaś jedna piąta z nich stwierdziła, że w ich przypadku jest to powyżej 40 kW.

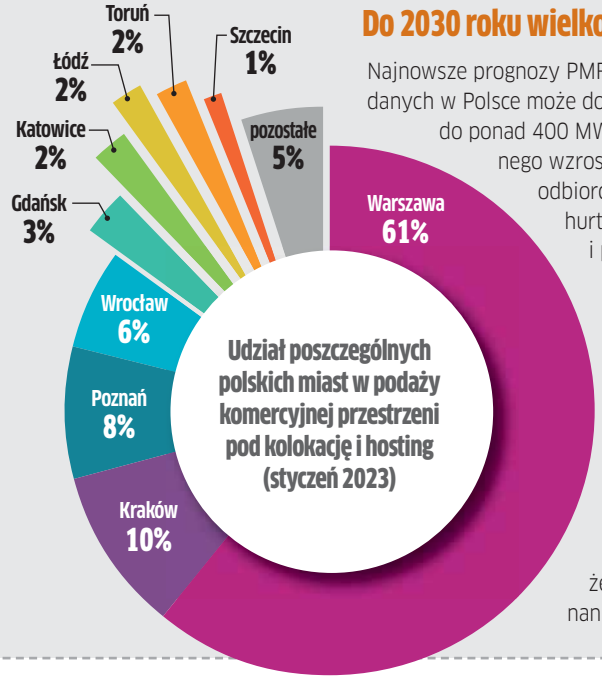
U wielu operatorów centrów danych **gęstość szaf** w ostatnim czasie szybko **wzrosła.**

Gęstość mocy środowisk IT rośnie wraz z rozwojem aplikacji związanych ze sztuczną inteligencją, uczeniem maszynowym, rozszerzoną rzeczywistością i wszelkich innych, bazujących na mechanizmach wysokowydajnego przetwarzania danych (High Performance Computing). To z ich powodu wzrasta ilość ciepła, które należy z centrum danych odprowadzać. W rezultacie wielu operatorów takich placówek, którzy tradycyjnie polegali na chłodzeniu powietrzem, zwraca się w stronę wydajniejszych rozwiązań zarządzania ciepłem, jak chłodzenie cieczą.

Gdy chłodzenie cieczą zaczyna być konieczne w centrach danych, w których obsługiwane są wymagające wysokiej mocy obliczeniowej aplikacje, przechodzenie na nowy sposób odprowadzania ciepła ułatwiają dostawcy serwerów, coraz powszechniej wprowadzający na rynek dostosowane do tego maszyny.

Jednak chłodzenie cieczą wiąże się z nowymi wyzwaniami i może wręcz budzić opory zarządzających centrami danych, przyzwyczajonych do tradycyjnej architektury z obiegiem powietrza. Dlatego to nowatorskie rozwiązanie wymaga niezawodnych systemów dystrybucji cieczy do szaf serwerowych lub zbiorników zanurzeniowych. Dzięki temu wyeliminowane zostaną obawy o bezpieczeństwo krytycznej infrastruktury IT, dotyczące jakości i właściwości płynu, jego potencjalnych wycieków, kontroli natężenia przepływu oraz zarządzania całym obiegiem cieczy w instalacji.

Chociaż ten typ chłodzenia nie jest całkowitą nowinką, to właśnie w tej metodzie eksperci upatrują obecnie szansę na tworzenie bardziej innowacyjnych rozwiązań w zakresie zarządzania ciepłem. Mechanizm ten stanowi także bardziej ekologiczną alternatywę dla wykorzystywania powietrza w centrum danych. ■



Do 2030 roku wielkość rynku centrów danych w Polsce może przekroczyć 500 MW

Najnowsze prognozy PMR pokazują, że realizacja planów największych dostawców usług centrów danych w Polsce może do 2030 r. spowodować maksymalny przyrost mocy komercyjnych serwerowni do ponad 400 MW (z około 120 MW w roku 2022). Analitycy nadal spodziewają się sukcesywnego wzrostu zapotrzebowania na usługi kolokacji w kraju oraz pojawienia się nowych odbiorców zagranicznych. Rynek będzie się coraz bardziej dzielił na dwie części: hurtową i detaliczną. Wzrośnie także jego wielkość w rozumieniu podaży mocy i przestrzeni w centrach danych o charakterze hiperskalowym.

Na liście dostawców usług centrów danych działających w Polsce i ukierunkowanych na rynek hurtowy są m.in. EdgeConneX, Vantage Data Centers, Data4, jak również operatorzy znani dotychczas głównie z obsługi rynku detalicznego (Atman, Equinix Poland). Klientami na rynku hurtowym są przede wszystkim najwięksi dostawcy chmury publicznej, tj. AWS, Google i Microsoft. AWS i Google już posiadają region chmurowy w Polsce. Microsoft uruchomił swój region 26 kwietnia 2023 r. na bazie trzech autonomicznych centrów danych. Dwa z nich wybudował i obsługuje na wyłączne potrzeby Microsoftu zewnętrzny partner. Wraz ze wzrostem rynku rosną wydatki firm na usługi centrów danych. Z tegorocznych badań PMR wynika, że dwie trzecie przedsiębiorstw zwiększyło na nie wydatki w 2022 r. w porównaniu z rokiem 2021, a w 2023 r. odsetek ten jeszcze wzrośnie.

Źródło: raport PMR „Rynek centrów danych w Polsce 2023"

Executive view

Data4: zrównoważone i innowacyjne centra danych

„W świecie, w którym zapotrzebowanie na moc obliczeniową nieustannie rośnie, centra danych, aby temu sprostać, muszą wprowadzać innowacje, ale jednocześnie ograniczać swój ślad środowiskowy" – mówi **Adam Ponichtera, Country Director and Head of Sales Poland, Data4 Group.**

Jaki typ podmiotów dominuje obecnie wśród nowych klientów zainteresowanych usługami centrów danych?

Wśród odbiorców Data4 znajdują się dostawcy usług chmurowych, operatorzy telekomunikacyjni, innowacyjne firmy technologiczne oraz koncerny międzynarodowe. Ogromną grupę stanowią klienci z branży bankowości, ubezpieczeń, integratorzy usług oraz podmioty sektora publicznego. Najważniejszą miarą jest jednak moc pobierana przez urządzenia IT. Patrząc z tej perspektywy, niekwestionowanym liderem są globalni operatorzy usług chmurowych, a wkrótce technologii AI.

W jakim stopniu klienci są zainteresowani fizycznym dostępem do rozwiązań kolokowanych w centrach danych Data4 lub wdrażaniem własnych procedur ochronnych?

Odpowiadając na potrzeby klientów dotyczące bezpieczeństwa, opracowaliśmy wszechstronny portal, który zapewnia bezpośredni dostęp do szeregu usług, w tym pełny podgląd sieci i pomieszczeń. Dzięki temu informacje o ewentualnych problemach docierają do klientów bezzwłocznie. Stosujemy również mniej oczywiste rozwiązania, takie jak wynoszenie całej infrastruktury technicznej poza komorę IT. Skutkiem tego jej przeglądy serwisowe są prowadzone bez fizycznego dostępu do serwerów klienta. Część firm stosuje dodatkowe procedury, jak nadzorowanie wejścia każdej osoby, w tym pracowników klienta, a także dodatkowe kamery, detektory metalu czy posterunek własnej firmy ochroniarskiej.

Portal dostępny dla klientów zapewnia podgląd sieci i pomieszczeń.

Jak duże znaczenie dla klientów mają aspekty związane z ekologią i jak w tym zakresie przedstawia się oferta Data4?

Realizując zobowiązania w obszarze zrównoważonego rozwoju, w naszych obiektach stosujemy szereg technik, których celem jest zmniejszenie śladu środowiskowego. Ich wdrażanie obejmuje zarówno etap budowy centrum danych, jak też jest widoczne podczas jego eksploatacji. Co więcej, realizujemy kompleksowy plan zarządzania wodą, wykorzystując w tym celu najnowsze techniki, takie jak „free-cooling" i „free-chilling". Pracujemy też nad udoskonaleniem metod nawilżania powietrza i optymalizacji temperatury. Jednym z najważniejszych osiągnięć w tym obszarze, wyróżniającym nas na rynku, jest Green Dashboard. To bezkonkurencyjne narzędzie, dzięki któremu klienci mogą monitorować ślad środowiskowy wynajętej infrastruktury. Pozwala im to ocenić jej wpływ na środowisko, a finalnie może okazać się pomocne w prowadzeniu obowiązkowego raportowania ESG.

W maju 2023 roku otworzyliście swoje pierwsze centrum danych w Jawczycach. Jakie są dalsze plany rozbudowy kampusu?

Nasza działalność w Polsce jest skupiona na rozwoju kampusu w podwarszawskich Jawczycach. Działka zajmuje powierzchnię 4 hektarów, więc ma potencjał do dalszej rozbudowy. Pełną inwestycję stworzą cztery obiekty, których całkowity przydział mocy wyniesie 60 MW. Zapewni to klientom potencjał korzystania z większej mocy obliczeniowej, co przełoży się na ciągłość rozwijającego się biznesu.

W jak dużym stopniu w infrastrukturze centrów danych wciąż możliwe jest wprowadzanie innowacyjności?

W świecie, w którym zapotrzebowanie na moc obliczeniową nieustannie rośnie, centra danych muszą wprowadzać innowacje, aby temu sprostać, ale jednocześnie ograniczać swój ślad środowiskowy. Świetnym tego przykładem jest wspomniany Green Dashboard. Dzięki niemu nie tylko ograniczamy własny ślad węglowy, ale także całego cyfrowego ekosystemu. Innowacje pojawiają się już na etapie budowy, a dzięki nim powstają trwałe, zrównoważone obiekty, zawierające opatentowaną komorę sufitową, czyli nowoczesny system chłodzenia. Naturalnie cały czas przyglądamy się kolejnym rozwiązaniom. Celem wszystkich tych działań jest zapewnienie każdemu z naszych klientów bardziej zoptymalizowanych operacji, większej modułowości oraz lepszej efektywności energetycznej i gęstości mocy.

Data4
SMART & SCALABLE DATACENTERS

Dodatkowe informacje:
Adam Ponichtera,
Country Director and Head of Sales Poland, Data4 Group
adam.ponichtera@data4group.com

Snowflake: wyższa wydajność chmury danych

Zapewnianie optymalnej wydajności i skalowalności mechanizmów analitycznych w dużych repozytoriach danych to duże wyzwanie. Snowflake traktuje to zadanie priorytetowo w odniesieniu do swojego flagowego produktu – autorskiej Chmury Danych (Snowflake's Data Cloud).

Podczas czerwcowej edycji konferencji Snowflake Summit 2023 firma zaprezentowała nowe funkcje Chmury Danych Snowflake, która ułatwia przedsiębiorstwom uzyskiwanie wartości z posiadanych danych. Wyposażono ją między innymi w mechanizm dużego modelu językowego bazującego na technologii stworzonej przez **polskich inżynierów z przejętej przez Snowflake firmy Applica**, zapewniono możliwość integracji ze środowiskiem Apache Iceberg Tables, jak też przedstawiono pierwsze wyniki pracy nowej wersji wskaźnika pomiaru wydajności SPI.

Snowflake rozwija też swoją platformę, aby obsługiwać szerszy zestaw zaawansowanych funkcji analitycznych, w tym mechanizmy uczenia maszynowego dla użytkowników baz SQL. Firma rozszerzyła także funkcje ujednoliconego zarządzania i prywatności o nowe wskaźniki jakości danych i mechanizmy ich klasyfikacji.

Duże modele językowe w Chmurze Danych

Według IDC w ciągu najbliższych pięciu lat ponad 90 proc. danych na świecie będzie nieustrukturyzowanych – w postaci dokumentów, obrazów, wideo, audio i innych. Te ogromne zbiory są zazwyczaj rutynowo przechowywane przez firmy, jednak uzyskanie z nich jakichkolwiek wartościowych informacji jest trudne. Do niedawna wymagało to realizowania ręcznych, podatnych na błędy procesów przez osoby, których umiejętności nie zawsze były wystarczające.

Obecnie problem ten jest w stanie rozwiązać firma Snowflake za pomocą wbudowanej w Chmurę Danych funkcji Document AI, która została zaprojektowana przez zespół specjalistów z przejętej we wrześniu 2022 roku firmy Applica. Zawiera ona mechanizmy sztucznej inteligencji umożliwiające analizę nieustrukturyzowanych danych, ułatwiającą ich zrozumienie oraz wydobycie z nich wartości za pomocą przetwarzania języka naturalnego. Funkcja ta znajduje się obecnie w fazie prywatnych testów dla wybranych użytkowników.

Document AI jest wyposażony w specjalny duży model językowy (LLM), dzięki któremu w platformie Snowflake dostępna jest funkcja łatwego wyszukiwania w dokumentach PDF takich treści jak kwoty faktur lub warunki umów. Użytkownik może następnie przekazać informacje zwrotne za pomocą interfejsu wizualnego i języka naturalnego, aby dostosować wyniki, a następnie odpowiednio przetrenować model. Możliwe jest również pobieranie informacji o strukturze tych dokumentów, przechowywanie jej w tabeli lub przekazanie do innej aplikacji. Po wprowadzeniu funkcji Document AI do publicznego użytku będzie ona rozszerzana na więcej typów nieustrukturyzowanych danych.

Lodowe tabele w Snowflake

Rozwiązanie Apache Iceberg stale zyskuje na popularności jako standard branżowy dla otwartych formatów tabel. Oprogramowanie to bazuje na otwartym źródle, które zostało stworzone w celu efektywnego zarządzania dużymi zbiorami danych w eko-

Kluczowe cechy nowoczesnej platformy danych

Nowoczesna platforma danych, aby zagwarantować właściwy poziom skalowalności i automatyzacji pracy, powinna charakteryzować się takimi cechami, jak:

- **Elastyczność** – wydajne środowisko wyszukiwania i analizowania informacji umożliwia zarządzanie wszystkimi danymi, w tym ustrukturyzowanymi, częściowo ustrukturyzowanymi i nieustrukturyzowanymi.
- **Skalowalność** – gotowość na przyrost ilości danych i ich częste zmiany, bez wpływu na wydajność ich automatycznej klasyfikacji.
- **Bezpieczeństwo** – spójne zasady dostępu do danych, które ich administrator może definiować i egzekwować zgodnie z wymogami zgodności z regulacjami.
- **Wysoki stopień automatyzacji** – zapewnia łatwe skalowanie i zmniejsza prawdopodobieństwo narażenia na naruszenie bezpieczeństwa oraz zgodności.
- **Heterogeniczność** – zdolność do obsługi danych z różnych środowisk i aplikacji.

systemie Hadoop oraz innych systemach przetwarzania danych. Jego głównym celem jest dostarczenie niezmiennej struktury przechowywania danych, która umożliwia zarówno efektywne zapytania analityczne, jak i zmiany danych w sposób zbliżony do tradycyjnych relacyjnych baz danych.

Jednym z głównych aspektów rozwiązania Apache Iceberg jest jego zdolność do obsługi operacji czasu rzeczywistego, przeprowadzanych na dużych zbiorach danych. Dzięki mechanizmowi „table snapshots" Iceberg umożliwia równoczesny dostęp do różnych wersji danych, co jest niezwykle przydatne w środowiskach, w których często ulegają one zmianom. System ten umożliwia również odczyt danych w sposób spójny (nawet jeśli są one zmieniane w trakcie odczytu), a jest to funkcja kluczowa w przypadku operacji analitycznych.

Jedną z nowości w ramach Snowflake Data Cloud jest jego integracja z architekturą Apache Iceberg Tables. Dzięki temu firmy mogą pracować z danymi w formacie Apache Iceberg przechowywanymi we własnym repozytorium (niezależnie od tego, czy są one zarządzane przez Snowflake, czy zewnętrznie), a jednocześnie czerpać korzyści z łatwości użytkowania, wydajności i ujednoliconego zarządzania charakterystycznego dla platformy Snowflake. Takie podejście upraszcza zarządzanie danymi, eliminując potrzebę przenoszenia lub kopiowania ich między systemami, a jednocześnie zwiększa elastyczność tego procesu i wpływa na obniżenie kosztów.

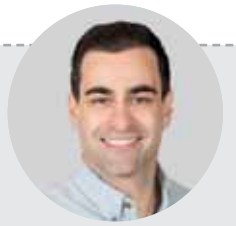
SPI poprawiony o 15 procent

Snowflake Performance Index (SPI) to z kolei metryka opracowana przez firmę Snowflake, która ma na celu mierzenie i ocenę wydajności zapytań przeprowadzanych w Chmurze Danych. Indeks wydajności SPI uwzględnia różnorodne aspekty związane z przetwarzaniem zapytań, takie jak czas uzyskania odpowiedzi, wykorzystanie zasobów obliczeniowych oraz efektywność operacji I/O.

Kluczowym celem SPI jest umożliwienie użytkownikom monitorowania, analizowania i poprawy wydajności swoich zapytań na platformie Snowflake. Dzięki tej metryce użytkownicy mogą zidentyfikować potencjalne źródła opóźnień czy niedoskonałości w zapytaniach, co pozwala na efektywną optymalizację oraz dostosowanie ich do konkretnych wymagań i scenariuszy użycia.

W ostatnim czasie Snowflake podjął działania w celu modyfikacji mechanizmu funkcjonowania wskaźnika SPI, aby jeszcze bardziej precyzyjnie określał wydajność środowisk klientów. Przez osiem miesięcy pracy nowego wskaźnika czas trwania zapytań poprawił się o 15 proc., co jest dowodem na precyzję działania tego mechanizmu, jak też jego przydatność do optymalizacji Chmury Danych.

Trzy pytania do...



Artina Avanesa,
dyrektora ds. zarządzania produktami w Snowflake

Przed jakimi wyzwaniami stoją menedżerowie firm, którzy chcą wdrożyć w nich strategię dotyczącą zarządzania danymi, aby czerpać z ich posiadania dodatkowe korzyści?

Coraz częściej doświadczają rosnącej presji ze strony klientów, aby inwestować w nowatorskie mechanizmy, takie jak sztuczna inteligencja, które lepiej pomogą im zrozumieć własne potrzeby, aby je zaspokoić. Z ich zastosowaniem wiąże się jednak konieczność spełnienia coraz bardziej rygorystycznych i złożonych wymogów w zakresie bezpieczeństwa danych, zarządzania nimi, a także pozostawania w zgodzie z wymogami regulacyjnymi. Żeby sprostać tym wyzwaniom, firmy powinny wybrać nowoczesną platformę, bazującą na sztucznej inteligencji, umożliwiającą zarządzanie danymi w chmurze, dzięki której będą mogły przyspieszyć pozyskiwanie informacji z danych i skupić się na swoich podstawowych kompetencjach.

W jaki sposób stworzyć strategię zarządzania danymi, która w swoich założeniach będzie wybiegać w przyszłość?

Dobrym przykładem jest tu sztuczna inteligencja, która w ciągu ostatnich kilku lat okazała się jedną z najgłębszych zmian technicznych, jakie widzieliśmy za naszego życia. Ponieważ tempo jej wpływu na funkcjonowanie przedsiębiorstw trudno jest określić, menedżerowie muszą zadbać o zapewnienie elastyczności w kontekście bezpieczeństwa i zarządzania, aby móc łatwo dostosować się do takich innowacji. Im więcej firm korzysta z generatywnej sztucznej inteligencji oraz dużych modeli językowych, tym rośnie poziom wykorzystywania wrażliwych i prywatnych danych. Chociaż to niezgodne z RODO, bywa, że po zakończeniu procesu szkolenia model językowy nadal będzie dysponował tymi danymi. A nie zawsze istnieje możliwość ich usunięcia. Chmura Danych Snowflake taką funkcję zapewnia, co stanowi znaczący krok w przyszłość, ponieważ w planowanej przez regulatorów Unii Europejskiej ustawie o sztucznej inteligencji temat ten prawdopodobnie będzie wzięty pod uwagę.

Jak w firmach powinny być skonstruowane zespoły pracowników, aby zapewnione było skuteczne i zgodne z regulacjami zarządzanie danymi?

W firmach zazwyczaj istnieją odrębne grupy osób zajmujących się bezpieczeństwem, zarządzaniem, zapewnianiem zgodności czy też przetwarzaniem danych. Obserwujemy, że gdy uruchamiane są procesy modernizacyjne w przedsiębiorstwach, często wychodzi na jaw brak współpracy pomiędzy tymi zespołami. Na przykład osoby zajmujące się platformami danych mogą chcieć wdrażać najnowsze technologie, aby dotrzymać kroku konkurencji lub tworzyć nowe produkty, ale zespół ds. zgodności może być niechętny ze względu na potencjalne naruszenia istniejących wymogów regulacyjnych. Dlatego konieczne jest zawczasu stworzenie modeli współpracy pomiędzy tymi grupami, aby mogły wspólnie stawiać czoła wyzwaniom i znajdować właściwe rozwiązania w celu skalowania środowiska zarządzania danymi przy ograniczeniu potencjalnych zakłóceń do minimum.

Dodatkowe informacje:
Nico Ziegler,
Senior Field Marketing Manager, Snowflake
nico.ziegler@snowflake.com

Cyfrowe dane na wagę biznesu

Rozwój sztucznej inteligencji ułatwia korzystanie z informacji, ale nie zwalnia od zapewnienia jak najlepszej jakości gromadzonych zasobów. Wręcz przeciwnie, narzędzia do zarządzania firmowymi danymi wciąż będą bardzo potrzebne.

Andrzej Gontarz

Informacja służy do działania – to jedno z przesłań współczesnej teorii informacji, które dobrze oddaje obecne podejście do wykorzystania jej w biznesie. W firmach dostęp do danych jest potrzebny zawsze w sprecyzowanym celu, do podjęcia konkretnych działań, czy realizacji zdefiniowanych procesów (wystawienia faktury, przyjęcia zamówienia, wykonania usługi, realizacji projektu, stworzenia strategii rozwoju itd.).

Powyższe założenie może być bardzo użyteczne przy konstruowaniu oferty narzędzi informatycznych wspierających zarządzanie informacją, jak i podczas negocjacji z potencjalnymi klientami. Podobnie zresztą jak pojęcie potrzeby informacyjnej, które pomaga w identyfikowaniu właściwych grup odbiorców poszczególnych treści. Informacja jest bowiem zawsze dla kogoś i po coś. Szczegółowe określenie faktycznych potrzeb informacyjnych poszczególnych zespołów pracowniczych, czy wręcz nawet pojedynczych osób w tych zespołach, pozwoli na przykład dobrać odpowiedni, rzeczywiście „szyty na miarę" system zarządzania obiegiem dokumentów i zawartych w nich danych.

Nie zwalnia to jednak od kompleksowego, całościowego podejścia do budowania systemu zarządzania informacją w przedsiębiorstwie. Przydatne w takiej sytuacji może być pojęcie infrastruktury informacyjnej. Obejmuje ona wszystkie zasoby, systemy i procesy, które umożliwiają sprawne gromadzenie, przetwarzanie i udostępnianie niezbędnych danych. Powinna działać na wzór infrastruktury drogowej – w każdej chwili umożliwiać wszystkim zainteresowanym korzystanie z potrzebnych informacji.

> Współcześni CDO chcą **koncentrować się** na działaniach strategicznych.

Rozwiązania dobrane do sytuacji

Do infrastruktury informacyjnej zalicza się zarówno rozwiązania sprzętowe, programistyczne, jak i organizacyjne, czy też prawne. Infrastruktura teleinformatyczna, czyli wyposażenie stricte techniczne, związane z warstwą sprzętową i oprogramowaniem narzędziowym, jest tylko jej częścią. Równie ważnym składnikiem są zasady tworzenia zasobów informacyjnych, reguły ich klasyfikacji czy procesy korzystania z nich.

Firmy oferujące rozwiązania z zakresu wspomagania zarządzania informacją powinny brać pod uwagę wszystkie te aspekty. Takie podejście otwiera perspektywy działania w wielu różnych obszarach, a jednocześnie pozwala na przygotowanie bardziej skonkretyzowanych ofert, które są dopasowane do aktualnych potrzeb klienta.

Infrastruktura techniczna jest ważna nie tylko dlatego, że umożliwia przechowywanie, przesyłanie i automatyczne przetwarzanie firmowych zasobów informacji. Odpowiednio dobrane wyposażenie sprzętowe i programowe pozwala także dostarczyć odbiorcy informację w taki sposób, jakiego potrzebuje i tam, gdzie jej naprawdę potrzebuje. To daje integratorom duże pole do popisu w kontekście doboru odpowiednich narzędzi i rozwiązań. W biurze mogą być to urządzenia wielofunkcyjne z opcją druku podążającego, pracownikom działającym w terenie przydadzą się drukarki do urządzeń mobilnych, zaś pracownicy wykonujący swoje obowiązki w trybie home office chętnie skorzystają z niewielkich, „domowych" drukarek. W każdym miejscu i w każdej sytuacji mogą być potrzebne inne, dobrze dopasowane rozwiązania.

W dobie postępującej cyfryzacji wszelkich form aktywności biznesowej ważne jest też zapewnienie odpowiednich narzędzi do skutecznego wprowadzania informacji do systemów informatycznych. Gdy dokumenty dostarczane są do firmy w postaci papierowej, potrzebne będą odpowiednie skanery – znów inne do wykorzystania w biurze, inne przy pracy zdalnej. Gdy zaś konieczne będzie przeniesienie danych z jednego systemu do drugiego, pomocne mogą okazać się narzędzia automatyzujące te działania.

Nie zawsze już „ręczne" wprowadzanie danych jest opłacalne, a nawet skuteczne. Przy dużej ilości operacji istnieje ryzyko

Fot. Adobe Stock

Nie zawsze już „ręczne" wprowadzanie danych **jest opłacalne, a nawet skuteczne.**

popełnienia błędu, przeinaczenia wartości, zamiany nazwy itp. Dlatego automatyzacja procesu cyfryzacji dokumentów, na przykład faktur, niesie z sobą wiele korzyści. Tutaj może być przydatny skaner z możliwością rozpoznawania tekstu za pomocą oprogramowania OCR, a następnie automatycznej klasyfikacji zawartych w dokumencie treści. Z kolei przy przenoszeniu dużych ilości danych z jednego oprogramowania do drugiego sprawdzają się bardzo dobrze roboty programistyczne, które automatyzują oraz przyspieszają żmudne czynności przepisywania danych.

Sprawny dostęp to pieniądz

Równie ważny jest sam system zarządzania firmowymi zasobami informacji. Chodzi o właściwe oznaczanie, klasyfikowanie, katalogowanie czy tagowanie poszczególnych składników informacyjnego zbioru. To bardzo ważny, newralgiczny wręcz, chociaż często niestety lekceważony zarówno przez użytkowników, jak i dostawców narzędzi informatycznych, element systemu zarządzania informacją w przedsiębiorstwie. To on decyduje o tym, czy do konkretnego odbiorcy trafią rzeczywiście potrzebne mu informacje, takie jakich faktycznie oczekuje. To on przesądza o tym, czy do innej, zintegrowanej aplikacji przekazywane będą dokładnie te dane, o które chodzi.

Problemy z dotarciem do właściwej informacji mogą czasami wręcz zaburzyć sprawne funkcjonowanie firmy. Zbyt długi czas poświęcony na poszukiwanie, to w konsekwencji również wymierne straty biznesowe. Konkretne korzyści można osiągnąć już chociażby poprzez uporządkowane, zorganizowane zarządzanie samą korespondencją przychodzącą do firmy. W niektórych przypadkach mogą to być tysiące dokumentów i wiadomości e-mail, do tego jeszcze w różnych formatach, rodzajach, typach. Z danych firmy Iron Mountain wynika, że optymalizacja zarządzania korespondencją przychodzącą może pozwolić na ograniczenie kosztów operacyjnych w tym obszarze nawet do 25 proc.

Korzyści bywają odczuwalne również w innych obszarach, na przykład poprzez uwolnienie mocy przerobowych pracowników, którzy mogą zająć się innymi zadaniami. Automatyzacja obsługi przychodzącej korespondencji powoduje, że dokumenty czy mejle kierowane są od razu do właściwego pracownika zajmującego się daną sprawą. Żeby to faktycznie sprawnie działało, do kategoryzacji zasobów firmowej poczty trzeba również użyć nowoczesnych technik klasyfikowania ➤

Lepszy dostęp do informacji to większa interoperacyjność

Znaczenie odpowiedniej infrastruktury technicznej w dostępie do informacji widać na przykładzie branży ochrony zdrowia. Podstawowym wyzwaniem we wprowadzaniu interoperacyjności systemów – umożliwiającej szerokie, wszechstronne wykorzystanie przetwarzanych danych – są tu ograniczenia techniczne. Tak twierdzi aż 68 proc. przedstawicieli podmiotów medycznych uczestniczących w badaniu przeprowadzonym przez Snowflake we współpracy z Fierce Healthcare. Do pozostałych przeszkód respondenci zaliczyli: wyzwania regulacyjne (55 proc.), nieaktualność danych (55 proc.) czy ograniczenia organizacyjne (44 proc.).

Placówki ochrony zdrowia są zmuszone, między innymi za sprawą rozwoju usług telemedycznych, do coraz szerszej cyfryzacji swojej działalności, jak chociażby korzystania w coraz większym zakresie z rozwiązań funkcjonujących w trybie online i usług w chmurze. Intensyfikacja procesów digitalizacji wiąże się z potrzebą zapewnienia interoperacyjności wykorzystywanych systemów, co umożliwia ich dobrą współpracę, a tym samym lepszą integrację i łatwiejszy dostęp do informacji. Do tego potrzebna jest odpowiednia infrastruktura teleinformatyczna i narzędzia techniczne, głównie z zakresu cyfrowego przetwarzania dokumentacji medycznej.

Niestety, jak wynika z badania przeprowadzonego przez Centrum e-Zdrowia we współpracy z Ministerstwem Zdrowia, w ubiegłym roku aż 74 proc. placówek opieki zdrowotnej w Polsce nie poddawało papierowej dokumentacji procesom digitalizacji. Dla 78 proc. najpowszechniejszym sposobem udostępniania dokumentacji medycznej innym podmiotom medycznym był wydruk. Jak więc widać, jest jeszcze wiele do zrobienia w tym obszarze.

w miejsce „ręcznego" tagowania. Dzisiaj na rynku dostępne są już rozwiązania wykorzystujące w procesach katalogowania systemy sztucznej inteligencji, bazujące na uczeniu maszynowym.

Narzędzia z dziedziny generatywnej sztucznej inteligencji, takie jak ChatGPT i podobne, też są już coraz częściej wykorzystywane do wyszukiwania potrzebnych informacji i automatycznego kreowania gotowych treści. Przedsiębiorstwa korzystają z nich przy tworzeniu ofert marketingowych, opisów produktów na stronę internetową, odpowiadaniu na korespondencję, sporządzaniu zestawień i raportów czy sprawozdań. Jednak stosowanie tych rozwiązań wciąż jeszcze wymaga nadzoru ze strony człowieka. Poza tym osiągane przy ich pomocy efekty są tym lepsze, im do bardziej uporządkowanych i o wysokiej jakości zasobów informacyjnych narzędzia sztucznej inteligencji mają dostęp.

Synteza dla zarządu

W przedsiębiorstwach szczególną rolę pełni informacja zarządcza. Służy ona przede wszystkim do podejmowania decyzji – zarówno tych krótkoterminowych, jak i strategicznych. Żeby dobrze spełniała swoją rolę, musi być jednak odpowiednio przygotowana dla potrzeb użytkowników, jakimi są menedżerowie czy członkowie zarządu. Powinna być w dużym stopniu przetworzona, zagregowana, zsyntetyzowana. W ramach tego procesu konieczne jest poddanie dostępnych danych analizie, której wynik pozwoli na wypracowanie wniosków służących podjęciu decyzji.

Narzędzia analityczne stanowią dzisiaj jeden z kluczowych elementów systemu zarządzania informacją. Mogą mieć różny charakter w zależności od skali działania przedsiębiorstwa, jego strategii rynkowych, czy potrzeb informacyjnych poszczególnych członków kadry zarządzającej. Nie musi to być od razu zaawansowane, specjalistyczne oprogramowanie analityczne klasy business intelligence. W wielu przypadkach wystarczy Excel. Wprawni użytkownicy, szczególnie z działów finansowo-księgowych czy marketingowych, potrafią za pomocą tego narzędzia uzyskać wiele interesujących zestawień i raportów niezbędnych w procesach decyzyjnych.

Rolą integratora jest więc rozpoznanie faktycznych potrzeb informacyjnych poszczególnych grup pracowników klienta oraz zaproponowanie odpowiedniego dla jego celów analitycznych narzędzia. Ważne, by zapewniało ono decydentom dostęp do tzw. jednego, wspólnego dla wszystkich obrazu prawdy. W tym celu potrzebna jest odpowiednia integracja danych z różnych aplikacji. Samo fizyczne, techniczne połączenie tych systemów i umożliwienie przesyłania między nimi informacji nie wystarczy do zapewnienia jednolitego oglądu sytuacji. Potrzebne jest też właściwe przygotowanie danych poddawanych integracji.

Aby operacja ta powiodła się, konieczne jest stworzenie zaplanowanego, ustandaryzowanego procesu wymiany informacji między systemami. Do tego niezbędna jest ustalona i realizowana przez wszystkich klasyfikacja danych. Obecnie w coraz większym zakresie możliwe jest jej wspieranie przez algorytmy sztucznej inteligencji. Jej główne zasady muszą być jednak określone przez człowieka, jak również zapewnione procedury weryfikacji jej poprawnego funkcjonowania.

Jakość danych to podstawa

Postępująca cyfryzacja i automatyzacja procesów przetwarzania danych oraz korzystania z informacji zwiększa znaczenie starań na rzecz zapewnienia właściwej jakości danych. Nawet rozwiązania bazujące na sztucznej inteligencji nie zawieszają podstawowej, obowiązującej w informatyce od lat zasady GIGO (Garbage In, Garbage Out – śmieci na wejściu, śmieci na wyjściu). Wprost przeciwnie, trenowanie modeli uczenia maszynowego wymaga przede wszystkim dostępu do dobrej jakości danych.

Jak wykazało badanie grupy naukowców z Politechniki Wrocławskiej, generatywne modele językowe, trenowane

Korzyści płynące z zarządzania jakością danych

Dzięki zarządzaniu jakością danych firmy mogą:

- liczyć na lepsze wyniki w działalności operacyjnej,
- zwiększyć oszczędności,
- zyskać większe zaufanie i satysfakcję klientów,
- monetyzować dane,
- ulepszyć ochronę reputacji produktów i samej firmy,
- podejmować trafniejsze decyzje,
- przyśpieszyć działania w obszarze inicjatyw związanych z danymi,
- zmniejszyć ryzyko płynące z niewłaściwej interpretacji firmowych danych.

Źródło: Wyzwania Chief Data Officerów, Deloitte 2023

Zdaniem integratora

Jakub Koba, CTO, Kogifi, ekspert organizacji SoDA

Obserwujemy skokowy wzrost zainteresowania cyfryzacją obiegu dokumentów w związku z rozwojem pracy hybrydowej. Dzisiaj nakłada się na to dynamiczny rozwój sztucznej inteligencji. Firmy rozumieją, że już wkrótce cyfrowy obieg dokumentów stanie się kluczowy dla odblokowania ich pełnego potencjału informacyjnego. Sztuczna inteligencja przeprowadzi zaawansowane analizy dokumentów lub na ich podstawie będzie generować automatycznie nowe. Przykładowo, na podstawie dokumentów ofertowych dział sprzedaży będzie mógł generować odpowiedzi na zapytania klientów, prosząc o to jedynie sztuczną inteligencję. Dział administracji będzie mógł generować opisy firmowych procesów na podstawie szczątkowych informacji, jakie sztuczna inteligencja odnajdzie w dokumentach finansowych czy operacyjnych. Wszystko to stanie się możliwe dzięki cyfryzacji obiegu dokumentów.

na dziedzinowych bazach wiedzy, lepiej radzą sobie z obsługą specjalistycznych zapytań niż ChatGPT, który miał dostęp do olbrzymich, ale bardziej ogólnych zasobów informacji. To może być istotna wskazówka dla przedsiębiorstw, które chcą korzystać w swojej działalności z najnowszych narzędzi bazujących na sztucznej inteligencji. Jeśli chcą mieć w tym zakresie dobre wyniki, muszą przede wszystkim zadbać o jak najlepszą jakość danych, z których modele uczenia maszynowego będą korzystać i jak najlepszą jakość zasobów informacji, do których będą sięgać gotowe narzędzia sztucznej inteligencji.

Sposobów na zapewnienie odpowiedniej jakości danych może być wiele, w zależności od specyfiki, wielkości, sposobu działania czy strategii rynkowej danego przedsiębiorstwa. W wielu dużych firmach wdrażane są horyzontalne programy data governance, wprowadzane generalne reguły polityki zapewnienia jakości danych. W mniejszych mogą wystarczyć odpowiednio opracowane procedury przygotowywania dokumentów i wprowadzania danych do systemów, na przykład przy wystawianiu faktur czy przyjmowaniu zleceń. Tu znowu może być pole do popisu dla integratorów, żeby doradzić optymalne rozwiązanie i w ślad za tym zaproponować system informatyczny adekwatny do zdiagnozowanych uwarunkowań i potrzeb. Są dostępne różne modele mierzenia dojrzałości informacyjnej, z których można skorzystać w ramach konsultowania najlepszych rozwiązań dla klienta.

Coraz częściej w firmach pojawiają się specjalne osoby do zarządzania danymi – Chief Data Officer (CDO). Według raportu Deloitte'a „Chief Data Officer 2022" obecnie rola takich specjalistów skupia się w większości na wspieraniu działalności operacyjnej przedsiębiorstw. Docelowo jednakże współcześni CDO chcą bardziej skoncentrować się na działaniach strategicznych, koordynując wszelkie inicjatywy związane z wykorzystaniem danych na poziomie całej firmy. Nieco ponad 70 proc. uczestniczących w badaniu Deloitte'a CDO przyznało, że niewystarczający poziom umiejętności w zakresie zarządzania danymi w ich przedsiębiorstwach stanowi jeden z największych problemów.

Grupa specjalistów zajmujących się danymi jest już na tyle liczna i w Polsce, że powstało zrzeszające ich stowarzyszenie – DAMA Poland Chapter, jako polski oddział międzynarodowej organizacji DAMA International (The Global Data Management Community). Ta grupa zawodowa powinna stać się dla firm oferujących rozwiązania z zakresu zarządzania informacją jednym z głównych partnerów do rozmów biznesowych, oprócz szefów IT czy menedżerów innych działów merytorycznych, na przykład finansowo-księgowych lub handlowych. Jak bowiem pokazał ubiegłoroczny raport Gartnera, 67 proc. osób zaangażowanych w decyzje dotyczące zakupów nowych technologii nie jest już związanych z IT. Integratorzy powinni z pewnością ten fakt uwzględniać w swoich planach biznesowych. ■

Expert view

W środowisku druku bezpieczeństwo ma priorytet

„Korzystanie z dużych urządzeń przekłada się na znaczną oszczędność czasu, nawet uwzględniając konieczność podejścia do nich po odbiór wydruku – są po prostu znacznie szybsze i wydajniejsze niż drukarki nabiurkowe" – mówi **Jarosław Kolczyński, Senior Systems Engineer w firmie Fast IT, która jest partnerem Epsona o statusie Solutions+ Gold.**

■ Na ile klienci są świadomi wyzwań związanych z bezpieczeństwem danych przy obsłudze sprzętu drukująco-skanującego?

Już od kilkunastu lat jest to główny temat podczas spotkań z klientami dotyczących sprzedaży i wdrażania urządzeń wielofunkcyjnych. Często bywa ważniejszy od kwestii funkcjonalności czy jakości druku. Świadomość odnośnie do bezpieczeństwa jest zaskakująco wysoka, zwłaszcza po wprowadzeniu RODO. Nawet najbardziej oporni klienci zrozumieli wagę problemu, a na nas jako wdrożeniowców spadły dodatkowe zadania i odpowiedzialność z tym związane. Oczywiście nadal można zauważyć zróżnicowanie w skali tej świadomości, w zależności od wielkości firmy. W korporacjach poziom wiedzy z zakresu bezpieczeństwa jest bardzo wysoki, podobnie jak potrzeby. Jednak temat ten jest obecny także w małych podmiotach, używających tylko kilku urządzeń.

■ Zapewnienie bezpieczeństwa z reguły wiąże się z koniecznością wypracowania kompromisu na różnych szczeblach. Jak wygląda ten proces i czy w trakcie negocjacji dochodzi do jakichś sytuacji konfliktowych?

Raczej nie. Świadomi klienci zazwyczaj od razu w zapytaniach ofertowych precyzują jaki poziom bezpieczeństwa ich interesuje pod względem przesyłania dokumentów czy też przechowywania ich w urządzeniach drukujących i skanujących. Wówczas naszym zadaniem jest dobór odpowiedniego sprzętu czy oprogramowania, aby spełnić wymagania. Natomiast w przypadku mniej świadomych klientów zazwyczaj to my sugerujemy najbezpieczniejsze rozwiązania oraz konieczność modyfikacji procedur, aby zarówno spełnili wymagania RODO, jak też doświadczali mniejszego ryzyka wycieku poufnych danych, a więc konsekwencji finansowych, prawnych i wizerunkowych. Funkcjonujemy dla nich jako eksperci, więc muszą nam zaufać, ale ewentualne ograniczenia i konieczność kompromisu są wyłącznie dla ich dobra.

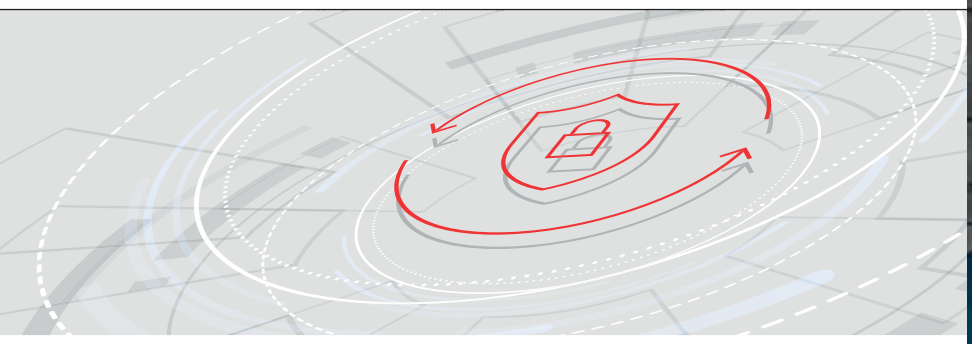
Ujednolicenie środowiska druku upraszcza wdrożenie spójnych zasad bezpieczeństwa.

■ Jakiego rodzaju modyfikacje procedur są konieczne?

Wdrożenie zaawansowanych i odpowiednio zabezpieczonych urządzeń wielofunkcyjnych przekłada się na konsekwencje dla ich użytkowników. W trakcie modernizowania środowiska skanowania i druku staramy się je optymalizować i centralizować, przykładowo poprzez eliminowanie nadmiarowych drukarek nabiurkowych i zastępowanie ich dużymi, wydajnymi „kombajnami". Proporcja tych zmian zależy od układu biura, stopnia skomplikowania budynku lub w ogóle rozproszenia firmy na kilka budynków. Zdarza się, że jedno duże urządzenie potrafi zastąpić ponad dziesięć mniejszych. Natomiast to oznacza, że użytkownik musi wstać od biurka, podejść do drukarki znajdującej się na korytarzu lub w specjalnym pokoju, dokonać uwierzytelnienia, zaczekać krótką chwilę na wydruk i odebrać dokumenty. Zdarza się, że pracownicy w początkowym okresie po wdrożeniu traktują tę nową sytuację jako uciążliwą, ale trzeba ich uświadamiać, że to jedyny sposób, aby zarówno firma, jak i bezpośrednio oni odnieśli korzyści.

■ Jakie?

Zacznijmy od tych nie związanych z bezpieczeństwem. Użytkownik wiedząc, że będzie musiał iść do urządzenia, kilka razy się zastanowi, zanim podejmie decyzję o wydrukowaniu dokumentu – często z tego zrezygnuje, co stanowi oszczędności dla firmy. A jeśli już się zdecyduje, to tylko z korzyścią dla swojego... zdrowia, bo jak wszyscy wiemy, warto czasami rozprostować kości. Paradoksalnie, korzystanie z takich dużych urządzeń przekłada się na znaczną oszczędność czasu, nawet uwzględniając konieczność podejścia do nich – są po prostu znacznie szybsze i wydajniejsze niż drukarki nabiurkowe. Kolejną korzyść zapewnia funkcja wydruku podążającego. Użytkownik może zlecić na komputerze drukowanie na kolejkę „centralną", bez wskazywania konkretnej drukarki. Następnie wystarczy podejść do dowolnego urządzenia w firmie i po uwierzytelnieniu uruchomić drukowanie. W przypadku niedostępności najbliższego sprzętu spowodowanej przykładowo awarią, brakiem materiałów eksploatacyjnych lub papieru, nie ma potrzeby ponownego generowania wydruku – wystarczy podejść do innego urządzenia. To ogromne ułatwienie dla pracowników oraz działów administracji i IT.



A korzyści związane z bezpieczeństwem?

Najważniejszą jest zminimalizowanie ryzyka wycieku danych bezpośrednio z drukowanego dokumentu. Wyobraźmy sobie firmę, w której zostało już zainstalowane duże urządzenie wielofunkcyjne, ale bez możliwości uwierzytelniania. Użytkownik zleca wykonanie wydruku, ale nie zawsze od razu go odbiera. Z różnych powodów, czasami zatrzyma go telefon albo współpracownik z ważną sprawą. W efekcie na tacy odbiorczej drukarki leży stos dokumentów. Nie dość, że trzeba później poszukać swojego, to bardzo często zdarza się, że ktoś zabiera nie swoje dokumenty, które mogą zawierać poufne informacje. Wdrożenie mechanizmów bezpieczeństwa, które uwierzytelniają użytkownika za pomocą wpisanego kodu, hasła lub po przyłożeniu karty rozwiązuje wszystkie te problemy – w ten sposób realizowana jest funkcja wydruku poufnego.

Za pomocą jakich narzędzi można uruchomić tę funkcję?

W tym celu należy wdrożyć dodatkowe oprogramowanie do centralizacji druku i skanu, chociażby Epson Print Admin, które pozwala na łatwe i przyjazne zarządzanie nawet dużymi, skomplikowanymi środowiskami druku. Można również skorzystać z mechanizmów wbudowanych w urządzenia drukujące. Najprostszy z nich polega na wcześniejszym zabezpieczeniu pliku przeznaczonego do druku, poprzez nadanie mu numeru PIN, który należy wpisać na panelu dotykowym wybranego urządzenia. To rozwiązanie dla małych firm, które chcą podnieść poziom bezpieczeństwa, ale nie potrzebują zaawansowanych funkcji wydruku podążającego. Inną opcją jest stworzenie puli kont autoryzowanych użytkowników, którzy po uwierzytelnieniu mają pełen dostęp do funkcjonalności drukarki.

Duże urządzenie potrafi zastąpić ponad dziesięć mniejszych.

W jaki sposób we wdrażaniu tych rozwiązań wspiera was Epson?

Bardzo pomocne są zbudowane przez Epsona showroomy działające jako centra wiedzy. Jest też bardzo duży nacisk, abyśmy jako autoryzowany partner mieli zaawansowaną wiedzę o rozwiązaniach oraz wykazywali się skutecznością i profesjonalizmem na etapie posprzedażowym. Jako partner Epsona doceniamy dostęp do stale aktualizowanej bazy wiedzy oraz wsparcie ze strony producenta w rozwiązywaniu bieżących problemów, również w zakresie serwisu gwarancyjnego i pogwarancyjnego. Środowisko druku to już nie tylko sprzedaż drukarek i materiałów eksploatacyjnych. To często rozbudowane, zaawansowane centra druku, często stojące na styku infrastruktury i procesów krytycznych u klienta. A niewłaściwa realizacja projektu może spowodować nieprzyjemne dla niego konsekwencje.

W jakim zakresie to wsparcie dotyczy także aspektów związanych z bezpieczeństwem?

Większość mechanizmów umożliwiających stworzenie procedur ochrony danych jest wbudowanych w rozwiązania biznesowe, w tym WorkForce Pro RIPS i Enterprise, jak też we wspomniane oprogramowanie Epson Print Admin, które umożliwia autoryzowanie użytkowników na różne sposoby w celu uruchomienia procesu druku poufnego. Zapewnia ono również szyfrowaną komunikację pomiędzy komputerami a drukarkami oraz ma funkcję wymuszającą, aby połączenie przez sieć bezprzewodową było możliwe tylko gdy jest ona zabezpieczona protokołem WPA. Administratorzy otrzymują informacje o aktualności oprogramowania drukarek oraz mają dostęp do bardzo szczegółowych raportów. Co ważne, w przypadku wykorzystania na dwóch urządzeniach EPA dostępny jest za darmo, zaś w zastosowaniach wielostanowiskowych można skorzystać z wersji serverless.

Czy jest możliwe zarządzanie sprzętem konkurencyjnych dostawców za pomocą tego oprogramowania?

Nie, ale nie należy postrzegać tego jako jego wadę. Środowiska składające się z rozwiązań wielu producentów są znacznie bardziej skomplikowane w utrzymaniu pod względem zarządzania i bezpieczeństwa ze względu na różnorodność zastosowanych w nich funkcji. Ujednolicenie środowiska druku upraszcza wdrożenie spójnych zasad bezpieczeństwa i reguł uwierzytelniania. Korzystanie z rozwiązań oraz materiałów eksploatacyjnych oferowanych tylko przez jednego dostawcę stawia też klienta w korzystniejszej pozycji negocjacyjnej. Firmy dobrze to rozumieją, dlatego tak często widzimy projekty unifikacji środowisk skanowania i druku.

EPSON®

Kontakt:
biznes@epson.pl

OCHRONA DANYCH: trudna sztuka wyboru

Budżety na rozwój infrastruktury IT w ostatnich latach pozostają niezmienne lub nieznacznie rosną. Nie można tego powiedzieć o danych, których ilość przyrasta w szaleńczym tempie i coraz trudniej nad tym zapanować. Niestety, wybór najbardziej odpowiedniego remedium nie jest zadaniem łatwym.

■ *Wojciech Urbanek*

Potok spływających zewsząd danych nie jest jedynym problemem. Postępująca migracja do chmury publicznej oraz hybrydowy model pracy przyczyniły się do ich rozproszenia, co dodatkowo utrudnia zarządzanie zasobami IT. Bieżący rok nie przyniósł też przełomu w zmaganiach z atakami ransomware. Jak wynika z danych Chainalysis, firmy analitycznej śledzącej rynek kryptowalut, ofiary w pierwszym półroczu tego roku zapłaciły grupom ransomware 449,1 mln dol. Dla porównania, w całym ubiegłym roku kwota opłaconych okupów nie przekroczyła 500 mln dol.

Zgodnie ze znanym powiedzeniem, że potrzeba jest matką wynalazków, producenci opracowują rozwiązania, które pozwalają ich użytkownikom uporać się z wyzwaniami, jakie niesie konieczność ochrony danych. Jednym z najgorętszych tematów jest wykorzystanie generatywnej sztucznej inteligencji. Dostawcy myślą o niej jako uzupełnieniu istniejącej funkcjonalności oferowanych rozwiązań. Natomiast część ekspertów od bezpieczeństwa IT dostrzega w tej technologii zdecydowanie większy potencjał.

> 59 proc. ofiar cyberataków **nadal nie chroni** swoich danych w chmurze.

Do kolejnych istotnych trendów należy zaliczyć wzrastającą rolę pamięci obiektowej, rozwój rozwiązań backupu dla SaaS czy użycie mechanizmów blockchain do przechowywania dużych ilości poufnych danych z gwarancją ich niezmienności.

Specjalizacja czy unifikacja?

Wśród produktów IT na popularności zyskują rozwiązania wielofunkcyjne. Jednak, o ile w przypadku urządzeń drukujących firma nic nie ryzykuje inwestując w wielozadaniowy kombajn, o tyle w przypadku ochrony i archiwizacji danych ma do czynienia ze znacznie bardziej delikatną materią. Pójście na łatwiznę może w ekstremalnych przypadkach skończyć się ze stratami liczonymi w milionach złotych. Jednym z przeciwników zintegrowanych rozwiązań do ochrony danych jest Paweł Mączka, CTO Storware. Jego zdaniem wyspecjalizowane narzędzia oferują znacznie większe możliwości tworzenia backupu danych z urządzeń końcowych.

– *Preferujemy takie podejście, stawiając na ciągłą ochronę danych jako najbardziej optymalne zabezpieczenie dla urządzeń końcowych. Poza tym klienci często chcą chronić tylko wybraną część danych, aby ograniczyć przestrzeń dyskową przeznaczoną na backup. Przywiązujemy wagę do deduplikacji i kompresji, aby ograniczyć koszty przechowywania kopii zapasowych. Reasumując, nie preferujemy zintegrowanych systemów, a skupiamy się na użyteczności i redukcji kosztów* – tłumaczy Paweł Mączka.

Większość małych, a także średnich firm jest skazana na wielozadaniowe rozwiązania bądź wsparcie dostawców oferujących zarządzane usługi backupu i disaster recovery. Jednakże część specjalistów zwraca uwagę, że póki co na rynku nie ma zintegrowanego narzędzia do zabezpieczania danych w całym środowisku.

– *Przyczyną takiego stanu rzeczy jest wielowarstwowość ochrony danych. Często trzeba zapewnić bezpieczeństwo w wielu lokalizacjach dla rozmaitych systemów fizycznych i oprogramowania. Jakby tego było mało, aplikacje znajdują się pod kontrolą różnych działów* – mówi Piotr Drąg, Storage Category & Data Services Business Development Manager w HPE.

Choć nie ma idealnego zunifikowanego rozwiązania, to wiele przemawia za tym, że szala będzie przechylać się w stronę

Fot. Adobe Stock

Dziś już **nikogo nie dziwią** archiwa zawierające petabajty danych.

produktów prostych w obsłudze i tanich w eksploatacji. Natomiast wyspecjalizowane narzędzia do ochrony i odzyskiwania danych pozostaną domeną klientów korporacyjnych.

– *Narzędzia do wykonywania kopii zapasowych i ich odtwarzania od dawna uznaje się za skomplikowane. Dlatego firmy szukają przede wszystkim rozwiązań, które mogą uprosić proces związany z zabezpieczeniem danych. Zminimalizowanie liczby punktów obsługi do jednego i centralizacja zarządzania to dziś bez wątpienia te elementy, dzięki którym zintegrowane rozwiązania do backupu cieszą się niesłabnącą popularnością* – mówi Michał Zalewski, inżynier w Barracuda Networks.

Poza wielkością firmy o wyborze narzędzi do ochrony danych decyduje specyfika środowiska, na którą składają się posiadane przez nią rozwiązania, liczebność zespołu IT, a także ilość danych o znaczeniu krytycznym zarówno z punktu widzenia samego przedsiębiorstwa, jak i regulatorów. Rodzime firmy bardzo często do backupu wykorzystują serwery NAS, a tacy producenci jak QNAP czy Synology dołączają do urządzeń autorskie oprogramowanie do tworzenia kopii zapasowych.

Swoich zwolenników mają też produkty PBBA (Purpose Built Backup Appliance). W ramach takiego systemu użytkownik otrzymuje sprzęt z zainstalowanym oprogramowaniem do backupu. Urządzenia te mają bogatą funkcjonalność, zapewniają między innymi deduplikację, szyfrowanie, kompresję, redundantne komponenty sprzętowe, zautomatyzowaną konfigurację i konserwację.

– *Jak do tej pory najczęściej użytkownikami systemów PBBA były małe i średnie firmy, ale obecnie duże przedsiębiorstwa przyglądają się tym urządzeniom i też zaczynają je wdrażać. Ma to związek z ekspansją biznesu oraz powstawaniem mniejszych biur i oddziałów* – zauważa Michał Zalewski.

Archiwa pękają w szwach

Szacuje się, że około 80 proc. nieustrukturyzowanych danych w firmach oraz instytucjach jest używanych sporadycznie lub w ogóle. Z tego powodu często nazywa się je zimnymi danymi. Ich ilość w przewidywalnej przyszłości będzie szybko rosnąć. Zresztą dziś już nikogo nie dziwią archiwa zawierające petabajty danych, a dostawcy rozwiązań otrzymują pierwsze zlecenia na repozytoria o powierzchni dyskowej jednego eksabajta, co jeszcze do niedawna można było spotkać jedynie u hiperskalerów.

Ciężar związany z archiwizacją danych próbują wziąć na swoje barki najwięksi dostawcy usług chmurowych: Amazon Web Services, Microsoft Azure i Google Cloud Platform. Alternatywę dla usług chmury publicznej stanowią systemy hybrydowe bądź własne serwerownie. Niejednokrotnie zdarza się, że są to tańsze rozwiązania od tego, co proponują chmurowi giganci.

Przyrost danych nieustrukturyzowanych mocno wywindował w górę akcje pamięci obiektowej. Jej największą zaletą jest możliwość grupowania urządzeń w duże pule pamięci i ich dystrybuowanie w wielu lokalizacjach, dzięki czemu można uzyskać wysoką skalowalność. Dileeshvar Radhakrishnan, inżynier w MinIO, zwraca uwagę na fakt, iż jeziora danych używają pamięci obiektowej zamiast systemów NAS czy SAN, bowiem te pierwsze nie mają sobie równych pod względem możliwości w zakresie skalowania. Założyciele relatywnie młodych firm, jak MinIO, Qumulo czy Versity uważają, że kluczowy wpływ na efektywność cyfrowych archiwów będą mieć systemy typu software defined storage (SDS).

Inną drogę wskazują dostawcy kombajnów realizujących funkcje backupu, archiwizacji, zarządzania kopiami ➤

danych, a nawet analitykę. Choć w USA czy niektórych krajach Europy Zachodniej znajdują one klientów, to w Polsce nie osiągnęły sukcesu.

– *Zakup tego typu rozwiązań może wydawać się kuszący, jednak warto pamiętać, że w każdym obszarze funkcjonalnym istnieją wyspecjalizowane firmy. W zależności od tego czy poszukujemy oprogramowania do backupu, analityki, bezpieczeństwa czy archiwizacji, warto zwrócić uwagę na produkty liderów w danych dziedzinach. Jeśli jest to możliwe, zalecaną praktyką jest integrowanie najlepszych w swojej klasie rozwiązań* – mówi Andrzej Niziołek, dyrektor regionalny na Europę Środkowo-Wschodnią w Veeam.

Nie mniej ciekawie wygląda rywalizacja w segmencie nośników do archiwizacji, gdzie na fali wznoszącej wciąż znajdują się taśmy. W ubiegłym roku technologia zapisu LTO pobiła kolejny rekord, producenci sprzedali taśmy o łącznej pojemności 148,3 eksabajtów. Oczywiście broni nie składają producenci dysków twardych, o czym świadczy chociażby przykład WD, które na początku bieżącego roku wprowadziło do sprzedaży nośnik o pojemności 26 TB z przeznaczeniem głównie dla centrów danych. Trochę kolorytu do tej rywalizacji wprowadza amerykański startup VAST Data, który zachęca do archiwizacji danych na... pamięciach flash QLC.

Backup dla SaaS

Według raportu „State of SaaSOps 2023" w 2022 r. przeciętna firma korzystała średnio ze 130 aplikacji chmurowych, a rok wcześniej ze 110. Popularność SaaS rośnie w szybkim tempie, ale nie zawsze idzie to w parze ze świadomością w zakresie ochrony danych. Jak wynika z badania przeprowadzonego przez Enterprise Strategy Group (ESG), użytkownicy SaaS najczęściej tracą dane w wyniku awarii u dostawcy usług (35 proc.), a w dalszej kolejności cyberataku (34 proc.), przypadkowego skasowania przez pracownika (33 proc.), po zamknięciu konta (29 proc.), a także z powodu stosowania niewłaściwych mechanizmów backupu (28 proc.). Co istotne, dostawca usługi poczuwa się do odpowiedzialności jedynie w pierwszym z wymienionych przypadków. Jeszcze do niedawna wielu usługobiorców nie miało o tym zielonego pojęcia i było przekonanych, że nie trzeba inwestować w narzędzia backupu dla SaaS.

– *Zauważamy wzrost świadomości użytkowników dotyczącej odpowiedzialności za ochronę danych przechowywanych w aplikacjach SaaS zarówno w Polsce, jak i na świecie. Klienci zaczynają sobie zdawać sprawę z zagrożeń związanych z tym modelem i poszukują dodatkowych zabezpieczeń. Z tą wiedzą docierają do nich zarówno dostawcy narzędzi do backupu, jak i sami usługodawcy, którzy jaśniej formułują przepisy dotyczące bezpieczeństwa i prywatności danych* – tłumaczy Paweł Mączka.

Największym popytem wśród rozwiązań backupu dla SaaS cieszą się produkty chroniące użytkowników Microsoft 365. Nie powinno to dziwić, bowiem autorzy raportu Veeam Cloud Protection Trends Report 2023 informują, że 80 proc. spośród cyberataków wymierzonych w klientów usług chmurowych jest skierowanych przeciwko użytkownikom Microsoft 365. Wprawdzie świadomość na temat zagrożeń, jakie niesie ze sobą SaaS, wzrosła, ale wciąż jest daleka do ideału. Aż 59 proc. respondentów biorących udział w badaniu ESG przyznało, że nie robią nic, aby chronić dane w chmurze. Pikanterii dodaje fakt, iż ankietowani wywodzili się wyłącznie z firm, które wcześniej już doświadczyły utraty danych.

Dostępność: mierzyć siły na zamiary

Analitycy wyliczają straty wywołane przez przestoje infrastruktury IT bądź brak dostępu do ważnych informacji. Co jednak zrobić, aby zapobiec takim sytuacjom? W pierwszym rzędzie należałoby określić kryteria dostępności. Według badań przeprowadzonych przez Gartnera jedynie 30 proc. radzi sobie z tym zadaniem, a 70 proc. nie ma określonego celu w zakresie dostępności i nie wie, jak go osiągnąć. W wielu firmach panuje przekonanie, że „jakoś to będzie" lub „nic nam nie zagraża". Co więcej, czasami pracownicy działów IT nie zawracają sobie głowy wskaźnikami RTO czy RPO, które powinny być ustalone lub przynajmniej zaakceptowane przez zarząd.

– *Nieraz spotykam się z sytuacjami, gdy klienci zachowują błogi spokój, wychodząc z założenia, że jeśli aplikacje przez pewien czas nie będą działać, to nic wielkiego się nie wydarzy. Jednak w większości przypadków dzieje się na odwrót, a otrzeźwienie przychodzi z pierwszą poważniejszą awarią* – podkreśla Piotr Drąg.

Są też klienci, którzy chcieliby zapewnić maksymalny poziom ochrony swoich danych jak najniższym kosztem. Niestety, są to oczekiwania nierealne. Takie firmy w czasie negocjacji z dostawcami przekonują ich, że nie mogą sobie pozwolić na brak dostępności, a nawet krótką przerwę. Nigdy nie idą za tym konkretne wyliczenia pokazujące wielkość strat finansowych spowodowanych przez przestój.

– *Firmy nie podejmują próby oszacowania kosztów, dajmy na to, jednogodzinnego zawieszenia usługi. Taka analiza ułatwiłaby podjęcie decyzji o wdrożeniu odpowiednich rozwiązań i zapewnieniu dostępności do kluczowych usług, a tych nie brakuje. Bardzo funkcjonalne są układy hybrydowe, szczególnie przydatne do dublowania*

Zdaniem integratora

Mirosław Malinowski, Manager GIDC EE, Local ITO Delivery Poland, DXC Technology

W procesach związanych z zabezpieczaniem danych musimy zmierzyć się z dwoma wyzwaniami: szybkością i częstotliwością tworzenia backpu oraz czasem dostępu do danych w przypadku ich utraty. Dobrze radzą sobie z tym wirtualne biblioteki taśmowe. Nie bez przyczyny cieszą się one rosnącą popularnością. Osobną grupą urządzeń, znajdującą się na fali wznoszącej, są specjalistyczne systemy do archiwizacji, które umożliwiają jednokrotny zapis danych, ale nie pozwalają na ich modyfikację. Nie zastąpią one backupu, ale pozwalają na bezpieczne, długotrwałe przechowywanie plików w sposób zapobiegający ich utracie czy zniekształceniu.

krytycznych funkcji i eliminowania pojedynczych punktów awarii – tłumaczy Maciej Wójcicki, IT Solutions Architect w ITBoom.

Oferta producentów w zakresie rozwiązań zapewniających wysoką dostępność wychodzi naprzeciw oczekiwaniom różnych grup odbiorców. Replikacja synchroniczna gwarantuje powrót do pracy po kilku sekundach. Ważną rolę w disaster recovery odgrywa ciągła ochrona danych (CDP), która pozwala na przywracanie danych z kopii zapasowej od kilkudziesięciu sekund do kilku minut. Stałe postępy czynią też producenci rozwiązań do backupu, niektórzy chwalą się parametrami RPO na poziomie 5–15 sekund, a RTO – kilku minut.

Warto też zwrócić uwagę na takie rozwiązania, jak cybervault lub cyberbunkier. To odizolowane od infrastruktury IT kopie danych, dla których opracowane są procedury odtworzeniowe dla krytycznych systemów.

Alternatywa dla RAID i replikacji

Mechanizm RAID, zabezpieczający dane przed awarią nośników w macierzy dyskowej ma już swoje lata – zbliża się powoli do czterdziestki. Dlatego nie zawsze radzi sobie z konsekwencjami wynikającymi ze współczesnych wyzwań, takich jak lawinowy przyrost danych, wzrost pojemności dysków czy rozwój usług chmury publicznej. W centrach danych najczęściej spotyka się dwa poziomy macierzy RAID – 5 oraz 6. Oba zapewniają solidną ochronę, ale mają pewne mankamenty. RAID 5 gwarantuje dalsze funkcjonowanie systemu i zachowanie danych w wyniku awarii jednego dysku, zaś jeśli zawiodą kolejne, użytkownik musi liczyć się ze stratą danych.

RAID 6 powstał w reakcji na sytuację, gdy przy odbudowywaniu struktury macierzy RAID 5 po wymianie uszkodzonego dysku na nowy wszystkie pozostałe są nadmiernie obciążone. Czasami dochodziło wówczas do kolejnej awarii – już bez koła ratunkowego. Dlatego RAID 6 zapewnia użytkownikom większy spokój, gdyż toleruje uszkodzenie dwóch nośników. Niestety, odbudowa struktury danych przy użyciu macierzy RAID jest czasochłonna. Dla RAID 6 i nośnika 10 TB proces ten trwa około 14 godzin.

Dlatego od kilku lat rośnie popularność mechanizmu erasure coding, który świetnie radzi sobie też z pamięciami obiektowymi. Dzieli obiekty na dane i bloki parzystości, gdzie te ostatnie wspierają rekonstrukcję brakujących lub uszkodzonych bloków danych. Zastosowanie takiego rozwiązania zmniejsza zapotrzebowanie na przestrzeń dyskową w porównaniu z RAID czy replikacją. Poza tym umożliwia odzyskanie danych w przypadku awarii dwóch lub większej liczby komponentów macierzy (dysków, kontrolerów).

Erasure coding wypada bardzo korzystnie na tle replikacji pod kątem użycia przestrzeni dyskowej. Wielu użytkowników rozproszonych systemów pamięci masowych stosuje replikację trójstronną (dane są zapisywane w trzech różnych węzłach). Jest to bardzo bezpieczna opcja, bowiem gwarantuje dostępność na poziomie 99,9999 proc. Niestety, za bezpieczeństwo trzeba słono zapłacić. Na przykład dla replikacji 10 PB danych potrzebna jest powierzchnia dyskowa 30 PB. Natomiast obiektowa pamięć masowa, w której wykorzystuje się erasure coding, wymaga od 15 do 20 PB, w zależności od konfiguracji proporcji danych do bloków parzystości.

Słabą stroną erasure coding jest duże zapotrzebowanie na moc obliczeniową. Przy zaawansowanych konfiguracjach wydajność systemu wyraźne spada. Poza tym jest to mechanizm opracowany z myślą o obsłudze rozwiązań do backupu czy archiwizacji. W związku z tym nie nadaje się do ochrony danych w środowiskach produkcyjnych. Dlatego wszystko wskazuje na to, że RAID, replikacja i erasure coding znajdą w najbliższych latach sporo zastosowań i żadna z tych metod na razie nie odejdzie do lamusa. ■

Zdaniem specjalisty

Paweł Chruściak, DPS Account Executive, Dell Technologies

Integracja oprogramowania i sprzętu do jednego systemu typu „wszystko w jednym" to trend, który obserwujemy już od ponad dziesięciu lat. Wybierając tego typu rozwiązanie, należy dokładnie przeanalizować swoje wymagania, te na dziś, ale także na jutro. Jeśli system rzeczywiście jest w stanie spełnić owe założenia, to wybór w pełni zintegrowanego rozwiązania może znacznie uprościć zarządzanie takimi procesami jak tworzenie kopii zapasowych, redukcję kosztów oraz rozbudowę systemu w przyszłości.

Mirosław Chełmecki, Data Center & Cloud Department Director, Exclusive Networks

Wielu producentów prowadzi prace nad wykorzystaniem sztucznej inteligencji i uczenia maszynowego w swoich produktach do backupu i archiwizacji. Ich zastosowanie może przynieść wiele korzyści w przyszłych implementacjach. Możemy do nich zaliczyć usprawnienie automatyzacji procesu backupu, automatyczne podejmowanie decyzji w miejscach, gdzie obecnie wykonywane jest to przez człowieka, zapewnienie większego poziomu bezpieczeństwa przez analizę logów i innego rodzaju danych w celu wykrywania anomalii. Powyższe elementy zmniejszą koszty administracyjne oraz podniosą bezpieczeństwo.

Alexander Ivanyuk, Senior Director Technology, Acronis

Podejście użytkowników usług SaaS do ochrony danych jest zróżnicowane. Wiele firm i osób prywatnych rozumie wartość tworzenia kopii zapasowych, ale nadal może to robić nieprawidłowo, chociażby nie przechowując kilku kopii w różnych lokalizacjach. Bezpieczeństwo danych w chmurze nie powinno budzić wielu obaw, jeśli ich dostawcą jest wyspecjalizowana fima. Tacy usługodawcy korzystają z odpowiednio chronionych centrów danych i bezpiecznego dostępu do chmury, a także przestrzegają ścisłych umów SLA dotyczących tych aspektów.

Przechowywanie i zabezpieczanie danych: wszystko w cenie

Serwery NAS, zaprojektowane przez inżynierów Synology, mogą służyć jako ekonomiczne, uniwersalne rozwiązanie do przechowywania danych, zabezpieczania ich przed utratą oraz gwarantowania ich wysokiej dostępności.

Komfort prowadzenia biznesu jest w bardzo dużym stopniu zależny od szeroko zakrojonej strategii dotyczącej przechowywania i zabezpieczania danych. Tak, aby dzięki bazującym na niej procedurom wyeliminować ze środowiska IT wszystkie słabe ogniwa. Synology ma w portfolio komplet rozwiązań (sprzęt, oprogramowanie, usługi chmurowe), które umożliwiają stworzenie pełnego środowiska przechowywania danych w celu ich bieżącego przetwarzania, zapewniania wysokiej dostępności oraz backupu i odzyskiwania.

Żeby uzyskać taką funkcjonalność, w centrali firmy należy zainstalować serwer NAS jako główne repozytorium danych – dostęp do nich będzie możliwy z komputerów poprzez lokalną sieć (np. protokół SMB) lub internet z aplikacji mobilnych oraz poprzez portal web. Opcjonalnie możliwe jest wdrożenie drugiego serwera, na który za pomocą narzędzia **Synology High Availability** będzie wykonywana w czasie rzeczywistym synchronizacja wszystkich danych i usług, a w razie awarii głównego serwera zapasowy natychmiast przejmie jego zadania. Jeżeli firma ma oddziały, w każdym z nich można wdrożyć mniejszy serwer NAS – na takie urządzenie przez internet synchronizowane będą pliki, do których pracownicy danego oddziału potrzebują mieć szybki dostęp.

Ochrona danych bez granic

Synology zapewnia równie bogate możliwości, jeśli chodzi o backup danych. Kopie zapasowe plików ze stacji roboczych, serwerów (w tym innych serwerów NAS), środowisk wirtualnych i aplikacji chmurowych mogą być gromadzone na dowolnym serwerze NAS w całym środowisku. Do wykonywania kopii plików na serwer ze stacji roboczych służy narzędzie Synology Drive, zaś do synchronizacji danych w chmurze – Cloud Sync. Zabezpieczanie danych możliwe jest także za pomocą mechanizmu migawek uruchamianych wewnątrz tego samego serwera, który udostępnia dane do produkcyjnego użycia, albo replikowanych na inny NAS Synology.

Za pomocą instalowanej na serwerze aplikacji **Hyper Backup** można wykonać dodatkową kopię danych – na kolejny serwer, podłączony przez port USB zewnętrzny zasób dyskowy lub do chmurowego repozytorium. Warto rozważyć skorzystanie z usługi **Synology C2 Storage** jako wydajnego chmurowego miejsca docelowego kopii zapasowej z obsługą deduplikacji i opcją przechowywania wielu wersji.

Stworzone przez Synology oprogramowanie **Active Backup for Business**, przeznaczone dla systemów Windows, Linux i macOS, umożliwia również szybkie odzyskiwanie danych według założonego wcześniej scenariusza, w tym tworzenie kopii bare-metal, przywracanie pojedynczych plików oraz natychmiastowe przywracanie backupu do pracy jako maszyny wirtualnej. Oprócz ochrony pecetów i fizycznych serwerów, możliwe jest również zabezpieczenie systemu Synology DSM oraz maszyn wirtualnych Hyper-V i VMware.

Użytkownicy serwerów NAS firmy Synology serii Plus i wyższych mają prawo do bezpłatnego korzystania z aplikacji Active Backup for Business. Wszystkimi zdefiniowanymi w niej zadaniami tworzenia pełnych kopii zapasowych można zarządzać za pomocą jednej centralnej konsoli, co upraszcza wdrożenie systemu backupu oraz minimalizuje ryzyko popełnienia błędu, jak też ogranicza ilość czynności konserwacyjnych.

Inżynierowie Synology zadbali też o kwestie optymalizacji procesu backupu – możliwe jest tworzenie przyrostowych kopii, a wszystkie pliki podlegają deduplikacji. Przekłada się to na zmniejszenie zużycia pojemności nośników oraz skrócenie czasu kopiowania danych, co ma znaczenie przy przesyłaniu ich w wolnej sieci lub przez internet. Można też zaplanować, aby backup wykonywany był poza godzinami pracy oraz sztucznie ograniczyć prędkość transmisji, żeby uniknąć przeciążenia sieci. Kopie zapasowe mogą być zaszyfrowane kluczem AES-256, aby ochronić je przed wyciekiem w przypadku ataku przeprowadzonego online lub w razie fizycznej kradzieży nośników.

Dla użytkowników pakietów biurowych w postaci usługi chmurowej dostępne są dodatkowe aplikacje. **Active Backup for Microsoft 365** umożliwia zabezpieczanie danych przechowywanych w usługach Exchange Online, OneDrive for Business, SharePoint Online i Teams, niezależnie od tego, czy klient posiada plan Business, Enterprise czy Education. Natomiast **Active Backup for Google Workspace** zapewnia tworzenie zapasowych kopii danych zapisanych w poczcie Gmail, aplikacjach Dysk, Kontakty i Kalendarz Google.

Synology

Dodatkowe informacje:
Przemysław Biel, Sales Channel Manager Poland, Synology
pbiel-a@synology.com

all of backup | EXCLUSIVE NETWORKS

#RazemMożemyWięcej

- wydarzenia dla Twoich klientów
- kampanie marketingowe
- lead generation
- case study
- mailingi
- baza wiedzy

WIĘCEJ NA:

www.backup.info.pl

EXAGRID FUJITSU Hewlett Packard Enterprise QUALSTAR Quantum storware VEEAM

Od kontroli do imitacji

Wielorakość potrzebnych form ochrony poufnych danych daje integratorom wiele możliwości działania. Do nowych wyzwań należy uwzględnienie skutków wykorzystania sztucznej inteligencji.

Andrzej Gontarz

Jeżeli prawdą jest, że dane stanowią siłę napędową współczesnej gospodarki i mają kluczowe znaczenie dla budowania przewagi konkurencyjnej przedsiębiorstw, to najważniejszym wyzwaniem biznesowym staje się dzisiaj ich ochrona. Obecnie znaczenie danych dodatkowo rośnie w związku z rozwojem zastosowań systemów sztucznej inteligencji. Ich twórcy, aby rozwijać coraz skuteczniejsze modele uczenia maszynowego, potrzebują dostępu do coraz większej ilości danych o jak najlepszej jakości. A z tym właśnie jest spory problem. Nie wszyscy dysponują potrzebnymi zbiorami właściwych informacji, a ci, którzy je posiadają, nie chcą się nimi dzielić z innymi, właśnie ze względu na ich wyjątkowe znaczenie dla powodzenia własnych strategii biznesowych.

Rośnie **liczba przypadków naruszeń** RODO w Polsce.

Z drugiej strony istnieją dane poufne, których udostępnianie jest ograniczone na mocy stosownych regulacji prawnych. Zgodnie z obowiązującą ustawą o zwalczaniu nieuczciwej konkurencji z 1993 r. do tajemnicy przedsiębiorstwa należą informacje posiadające wartość gospodarczą, ale które nie są powszechnie znane albo nie są łatwo dostępne dla osób nimi zainteresowanych (np. bazy klientów, receptury, informacje o kontrahentach, plany produkcji, informacje o rynkach zbytu itp.).

Z kolei informacje podlegające szczególnej ochronie ze względu na interes państwa wskazuje ustawa o ochronie informacji niejawnych z 2010 r. Określa ona zasady zabezpieczania czterech grup informacji: zastrzeżonych, poufnych, tajnych i ściśle tajnych. Ustawowej ochronie podlegają też tajemnice związane z funkcjonowaniem poszczególnych zawodów, branż i sektorów, np. bankowa, telekomunikacyjna, lekarska, prawnicza, dziennikarska, jak również tajemnica korespondencji, negocjacji, statystyczna czy geologiczna.

Poufność i integralność

Szczególny rodzaj informacji poufnych stanowią dane osobowe. Zasady korzystania z nich i ich ochrony definiuje unijne rozporządzenie, znane u nas powszechnie jako RODO. Jego artykuł 5 nakłada wprost na administratora danych osobowych obowiązek zapewnienia ich poufności i integralności. Muszą być one przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, „w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych".

W kontekście rosnącej popularności narzędzi bazujących na technikach sztucznej inteligencji warto też zwrócić uwagę na art. 22 RODO. Nakłada on na administratora danych zakaz zautomatyzowanego podejmowania decyzji w stosunku do osoby, której dotyczą przetwarzane dane. Osoba taka, jak czytamy w rozporządzeniu, „ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa". Chyba, że dana osoba sama wyrazi na to zgodę.

Wymogi wynikające z RODO powinni uwzględniać w swoich działaniach również sami twórcy rozwiązań z zakresu sztucznej inteligencji. Jak zwracali uwagę uczestnicy zorganizowanej przez Urząd

Fot. Adobe Stock

Ochrony Danych Osobowych konferencji „Sztuczna inteligencja w kontekście ochrony danych osobowych", obowiązek ten powinien być uwzględniany już na etapie projektowania stosownych narzędzi AI (data protection by design – art. 25 ust. 1 RODO). Powinny one funkcjonować zgodnie z zasadą domyślnej ochrony danych (data protection by default), wskazanej w ust. 2 art. 25. Obowiązkiem producentów systemów sztucznej inteligencji jest także przeprowadzenie oceny skutków przetwarzania danych w ich systemach w celu ich ochrony.

Nie tylko RODO

Przedsiębiorcy zajmujący się dostarczaniem produktów bądź usług związanych z ochroną danych osobowych powinni mieć na uwadze również to, że RODO nie jest jedynym, obowiązującym w naszym kraju aktem prawnym regulującym działania z tego zakresu. Dostosowaniu unijnego rozporządzenia do polskiego porządku prawnego służy uchwalona w 2018 r. ustawa o ochronie danych osobowych. Określa ona kompetencje organu nadzoru w postaci Urzędu Ochrony Danych Osobowych (UODO), zasady powoływania inspektorów ochrony danych w firmach i instytucjach oraz ich uprawnienia, warunki prowadzenia kontroli przestrzegania obowiązujących regulacji i zasady postępowania w przypadku stwierdzonych naruszeń, w tym nakładania stosownych sankcji, czy też tryb dochodzenia roszczeń cywilnych przed sądem.

Konieczne było też dostosowanie do wymogów RODO wielu już istniejących wcześniej w naszym kraju przepisów. Nowelizacji pod tym kątem poddano 162 polskie akty prawne dotyczące różnych branż oraz obszarów społeczno-gospodarczych (m.in. administracja publiczna, oświata, telekomunikacja, bankowość i ubezpieczenia, opieka zdrowotna, działalność prawnicza i doradcza). Stosowne zmiany wprowadzono też w kodeksie pracy i ustawie o zakładowym funduszu świadczeń socjalnych, ustawie o świadczeniu usług drogą elektroniczną, czy też w prawie telekomunikacyjnym.

Sprawnie i skutecznie

Dane są poufne dopóty, dopóki jedynie osoby upoważnione mają do nich dostęp. Trzeba mieć zatem możliwość skutecznego kontrolowania, kto próbuje z nich ➤

Wycieki i włamania

Rośnie liczba stwierdzonych naruszeń ochrony danych osobowych w Polsce. W 2022 r. do UODO zgłoszono niemal 13 tys. takich przypadków, czyli prawie dwa razy więcej niż dwa lata wcześniej (7,5 tys.). Jak wynika z badania przeprowadzonego w maju 2023 r. przez IMAS International na zlecenie ChronPESEL.pl i Krajowego Rejestru Długów Biura Informacji Gospodarczej, ponad 13 proc. respondentów doświadczyło wycieku swoich danych z firm (7,5 proc.) i instytucji publicznych (5,6 proc.). Z kolei 22 proc. badanych stwierdziło, że nie ma pewności, czy ich dane nie trafiły w ręce przestępców. Ponadto jedna trzecia uczestników badania potwierdziła, że w ciągu ostatniego roku zetknęła się z próbą wyłudzenia swoich danych osobowych przez telefon, link bądź e-mail, a 12 proc. padło ofiarą takiego oszustwa. Niemal 6 proc. badanych Polaków przyznało, że doświadczyło kradzieży danych w wyniku włamania na komputer lub telefon.

Wyłudzanie
na pierwszym miejscu

Jak wynika z raportu przygotowanego przez specjalistów Acronisa, wyłudzanie informacji wciąż jest najpopularniejszą formą kradzieży danych uwierzytelniających – globalnie odpowiada za 73 proc. wszystkich ataków. Na drugim miejscu znajdują się włamania do firmowej poczty e-mail, które stanowią 15 proc. ataków. Jak podają autorzy raportu, tylko w pierwszej połowie 2023 r. liczba ataków związanych z wyłudzaniem informacji przez wiadomości e-mail wzrosła o 464 proc. w porównaniu z 2022 r. W tym samym okresie liczba ataków na firmy i instytucje wzrosła o 24 proc. Cyberprzestępcy zaczęli wykorzystywać bazujące na dużych modelach językowych systemy sztucznej inteligencji do tworzenia, automatyzacji i ulepszania nowych ataków.

korzystać i blokować wszelkie próby nieautoryzowanego dostępu. W tym celu potrzebna jest na samym początku odpowiednia klasyfikacja zasobów pod kątem warunków ich udostępniania – kto, kiedy, w jakich okolicznościach, do jakich celów może z nich korzystać. Ważne jest w tym kontekście również określenie ról użytkowników pod kątem uprawnień dostępu do danych oraz stworzenie zasad uniemożliwiających osobom nieuprawnionym korzystanie z danych poufnych. Potrzebne są również narzędzia, które egzekwowanie tych zasad będą wspomagały lub wręcz automatycznie je realizowały.

Ochrona danych musi być zapewniona na wielu płaszczyznach i w wielu obszarach – nie tylko w odniesieniu do gromadzenia i przechowywania danych, lecz także ich przetwarzania, przesyłania i wykorzystania w poszczególnych procesach biznesowych. Potrzebne są zatem działania polegające na zabezpieczaniu informacji przed nieautoryzowanym dostępem w wielu miejscach i sytuacjach. Należy jednak przy tym pamiętać, że kontrola dostępu musi być na tyle sprawna i elastyczna, by nie utrudniać lub nie ograniczać osobom uprawnionym korzystania z danych, a przy tym na tyle skuteczna i wiarygodna, by zapewnić faktyczną ochronę tych poufnych.

Przydatne w takich działaniach będą narzędzia do klasyfikacji danych. Pozwalają one na indeksowanie przetwarzanych informacji pod kątem ich znaczenia dla bezpieczeństwa firmy. Dzięki temu możliwa jest potem ich automatyczna ochrona, jak chociażby blokowanie dostępu osobie nieupoważnionej, czy też uniemożliwienie przesłania drogą mailową poza firmę. Dokładna klasyfikacja zwiększa trafność podejmowanych przez systemy informatyczne decyzji, co w konsekwencji oznacza większą skuteczność ochrony newralgicznych zasobów.

Na rynku dostępna jest cała gama rozwiązań umożliwiających sprawne kontrolowanie dostępu do danych. Zgodnie z wytycznymi ITIL (Information Technology Infrastructure Library) zarządzanie uprawnieniami dostępowymi pomaga w kontrolowaniu poufności i integralności zasobów informacji. Można stosować do tego celu systemy uwierzytelniania, kontroli tożsamości, blokowania nieuprawnionego dostępu, czy też zarządzania kontami uprzywilejowanymi. Narzędzia do kontroli dostępu są generalnie coraz bardziej zaawansowane technicznie, gdyż oferują coraz więcej funkcji i możliwości ochrony firmowych zasobów. Część z nich bazuje na algorytmach sztucznej inteligencji, pozwalających na automatyzowanie wielu działań.

Rośnie znaczenie danych syntetycznych.

Narzędzia typu SSO (Single Sign-On) umożliwiają pracownikom jednorazowe, centralne logowanie do wszystkich przydzielonych zasobów, systemów i usług sieciowych, przez co pozwalają na skuteczniejszą kontrolę dostępu. Z kolei systemy klasy Identity Management (IM) i Identity and Access Management (IAM) służą do zarządzania tożsamością i dostępem poprzez przypisywanie użytkowników do określonych grup oraz ról, wyznaczanie im zakresu dostępu do danych treści. Monitorowaniu dostępu uprzywilejowanych użytkowników służą natomiast systemy klasy PAM (Privileged Access Management).

Anonimizacja daje nowe możliwości działania

Sposobem ochrony danych osobowych może być także ich anonimizacja. Polega ona na usunięciu wszystkich informacji umożliwiających identyfikację konkretnej osoby, której dane dotyczą. Dane zanonimizowane nie są już danymi osobowymi, więc nie podlegają regulacjom RODO. Anonimizację, w przeciwieństwie do pseudonimizacji, cechuje bowiem nieodwracalność. Z założenia, po jej wykonaniu nie da się już zidentyfikować poszczególnych osób.

Anonimizacja to, inaczej mówiąc, trwałe zastąpienie lub usunięcie danych osobowych. Służy ona do tworzenia zbiorów danych, które wyglądają strukturalnie podobnie do oryginalnych, ale mają ukryte informacje poufne. Metoda ta sprawdzi się zwłaszcza w sytuacjach, gdy istnieje potrzeba wykorzystania zasobów informacyjnych zawierających dane osobowe do innych celów niż określone przy ich zbieraniu. Może mieć zastosowanie w procesach analitycznych, przy testowaniu aplikacji w środowisku produkcyjnym, czy pozwalać na przekazywanie zbiorów informacji innym podmiotom przy współpracy nad tworzeniem nowych produktów lub usług.

Istnieje wiele technik i metod anonimizacji danych. W każdym przypadku dane modyfikowane są w nieco inny sposób. Wybór odpowiedniego rozwiązania zależy od konkretnej sytuacji i celów, jakim przekształcenia danych mają służyć. Na rynku dostępnych jest wiele narzędzi do anonimizacji danych – od bezpłatnych programów udostępnianych w modelu open source, po rynkowe produkty od wyspecjalizowanych dostawców.

Sztuczne też użyteczne

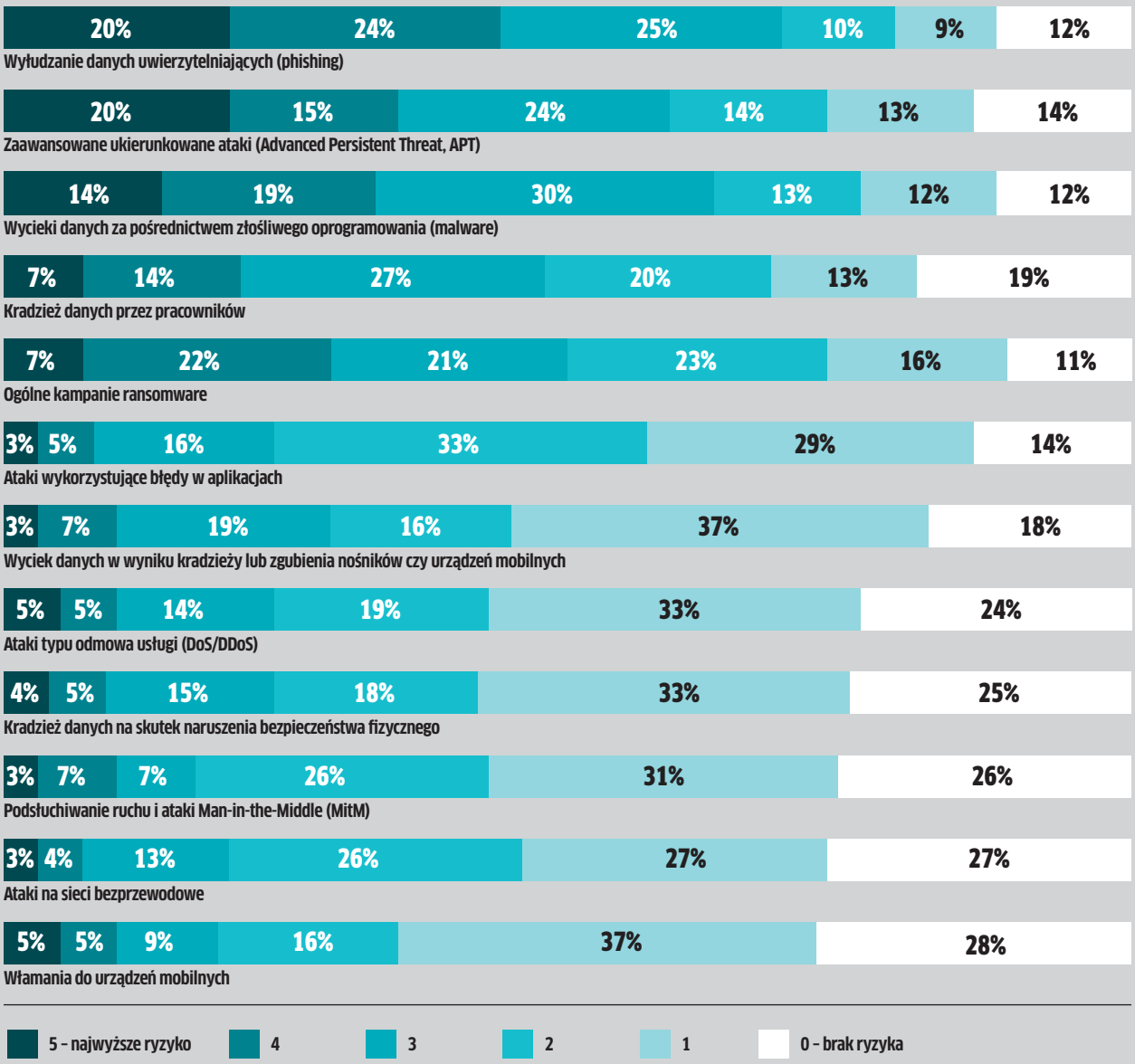
Może się jednak okazać, że w obliczu dynamicznego rozwoju technicznego i idących w ślad za nim możliwości cyberprzestępców, anonimizacja może być już w niektórych przypadkach niewystarczająca, bądź jej zastosowanie wiązałoby się ze zbyt dużym ryzykiem naruszenia prywatności

Zdaniem integratora

Rafał Barański, CEO, braf.tech

Systemy klasyfikacji danych i weryfikacji uprawnień dostępu stanowią kluczowy element w zapewnianiu bezpieczeństwa informacji w firmach. Doskonałym przykładem takiego rozwiązania jest system klasy Identity Governance and Administration (IGA). Integruje on funkcje zarządzania tożsamością i uprawnieniami dostępu, przez co umożliwia automatyczne i ciągłe monitorowanie uprawnień w całej firmie. Ma też funkcje audytu i raportowania, które pomagają w zrozumieniu kto ma dostęp do jakich danych i dlaczego. Kluczową rolę w systemach IGA odgrywa klasyfikacja danych. Są one kategoryzowane na podstawie różnych kryteriów, takich jak poziom wrażliwości, zgodność z przepisami, wartość dla przedsiębiorstwa itp. Na podstawie tych kategorii, zapadają decyzje, kto powinien mieć dostęp do określonych informacji.

Cyberzagrożenia stwarzające największy poziom ryzyka dla firm



Źródło: Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu; KPMG 2023

osób, których dane dotyczą. Rozwiązaniem problemu w takiej sytuacji mogą być dane syntetyczne. Są one sztucznie generowane z wykorzystaniem programów sztucznej inteligencji w celu imitacji danych rzeczywistych, z odzwierciedleniem ich faktycznych cech. W związku z dużym zapotrzebowaniem na dane do trenowania modeli uczenia maszynowego dane syntetyczne są też chętnie wykorzystywane przez samych twórców systemów sztucznej inteligencji.

W ostatnim czasie opracowano wiele technik i metod generowania danych syntetycznych, bazujących zarówno na modelach statystycznych, jak i głębokiego uczenia maszynowego. Na rynku jest już też dostępnych wiele różnych narzędzi i platform do generowania danych syntetycznych. Mogą one być tworzone zarówno na bazie danych rzeczywistych, jak i bez ich udziału, tylko za pomocą istniejących modeli w procesach matematyczno-statystycznych. Wytworzone w taki sposób dane syntetyczne nie są powiązane w żaden sposób z informacjami poufnymi, ale zachowują cechy danych rzeczywistych.

Jak piszą autorzy przygotowanej przez NASK „Analizy rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych", w przeciwieństwie do informacji anonimizowanych i pseudonimizowanych „dane syntetyczne nie są modyfikacją danych rzeczywistych. Składają się z nowych, całkowicie fałszywych, ale realistycznych informacji, których nie można powiązać z prawdziwymi osobami". Ten sposób radzenia sobie z wyzwaniami dotyczącymi ochrony danych poufnych, przy jednoczesnej potrzebie zapewnienia odpowiednich informacji do trenowania modeli sztucznej inteligencji, może zyskiwać na znaczeniu. ■

Indeks firm

CRN

VADEMECUM
VAR-ÓW i INTEGRATORÓW

DODATEK SPECJALNY DO MIESIĘCZNIKA
CRN POLSKA
www.CRN.pl

wrzesień 2023
PL ISSN 1640-9183

REDAKCJA
Aleja Stanów Zjednoczonych 51, lok. 508
04-028 Warszawa
redakcja@crn.pl

Tomasz Gołębiowski
(redaktor naczelny)
tel. 608 425 699
tomasz.golebiowski@crn.pl

Krzysztof Jakubik
(redaktor prowadzący)
tel. (22) 24 42 923
krzysztof.jakubik@crn.pl

Karolina Marszałek
(sekretarz redakcji)
karolina.marszalek@crn.pl

Andrzej Gontarz
andrzej.gontarz@crn.pl

Tomasz Janoś
tomasz.janos@crn.pl

Wojciech Urbanek
wojciech.urbanek@crn.pl

GRAFIKA, LAYOUT, KOORDYNACJA PRODUKCJI:
Tomasz Baziuk

FOTOGRAFIA NA OKŁADCE
Adobe Stock

FOTOGRAFIE
Adobe Stock, archiwum

PRENUMERATA
prenumerata@crn.pl

WYDAWCA
Peristeri Sp. z o.o.
Aleja Stanów Zjednoczonych 51, lok. 508
04-028 Warszawa

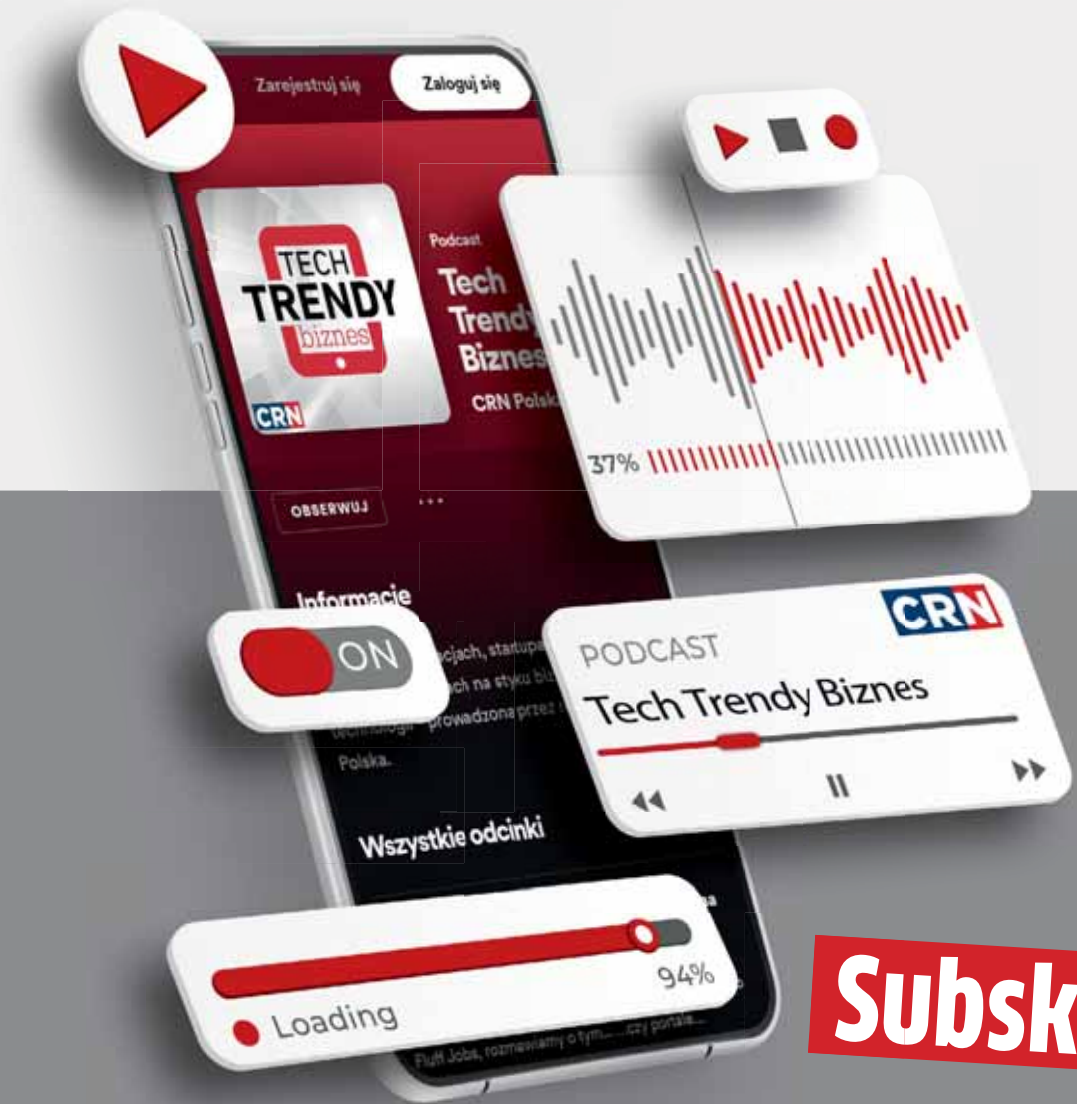
REKLAMA I PROJEKTY SPECJALNE
Agata Myśluk
tel. 694 455 426
agata.mysluk@crn.pl

Jacek Goszczycki
tel. 601 935 513
jacek.goszczycki@crn.pl

Reklamy są przyjmowane w siedzibie wydawnictwa. Za treść ogłoszeń redakcja nie ponosi odpowiedzialności.

Słyszałeś?

Co miesiąc na kanale CRN Polska (YouTube) nowa audycja Tech Trendy Biznes!



Subskrybuj

i słuchaj audycji Tech Trendy Biznes na YouTube, Spotify i Apple Podcasts!

NAKIVO®

Szybkie i niedrogie rozwiązanie do backupu

#1 Ochrona danych dla SMB, Enterprise oraz MSP

Wydajne tworzenie kopii zapasowych i odzyskiwanie danych - gdziekolwiek się znajdują:

vmware vSphere · Microsoft Hyper-V · NUTANIX · Amazon EC2 · Windows · Linux Server and Desktop

Microsoft 365 · Exchange · Microsoft SQL Server · ORACLE DATABASE · VMware Cloud Director™ · NAS

Oszczędzaj czas na rutynowych zadaniach

- ✓ Jedna konsola dla wszystkich Twoich backupów
- ✓ Szybki backup i replikacja
- ✓ Mnóstwo opcji automatyzacji

Niezawodny czas pracy bez przestojów, krótkie RTO

- ✓ Natychmiastowe pełne lub granularne odzyskiwanie
- ✓ Elastyczność wielu platform
- ✓ Niezawodna weryfikacja

Zacznij w parę minut

- ✓ Możliwość wdrożenia na dowolnym środowisku
- ✓ Bezagentowe rozwiązania dla Twoich VM
- ✓ Uruchom konsolę na swoim NAS!

POZNAJ AKADEMIĘ NAKIVO

Autorskie nagrania w języku polskim!

tinyurl.com/AkademiaNakivo

Konsorcjum FEN Sp. z o.o.
ul. Czarnkowska 13
60-415 Poznań

Dział handlowy Nakivo: nakivo@fen.pl
Polska strona Nakivo: https://nakivo.fen.pl
Wsparcie techniczne: helpdesk@fen.pl

510 044 710