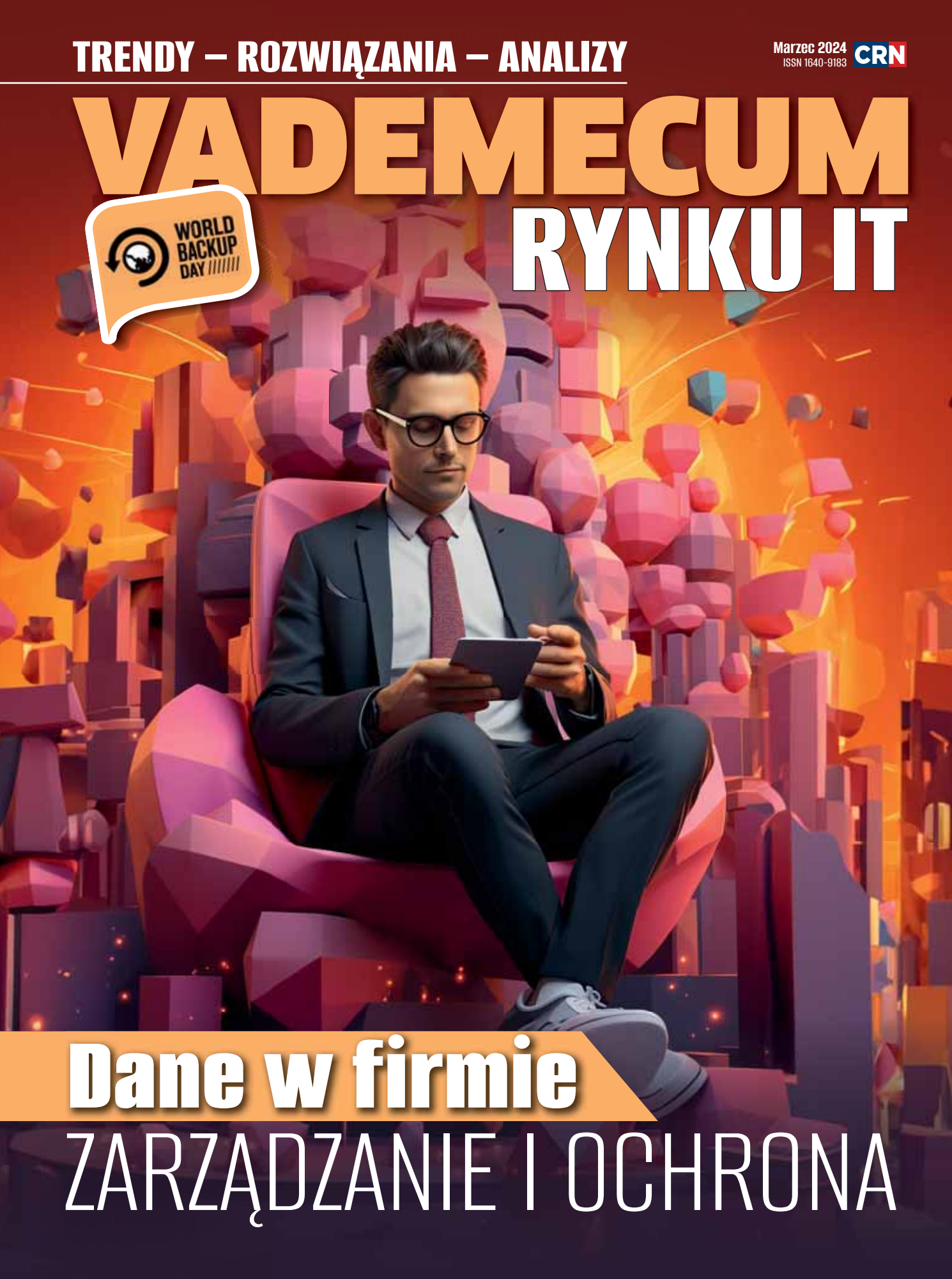
TRENDY – ROZWIĄZANIA – ANALIZY

Marzec 2024
ISSN 1640-9183
CRN

VADEMECUM RYNKU IT

WORLD BACKUP DAY



Dane w firmie

ZARZĄDZANIE I OCHRONA

CRN.pl liderem

w segmencie biznesowych portali IT

Średnia miesięczna liczba odsłon stron www
w okresie listopad 2023–styczeń 2024, źródło: SimilarWeb

Dziękujemy za Wasze zaufanie!

VADEMECUM RYNKU IT

1/2024

16 NIE MA UCIECZKI OD HYBRYDY

Dostawcy rozwiązań do backupu coraz bardziej starają się wykorzystywać w nich sztuczną inteligencję.

NOWYM MOTYWATOREM PRAWO I SZTUCZNA INTELIGENCJA

Firmy przekonują się do korzyści wynikających z elektronicznego obiegu dokumentów. Dla nieprzekonanych skutecznym impulsem mogą być regulacje prawne.

26

32

ZERO TRUST STYMULATOREM RYNKU

Brak zaufania wobec użytkowników infrastruktury IT staje się kluczową i docelową strategią zapewniającą ochronę przed wyciekami danych.

Fot. Adrian Stykowski

Krzysztof Jakubik
redaktor prowadzący

AI musi być pod kontrolą

Wyobraź sobie, że jesteś pracownikiem międzynarodowego przedsiębiorstwa. Współpracujesz bezpośrednio z zarządem i jesteś odpowiedzialny za wykonywanie przelewów na duże kwoty za strategiczne usługi i dostawy towarów. Wszyscy w Twojej firmie są świadomi istnienia zjawiska spear phishingu, dlatego dane do przelewów otrzymujesz nie w mejlu, ale podczas wideokonferencji z zarządem. Nie inaczej było wczoraj – dyrektor finansowy oraz kilka innych bardzo ważnych osób poprosiło o wykonanie przelewów na ponad 25 mln dol. Jednak dziś wydarzyło się coś dziwnego. Podczas rozmowy twarzą w twarz stanowczo zaprzeczyli takim zleceniom. Brzmi to jak scenariusz średniej klasy filmu sensacyjnego? A może to dział marketingu producenta narzędzi ochronnych zbyt popuścił wodze fantazji w celu promocji swojego „najlepszego na świecie i zabezpieczającego przed wszystkim" rozwiązania?

Nic z tych rzeczy – taka sytuacja wydarzyła się w lutym w Hong Kongu. Cyberprzestępcy od dłuższego czasu mieli dostęp do komputerów kilku pracowników jednej z firm. Zauważyli, w jaki sposób dokonywane są zlecenia przelewów i nagrali kilka takich spotkań. Te nagrania zaś posłużyły do wytrenowania mechanizmów sztucznej inteligencji, która bezbłędnie zasymulowała zarówno głos, jak i mimikę rozmówców, odtwarzając podstawiony przez oszustów tekst. Później wystarczyło tylko umówić kolejne spotkanie i poprosić o wykonanie pilnych przelewów na 200 mln dolarów hongkońskich. „Zleceniodawcy" do dziś nie wykryto.

Ale spear phishing to także potężne narzędzie ataku. Do tej pory wykorzystywane dość nieudolnie (tego typu próby były podejmowane także wobec naszej redakcji – obserwowaliśmy je z rozbawieniem), ale eksperci ostrzegają, że może to się zmienić. Wystarczy, że cyberprzestępca uzyska dostęp do skrzynek poczty elektronicznej przedsiębiorstwa, dzięki czemu będzie w stanie wyszkolić model językowy sztucznej inteligencji. Tak, aby perfekcyjnie imitował nie tylko treści, ale też styl prowadzonej w firmie korespondencji – i to w dowolnym języku. Wygląda na to, że nie bez powodu Światowe Forum Ekonomiczne w ostatnim czasie wskazało na generowane w ten sposób fałszywe informacje jako największe ryzyko dla globalnej gospodarki.

Zresztą do strat nie zawsze muszą doprowadzić cyberprzestępcy. W lutym świat obiegła informacja o samobójczym golu, który strzeliła sobie linia lotnicza Air Canada. Należący do niej chatbot, bazujący na AI, zaproponował klientowi obniżkę według procedury, która... nie istniała. Co więcej, pracownicy przewoźnika, zamiast zagryźć zęby i zrealizować obietnicę niepokornego „pracownika", odmówili klientowi, a ten poszedł do sądu i naturalnie wygrał. Oczywiście można założyć, że takie sytuacje będą się zdarzały (oszczędności z braku konieczności zatrudniania prawdziwych osób na stanowiskach konsultantów wciąż mogą być większe), a modele językowe będą coraz doskonalsze i lepiej wyszkolone. To jednak też ważny sygnał, że AI musi się znajdować pod nieustanną kontrolą.

Według analityków Forrester Research dwie trzecie konsumentów jest gotowych zapłacić więcej za produkt czy usługę, jeśli ich dostawca zapewni doskonałą obsługę klienta. W obecnej sytuacji raczej wyklucza to sztuczną inteligencję jako samodzielną jednostkę odpowiedzialną za prowadzenie tej obsługi – na jakimkolwiek etapie. Proponując rozwiązania AI swoim klientom (albo planując ich wdrożenie dla samych siebie) warto rozważyć skorzystanie z ich możliwości jako narzędzia dostarczającego dodatkowe informacje, np. analizującego postawę i oczekiwania klienta na przestrzeni ostatnich lat oraz dostarczającego najlepszych rekomendacji. Niech naturalna inteligencja jeszcze długo będzie niezastąpiona, choć od tej sztucznej nie ma ucieczki – czego najlepszym dowodem jest fakt, że w obecnym wydaniu „Vademecum rynku IT" wspomina się o niej w 80 proc. artykułów redakcyjnych i komercyjnych.

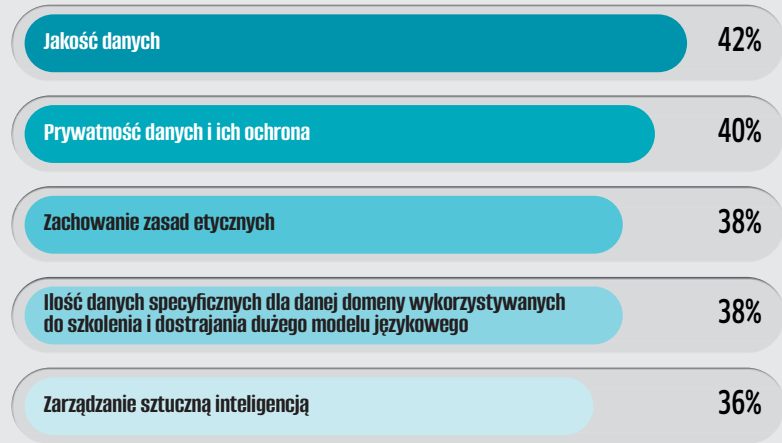
Fałszywe informacje największym ryzykiem dla globalnej gospodarki?

Za dużo danych i narzędzi

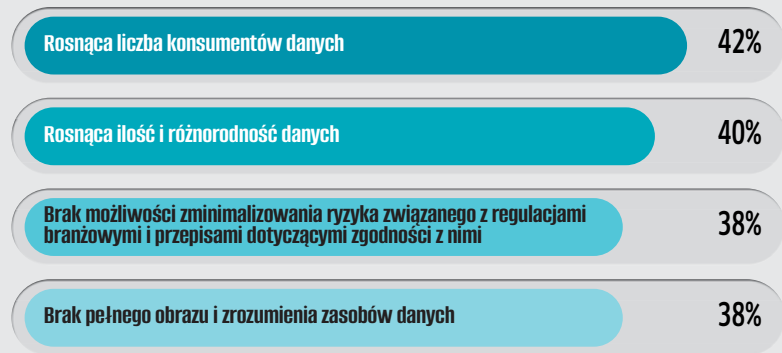
Na zlecenie firmy Informatica agencja badawcza Wakefield Research przeprowadziła ankietę dotyczącą wyzwań związanych z rozwiązaniami sztucznej inteligencji. W badaniu udział wzięło 600 administratorów danych (na stanowiskach Chief Data Officer, Chief Analytics Officer i Chief Data Analytics Officer) z firm z USA, Europy i Azji. Analiza zgromadzonych danych wskazuje jednoznacznie, że cyfrowa transformacja strategii przedsiębiorstw możliwa będzie wyłącznie dzięki równoległemu wdrażaniu rozwiązań sztucznej inteligencji, jak też zaawansowanych procedur zarządzania danymi.

Jednak nie będzie to proste. Aż 58 proc. ankietowanych już teraz zarządza ponad pięcioma narzędziami tylko po to, aby poradzić sobie z danymi pochodzącymi z ponad tysiąca źródeł. 41 proc. deklaruje, że potrzebuje jednego skonsolidowanego rozwiązania do zarządzania wszystkimi tymi danymi. Połowa zaś chce wyposażyć personel firm w narzędzia bazujące na sztucznej inteligencji, aby zoptymalizować wykonywanie ich służbowych zadań, jak też pomóc im w ewentualnym przekwalifikowywaniu się.

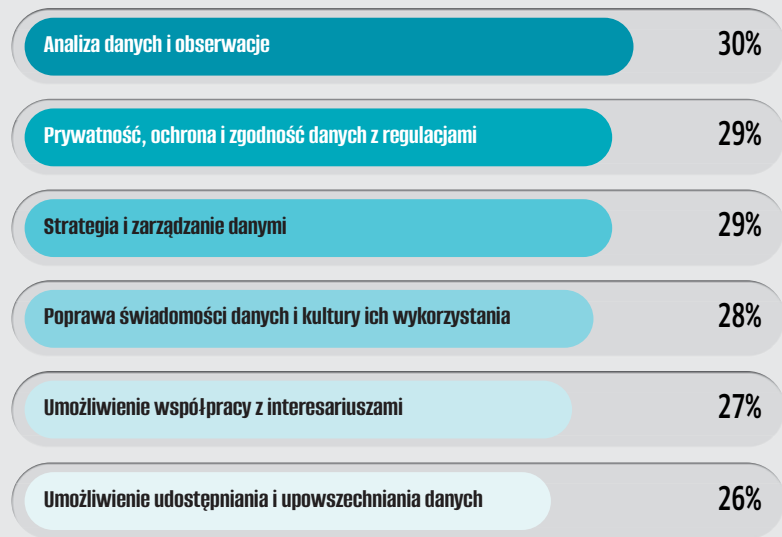
Największe wyzwania związane z generatywną sztuczną inteligencją



Przeszkody związane z danymi i technologią w realizacji strategii danych



Najważniejsze obowiązki administratorów danych



Źródło: „CDO Insights 2024: Charting a Course to AI Readiness", Informatica, 2024

Walczymy o większą elastyczność środowisk pamięci masowych

„Za pomocą koncepcji *computational storage* chcemy spowodować, aby powstawały systemy umożliwiające przetwarzanie danych tam, gdzie w danej sytuacji jest to najbardziej optymalne z punktu widzenia całego środowiska IT" – mówi dr J Michel Metz, przewodniczący Rady Dyrektorów SNIA oraz inauguracyjny przewodniczący Ultra Ethernet Consortium.

Organizacji SNIA należą się gratulacje ze względu na fakt, że od ponad 20 lat skupia walczących ze sobą na co dzień na śmierć i życie konkurentów z rynku pamięci masowych, aby wspólnie wypracowywali nowe standardy dla tej branży. Co jest największym czynnikiem tego sukcesu?

Rzeczywiście, to już ponad ćwierć wieku, a w tym czasie mieliśmy do czynienia z wieloma przełomami oraz zmieniającymi się trendami w branży pamięci masowych. Były one na tyle znaczące, że firmy doszły do wniosku, iż tylko współpraca, a nie zamykanie się na innych, zapewni możliwość skutecznego kontynuowania prac rozwojowych. Na początku XXI wieku obserwowaliśmy olbrzymi wzrost popularności protokołu Fibre Channel i generalnie łączności pamięci masowych w sieci, aby zapewnić szybko rosnącym wówczas firmom możliwość skalowania ich środowisk. Później zaczęły się bardzo szybkie zmiany w wydajności i interfejsach wykorzystywanych nośników – najpierw SATA, potem przekształcenia interfejsu SCSI, następnie błyskawiczny wzrost popularności pamięci flash i wreszcie pojawienie się protokołu NVMe. Mówimy tu o przechowywaniu na wielką skalę najważniejszych obecnie zasobów, jakie istnieją na świecie, a więc cyfrowych danych. Sukces polegający na udanym stworzeniu tak olbrzymiego ekosystemu nie byłby możliwy, gdyby firmy nie współpracowały ze sobą. Równolegle trzeba było zapewnić odpowiednie interfejsy API, narzędzia do produkcji danych rozwiązań, weryfikacji poprawności ich pracy i zarządzania nimi, działania edukacyjne itd. Z wieloma wyzwaniami nadal mamy do czynienia.

Jakie obecnie są najważniejsze?

Przez lata dane były zapisywane na nośnikach magnetycznych, a nawet jeśli trafiały do pamięci flash, to nadal dostęp do nich następował poprzez interfejs twardych dysków. Wszystko zmienił standard NVMe. Zgodne z nim nośniki z technicznego punktu widzenia – biorąc pod uwagę metodę zapisu, wydajność, interfejs – nie są dyskami, lecz pamięciami, tylko nieulotnymi w momencie odłączenia zasilania, więc trudno zaliczyć je do kategorii określanej jako *storage*. To wymusiło zmianę podejścia w naszej filozofii, ale także bardziej zakrojoną współpracę z innymi, jak DMTF czy nową organizacją Ultra Ethernet Consortium, która skupia się na zapewnianiu łączności sieciowej dla środowisk sztucznej inteligencji i wysokowydajnego przetwarzania, czyli HPC. Kiedyś w większych firmach mieliśmy do czynienia z sytuacją, że była w nich jedna duża macierz dyskowa lub kilka połączonych ze sobą w sieć Storage Area Network i to z nimi łączyły się serwery. Dziś możliwych scenariuszy jest o wiele więcej. Dla przykładu, ze względu na potrzebę eliminowania opóźnień w przesyłaniu danych serwery często dysponują własnymi pojemnymi zasobami dyskowymi, przy czym powinna być zapewniona możliwość centralnego zarządzania nimi oraz procesami ochrony zgromadzonych danych. Musimy więc na kwestię przetwarzania informacji w środowisku IT patrzeć całościowo, a nie wybiórczo, jak do tej pory.

Czy oznacza to, że możemy oczekiwać zmiany nazwy organizacji SNIA na bardziej dostosowaną do nowych okoliczności?

Ależ to się parę lat temu już wydarzyło! Wcześniej był to skrót od Storage

Fot. archiwum

Networking Industry Association, co oznaczało, że skupialiśmy się głównie na aspektach dotyczących łączenia systemów pamięci masowych w sieć. Ze wspomnianych już powodów ta nazwa przestała być adekwatna, ale że postrzeganie SNIA w branży IT było dość pozytywne, dlatego jako naszą nową nazwę przyjęliśmy właśnie „SNIA" – bez rozwinięcia skrótu.

■ Czym zatem będzie zajmować się SNIA w najbliższej przyszłości?

Musieliśmy pogodzić się z faktem, że wielu pracowników związanych z IT, których praca jest uzależniona od danych, ma o pamięciach masowych niewielkie pojęcie. Nawet ci związani z infrastrukturą techniczną, na przykład odpowiedzialni za środowiska wirtualizacji czy kontenerów, często nie są świadomi jak sposób ich przechowywania wpływa na wydajność lub jakie są możliwości ich przenoszenia pomiędzy różnymi środowiskami, a także do chmury. Po prostu tego nie wiedzą, to jest dla nich jak magia – oni nie używają takiej terminologii jak my, którzy znamy się na pamięciach masowych, musimy więc zmienić sposób, w jaki komunikujemy się z tymi ludźmi. To zaś oznacza konieczność intensyfikacji działań edukacyjnych, które zresztą i tak prowadzimy od początku istnienia SNIA, oraz skierowania ich do znacznie szerszej grupy odbiorców. Bardzo ważne dla nas jest, aby nawiązywać pozytywne relacje, bo ludzie, którzy potrzebują szybkiego i gwarantowanego dostępu do danych często nie wiedzą jak rozwiązać swój problem, my zaś tak. Muszą natomiast wiedzieć, że my jesteśmy gotowi do pracy i chcieć się komunikować z nami.

■ Jednym z takich wyzwań przyszłości z pewnością jest wspomniana już sztuczna inteligencja. Czy jej popularyzacja w jakimś znaczącym stopniu może wpłynąć na rynek pamięci masowych?

Wobec rozwiązań obsługujących mechanizmy sztucznej inteligencji wysuwane są bardzo znaczące wymagania architektoniczne, przede wszystkim pod kątem przepustowości i skalowalności. Zarządzają one ogromnym kopcem danych, które muszą zostać pozyskane, zamodelowane, usystematyzowane i wreszcie zrozumiane. A efekt tej pracy musi być dostępny natychmiast na żądanie każdego uprawnionego użytkownika. Tu nie ma miejsca nawet na jeden błąd w planowaniu potrzebnej infrastruktury pamięci masowych, zarówno pod kątem pojemności, wydajności, jak też łączności z serwerami odpowiedzialnymi za proces głębokiego uczenia oraz udostępniania jego wyników. Co więcej, od początku trzeba też zakładać, że takie środowisko będzie się często zmieniać – zazwyczaj szybko rosnąć. Na każdym etapie jego tworzenia i eksploatacji konieczna jest więc świadomość tego, w jaki sposób będzie można je rozbudowywać i zwiększać jego wydajność. To wszystko powoduje, że do środowisk AI potrzebne będą najwyższej jakości pamięci masowe – zarówno pod kątem wydajności, jak też trwałości oraz dostępności.

> Nie możemy w żaden sposób wpływać na kształt rynków czy ceny rozwiązań.

■ W takim środowisku bardzo ważne jest minimalizowanie opóźnień, czy więc nie będzie bardziej korzystne instalowanie nośników bezpośrednio w serwerach? Czy w tym kontekście w ogóle będą przydatne tradycyjne macierze dyskowe?

Środowiska sztucznej inteligencji uczenia maszynowego składają się z niezwykle dużych zbiorów danych. Nierzadko wykorzystywane są w nich petabajty danych, a słyszałem też już o repozytoriach w skali eksabajtów. Z oczywistych względów serwery nie są w stanie pomieścić takiej ilości danych wewnętrznie, a dostęp do nich musi być zapewniony za pomocą innych środków, w tym macierzy dyskowych. W przypadku serwerów najważniejszą kwestią jest dostarczanie do nich danych, aby mogły być przetworzone za pomocą ich mocy obliczeniowej. Tu wyzwaniem jest

skalowalność, a problem z wydajnością pamięci masowych robi się dopiero później, gdy trzeba udostępnić te dane użytkownikom w czasie jak najbardziej zbliżonym do rzeczywistego.

Jak skutecznie można dziś mierzyć tę wydajność? Przez wiele lat funkcjonowała organizacja Storage Performance Council, która stworzyła serię testów wydajnościowych SPC, zaakceptowanych prawie przez całą branżę. Ale obecnie wydaje się, że projekt umarł śmiercią naturalną...

Niestety, ze względu na wzrost funkcjonalności systemów pamięci masowych ich wydajność stała się uzależniona od ogromnej liczby czynników. W większości porównywalnych ze sobą macierzy zainstalowane są podobne nośniki, więc to nie od nich ta wydajność zależy, ale głównie od sprzętowej konstrukcji kontrolerów macierzowych oraz ich oprogramowania. Dla przykładu, nośniki nadal są drogie, więc popularne jest korzystanie z technik zmniejszających ilość przechowywanych danych, jak kompresja czy deduplikacja. Nie dość, że stosowanie ich do przeliczania danych w czasie rzeczywistym negatywnie wpływa na wydajność, to ten wpływ w praktyce jest niemożliwy do określenia, gdyż zależy od rodzaju aktualnie przetwarzanych danych. Co więcej, wydajność takiej macierzy może się zmienić w wyniku instalacji nowszej wersji zarządzającego nią oprogramowania, która na przykład będzie miała zaimplementowane bardziej rygorystyczne mechanizmy ochronne likwidujące jakąś podatność na zagrożenie, ale wpływające na szybkość pracy. Kolejny czynnik to wiele dostępnych opcji, w tym możliwość instalacji kart z procesorami GPU przyspieszającymi proces przetwarzania danych. Jednak nade wszystko ważna jest kwestia szybkości dostępu do danych. Gdy w macierzach dominowały mechaniczne twarde dyski, średni czas dostępu liczony był w milisekundach i różnica rzędu 20–30 procent pomiędzy konkurencyjnymi rozwiązaniami była znacząca. Pamięci flash sprowadziły ten parametr na poziom mikrosekund, a dzięki protokołowi NVMe zaczynamy mówić o nanosekundach. Oczywiście zapotrzebowanie na skrócenie czasu dostępu też wzrosło, ale różnice pomiędzy macierzami – przy założeniu, że wyłączone są funkcje spowalniające – zrobiły się niewielkie. Natomiast te funkcje zazwyczaj są włączone, co powoduje, że przy tak ogromnej liczbie możliwych kombinacji porównywanie staje się bezcelowe.

Do środowisk AI potrzebne będą najwyższej jakości pamięci masowe.

Czy technologia kwantowego przetwarzania i przechowywania danych spowoduje, że wszystkie te rozważania staną się przeszłością, bo wejdziemy na zupełnie inny poziom wydajności? Czy zajmujecie się już tymi zagadnieniami?

Abyśmy mogli ustanowić techniczną grupę roboczą muszą zgłosić się do nas trzy firmy działające w danym obszarze. Ostatnio założyliśmy taką grupę roboczą dotyczą przechowywania danych w molekułach DNA. W przypadku technologii kwantowej na razie jest ona rozwijana w instytucjach badawczych, więc za wcześnie jest, aby mówić o branżowej standaryzacji. Natomiast jeśli komercyjne przedsiębiorstwa uznają, że już jest czas, aby przekształcić to w produkt lub rozwiązanie dla swoich klientów, my jesteśmy otwarci na współpracę w celu stworzenia odpowiednich standardów.

Coraz więcej dostawców pamięci masowych rozszerza swoje rozwiązania o nowe funkcje związane z ochroną danych, chociażby zabezpieczające przed skutkami ataku ransomware lub umożliwiające integrację z mechanizmami antywirusowymi. Czy SNIA angażuje się także w tym obszarze, aby zapewnić interoperacyjność pomiędzy różnymi rozwiązaniami?

Mamy techniczną grupę roboczą ds. bezpieczeństwa, która zajmuje się takimi kwestiami. Analizujemy regulacje prawne wypracowane przez rządy poszczególnych państw lub regionów, jak Unia Europejska. Wyszukujemy najlepsze praktyki dotyczące bezpieczeństwa i pomagamy implementować je w specyfikacjach technicznych. Natomiast nie tworzymy mechanizmów prowadzenia testów interoperacyjności. W tej dziedzinie musimy być bardzo ostrożni, ponieważ mamy ograniczenia regulacyjne i antymonopolowe – nie możemy w żaden sposób wpływać na kształt rynków czy ceny rozwiązań. Prowadząc nasze działania edukacyjne musimy też być neutralni jak tylko to możliwe. Nie możemy też promować danej technologii poprzez tworzenie jej negatywnych porównań z innymi.

Jedną z najnowszych technologii promowanych przez SNIA, wobec której wciąż jest wiele nieporozumień, są pamięci masowe umożliwiające przetwarzanie danych, a więc *computational storage*. Jaki jest obecny status tego projektu?

To jest nasze oczko w głowie, ale rzeczywiście, wciąż wiele działań edukacyjnych przed nami. Zazwyczaj ludziom wydaje się, że głównym celem tego projektu jest wyposażenie nośników w jakiś rodzaj procesora przyspieszającego przetwarzanie zgromadzonych na nich danych. Oczywiście jest to możliwe i pojawiały się już takie nośniki z układem odpowiedzialnym za kompresję gromadzonych danych, aby odciążyć kontroler macierzowy. Jednak liczba możliwych zastosowań takiego podejścia jest bardzo ograniczona. Naszym celem jest doprowadzenie do takiej sytuacji, aby możliwe było tworzenie środowisk z zapewnioną elastycznością co do wyboru miejsca przetwarzania danych. Do tej pory dzieje się to w serwerach, do których dane dostarczane są trochę wolniej z zewnętrznych, łatwo skalowalnych macierzy dyskowych lub szybciej z wbudowanych nośników, których jest jednak ograniczona liczba. A co w sytuacji odwrotnej, gdy istnieje chwilowa potrzeba przetworzenia danych rozrzuconych na bardzo dużej liczbie nośników? Wówczas to

Fot. archiwum

macierz dyskowa powinna móc przeprowadzić taką operację, aby nie obciążać sieci przesyłanymi danymi. Docelowo chcemy spowodować, aby powstawały systemy umożliwiające przetwarzanie danych tam, gdzie w danej sytuacji jest to najbardziej optymalne z punktu widzenia całego środowiska IT. Opublikowaliśmy już główne założenia tej koncepcji.

Brzmi to jak niemała rewolucja w branży...

Muszę przyznać, że w tej dziedzinie zostaliśmy nieco ukarani przez sukces naszego własnego marketingu. Opowiadamy o zarysach tej koncepcji już od paru lat i wiele osób z niecierpliwością oczekuje na konkretne rozwiązania. Jednak pojawianie się ich będzie rozciągnięte w czasie, to będzie raczej szybko postępująca ewolucja. Ale cieszy nas, że firmy wykazują zapotrzebowanie na przyspieszenie działań obliczeniowych, bo to zagwarantuje rynkowy sukces tej koncepcji. Na razie łączymy wiele kropek, aby powstał finalny obrazek. Aktywnie współpracujemy z NVM Express, DMTF oraz wieloma różnymi przedsiębiorstwami, aby lepiej zrozumieć oczekiwania i zdefiniować jak w rzeczywistości będziemy w stanie je zaspokoić przy różnych rodzajach zadań obliczeniowych, ze szczególnym naciskiem na sztuczną inteligencję i HPC.

Dzięki *computational storage* możliwe będzie stworzenie szybszych kontrolerów RAID dla pamięci NVMe.

Kiedy i jakiego typu produkty pojawią się zatem jako pierwsze?

Pierwsze produkty już są dostępne, ale one wykonują predefiniowane, wpisane na stałe funkcje, jak szyfrowanie czy wspomniana kompresja. Dzięki koncepcji *computational storage* dość szybko możliwe będzie stworzenie też wydajnych kontrolerów RAID dla pamięci NVMe. Zastosowanie w nich dotychczasowego podejścia nie najlepiej się sprawdza, ponieważ wprowadzenie warstwy wirtualizacyjnej charakterystycznej dla RAID powoduje dezaktywację wielu funkcji zapewnianych przez protokół NVMe. Wskazane zatem jest wyposażenie kontrolerów RAID w dodatkowy szybki układ, który będzie wykonywał stosowne obliczenia związane nie tylko z dystrybucją paczek danych na poszczególne nośniki, ale też ich dostarczaniem do magistrali komputera. Jednakże docelowo w koncepcji *computational storage* chodzi o to, aby zapewnić większą elastyczność wyboru miejsca, gdzie przetwarzane są dane. Bardzo wyczekiwaną przez klientów funkcją jest wyposażenie kontrolerów macierzowych w możliwość dokonywania wstępnej analizy danych na potrzeby mechanizmów uczenia maszynowego. To też w dużym stopniu odciążyłoby sieć, ponieważ do przetworzenia przez serwery trafiałyby tylko wartościowe informacje. Oszczędności czasu i energii, które w dużej skali można dzięki temu uzyskać, są nie do przecenienia.

Czy tego typu podejście będzie wymagało też specjalnych aplikacji? Czy będzie konieczne przepisanie części oprogramowania, tak jak wymusiły to środowiska wirtualizacyjne i chmura obliczeniowa?

Na pewno nie można dopuścić do tego, aby klienci, którzy kupią rozwiązania z funkcją *computational storage*, byli zmuszani do przepisywania swojego oprogramowania. Dlatego korzystanie z niej powinno być opcjonalne. W niektórych przypadkach, gdy to układ w nośniku odpowiedzialny jest za wybrane operacje obliczeniowe, jak wspomniane szyfrowanie czy kompresję, aplikacja nie musi być świadoma istnienia tego procesu. Z tym, że docelowo należy zakładać, iż optymalne wykorzystanie dodatkowych możliwości zapewnianych przez *computational storage* będzie wymagało „świadomości" ich dostępności ze strony oprogramowania. My jednak w tym względzie pozostaniemy neutralni jak tylko to będzie możliwe – nie będziemy ani do tego zachęcali, ani też tego wymagali.

Rozmawiał
Krzysztof Jakubik

Dr J Michel Metz

już czwartą kadencję pełni funkcję przewodniczącego Rady Dyrektorów SNIA. Ponadto został przewodniczącym powstałego rok temu Ultra Ethernet Consortium, jak też jest dyrektorem technicznym ds. projektowania systemów w AMD. Wcześniej zajmował szereg stanowisk technicznych i menedżerskich (Field CTO, inżynier ds. badań i rozwoju, architekt rozwiązań i inżynier systemów) zarówno w startupach, jak i w firmach z listy Fortune 100. W przeszłości był członkiem zarządu Fibre Channel Industry Association (FCIA) oraz Non-Volatile Memory Express (NVMe). Uzyskał tytuł doktora na University of Georgia.

Coraz mniej kompromisów

Dostawcy pamięci masowych dla klientów korporacyjnych uporali się z wieloma wyzwaniami, które pojawiły się na ich drodze. To jednak nie koniec „podróży".

Wojciech Urbanek

Zmiany zachodzące w segmencie pamięci masowych mają dynamiczny charakter. „Po 2028 roku nikt już nie będzie sprzedawał dysków twardych", „petabajt stał się nowym terabajtem", „koniec kompromisów pomiędzy pojemnością a wydajnością" – to tylko niektóre stwierdzenia wygłoszone w ubiegłym roku przez branżowych specjalistów. Choć są nieco przerysowane, bardzo dobrze oddają tendencje występujące na tym rynku.

Od co najmniej kilku lat w branży pamięci masowych jesteśmy świadkami stopniowego odchodzenia od tradycyjnych dysków mechanicznych na rzecz SSD. Niewykluczone, że rok 2024 może być pod tym względem przełomowy, gdyż zapewne w najbliższych miesiącach pojemność wdrożonych pamięci flash po raz pierwszy przewyższy liczbę zainstalowanych dysków twardych. Co istotne, na początku ubiegłego roku sprzedaż macierzy all-flash na globalnym rynku przekroczyła barierę 50 proc. w ujęciu wartościowym (według Gartnera).

Korzystnie dla systemów all-flash wyglądają również statystyki dotyczące sprzedanej pojemności. Pod tym względem ich udział w całym rynku macierzy przekroczył 30 proc., choć zaledwie dwa lata wcześniej wskaźnik ten nie sięgał 20 proc. Jak widać, mamy do czynienia z poważnym progresem, tym bardziej, że jeszcze kilka lat temu na zakup systemu all-flash mogły sobie pozwolić jedynie bogate korporacje. Zasadne zatem wydaje się pytanie: skąd ten nagły skok?

Tańsze, ale mniej wytrzymałe

Decydujący wpływ na wzrost liczby dysków półprzewodnikowych w serwerowniach mają rozwój techniczny i spadek cen. Producenci macierzy all-flash zrezygnowali z droższych, choć cechujących się stosunkowo długą żywotnością pamięci SLC (komórki jednowarstwowe) oraz MLC (dwuwarstwowe) na rzecz tańszych i mniej wytrzymałych pamięci TLC (trzywarstwowych). W tzw. międzyczasie na horyzoncie pojawiła się najnowsza generacja dysków półprzewodnikowych z pamięcią QLC (czterowarstwową). Jak łatwo się domyślić, pozwala ona przechowywać więcej danych w tej samej przestrzeni niż TLC, ale jeszcze większym kosztem wydajności i trwałości.

Obecnie producenci macierzy dyskowych najczęściej wykorzystują nośniki TLC, zaś w znacznie mniejszym stopniu MLC. Wszystko wskazuje na to, że nie pogardzą nośnikami QLC ze względu na ich atrakcyjną cenę. Gartner prognozuje, iż do 2027 r. nośniki QLC będą stanowić 25 proc. spośród wszystkich dysków SSD używanych przez użytkowników korporacyjnych.

Innym ważnym trendem jest popularyzacja pamięci flash z interfejsem NVMe, które biją pod względem wydajności dyski półprzewodnikowe SAS lub SATA. Liczba operacji wejścia/wyjścia na sekundę (IOPS) w macierzach korzystających z NVMe praktycznie zawsze przekracza milion. Popularyzacja wykorzystania tych nośników w macierzach dyskowych może w dłuższej perspektywie zagrozić nawet rozwiązaniom SAN.

– *Odnotowujemy rosnące zainteresowanie ze strony klientów protokołem NVMe over TCP, który umożliwia wykorzystanie tradycyjnych sieci IP do wydajnego transportu danych. Technologia*

Nowym polem rywalizacji w segmencie pamięci masowych stała się cyberochrona.

Fot. Adobe Stock

ta może mieć spore znaczenie zwłaszcza w nowo powstających środowiskach, w przypadku których klienci nie chcą inwestować od początku w sieci SAN z protokołem Fibre Channel – tłumaczy Paweł Albert, Advisory Systems Engineer w Dell Technologies.

Pomimo tego, że liczba nośników SSD w centrach danych rośnie w szybkim tempie, to w najbliższych latach nie wyprą całkowicie „twardzieli". Dyski mechaniczne nadal znajdują szerokie zastosowanie w repozytoriach danych czy do celów backupu. Nie bez znaczenia jest przy tym fakt, że ich producenci cały czas rje rozwijają. Przykładowo, w ostatnich miesiącach zadebiutowały monstrualne napędy od WD oraz Seagate'a, o pojemności odpowiednio 26 TB i 30 TB. Jak łatwo się domyślić, oba modele są zaprojektowane z myślą o potrzebach hiperskalerów.

Niemniej wielu specjalistów uważa, że odpowiednio skonfigurowana macierz hybrydowa (w przypadku której buforowanie bazuje na pamięci flash) w zupełności wystarczy do pracy w tradycyjnych środowiskach. Po co więc przepłacać i „mielić powietrze"?

Inwazja obiektów

Jeszcze do niedawna w segmencie pamięci masowych obowiązywały dość proste i klarowne zasady. Firmy inwestowały w osobne rozwiązania do archiwizacji danych oraz ich przetwarzania w środowiskach produkcyjnych. Przez lata funkcjonował podział na pliki oraz bloki. Pojawienie się pamięci obiektowej zmąciło ten porządek. Dzięki wysokiej skalowalności możliwe stało się stosunkowo tanie przechowywanie dużych zbiorów nieustrukturyzowanych danych w rozproszonych środowiskach. W efekcie macierze obiektowe zaczęły służyć najczęściej do magazynowania tzw. zimnych danych.

Postęp techniczny, a zwłaszcza znaczna poprawa wydajności macierzy, sprawił, że znaleziono dla nich dodatkowe zastosowania, w tym obsługę aplikacji Big Data, pracę z modelami sztucznej inteligencji czy dostarczanie takich aplikacji online, które wymagają dużych przepustowości. Dlatego z tego typu rozwiązań korzystają zazwyczaj firmy telekomunikacyjne, dostawcy usług chmurowych czy też podmioty z branży mediów i rozrywki. Należy się liczyć z tym, że wraz z upowszechnianiem się pamięci obiektowej w korporacyjnych archiwach, będzie ona również wykorzystywana do obsługi bardziej wymagających aplikacji.

W systemach pamięci obiektowej dyski półprzewodnikowe, w tym nawet NVMe, są coraz częściej zastępowane przez niedrogie dyski mechaniczne. Ich dostawcy cały czas pracują nad poprawą wydajności swoich rozwiązań. Prym wiodą w tym przypadku tacy gracze jak MinIO, Scality czy Quantum. System pierwszej z wymienionych firm osiągnął maksymalną prędkość odczytu 325 Gb/s, a zapisu 117 Gb/s (testy przeprowadzono na klastrze składającym się z 32 węzłów). Z kolei specjaliści Scality chwalą się wdrożeniem u jednego z dostawcy usług chmurowych, u którego udało się osiągnąć 1,6 mln IOPS.

Jeszcze więcej bezpieczeństwa

Działania producentów pamięci masowych, dotyczące śrubowania wydajności bądź skalowalności, są czymś naturalnym. Natomiast nowym polem rywalizacji stała się cyberochrona, wykraczająca poza tradycyjne tworzenie kopii zapasowych oraz przywracanie i odzyskiwanie danych po awarii. Narastająca z roku na rok skala cyberataków, w tym szczególnie uciążliwy ransomware, wystawiają dane na duże ryzyko.

Przedsiębiorcy inwestują w oprogramowanie antywirusowe, firewalle, systemy UTM czy EDR, ale też zaczynają pytać o zabezpieczenia występujące w macierzach dyskowych. Producenci, wychodząc naprzeciw tym oczekiwaniom, wprowadzają różnego rodzaju rozwiązania pozwalające chronić kopie zapasowe czy wykrywać podejrzane aktywności.

– *Na szerokie wody wypłynęło kilka koncepcji związanych z ochroną danych i ich odzyskiwaniem po atakach typu ransomware. Jedną z nich jest cyfrowy bunkier, czasami określany jako twierdza czy sejf. Choć dostawcy posługują się różną terminologią, idea jest taka sama. Należy znaleźć jak najbardziej odcięte miejsce od świata, gdzie można przechowywać dane, a w przypadku katastrofy odtworzyć je i przywrócić do działania kluczowe systemy* – tłumaczy Piotr Drąg, Storage Category & Data Services Business Development Manager w HPE.

Oczywiście cyfrowy bunkier to tylko jeden z elementów systemów bezpieczeństwa. Zdaniem ekspertów poleganie na ofercie zewnętrznego dostawcy rozwiązania do skanowania zasobów cyfrowych nie jest najbardziej optymalnym rozwiązaniem. Dlatego też wykrywanie cyberzagrożeń staje się jedną z funkcji dodawanych przez wiodących dostawców do macierzy dyskowych.

Według analityków Gartnera do 2028 r. wszystkie systemy pamięci masowych będą oferować elementy aktywnej ochrony. Obecnie większość producentów aktywnie pracuje nad rozwiązaniami dołączanymi do macierzy bądź włączanymi jako oddzielne produkty.

Zmiany, zmiany, zmiany...

2023 rok nie przyniósł spektakularnych transakcji na rynku pamięci masowych. W tym czasie miało miejsce jedynie 16 fuzji i przejęć, podczas gdy w rekordowym 2006 r. było ich aż 104. Przy czym ubiegłoroczni nabywcy ujawnili cenę zaledwie czterech transakcji, co może oznaczać, że wartość pozostałych była stosunkowo niska. Na osobną uwagę zasługują poczynania firmy Western Digital. Wydawało się, że amerykański koncern połączy siły z Kioxią, czołowym producentem nośników SSD. Tym bardziej, że obie firmy współpracują nad rozwojem standardu BiCS NAND. Ostatecznie do fuzji nie doszło, a Western Digital podzielono na dwie części: jedna z nich zajmie się mechanicznymi twardymi dyskami, zaś druga pamięciami flash. Większość analityków uważa, że taki ruch powinien być korzystny i nie wpłynie negatywnie na współpracę z klientami. Poza tym ma sens na poziomie technicznym, bowiem obie jednostki biznesowe mają ze sobą niewiele wspólnego.

Więcej matematyki, mniej szumu

Wielu przedsiębiorców uodporniło się na slogany marketingowe dostawców usług chmurowych, co pozwala zaistnieć na rynku nowym graczom.

Wojciech Urbanek

Przechowywanie danych w chmurze publicznej najczęściej kojarzy się z Amazon Simple Storage Service (Amazon S3) – obiektową pamięcią masową. To zupełnie zrozumiałe, bowiem to właśnie Amazon jest prekursorem tego rozwiązania, a jednocześnie numerem jeden w tym segmencie rynku. Niemniej lider czuje na plecach oddech Microsoftu (Azure Blob Storage) oraz Google'a (Google Cloud Storage).

O sukcesie pamięci obiektowej w środowisku chmurowym zadecydowało kilka czynników: łatwość przesyłania danych do i z chmury, metadane zapewniające szybki dostęp do wyszukiwanych informacji oraz niemal nieograniczona skalowalność. Amazon i Google wyznaczyli jedynie limity co do obiektów (5 TB), zaś Microsoft ustalił pojemność całego konta do 5 PB.

Pamięć obiektowa nie jest jednak pozbawiona wad, do których należą wolny transfer danych, brak możliwości modyfikacji pojedynczych fragmentów pliku, a czasami również cena. Usługodawcy starają się budować swoją ofertę w taki sposób, aby sprostać zróżnicowanym wymaganiom klientów. Przykładowo, Amazon umożliwia przechowywanie danych aż na siedmiu poziomach wydajności i dostępności – od standardowego, do rzadko używanych archiwów. Jednak to nie wystarcza, aby zaspokoić wymagania firm wykorzystujących dane na setki sposobów.

W związku z tym dostawcy usług nie mogą zawężać oferty wyłącznie do przechowywania obiektów, dywersyfikują ją więc. Zapewniają pamięć blokową z nośnikami flash SSD, przechowywanie dokumentów w formie plików, a nawet specjalne przenośne urządzenia z danymi. Zróżnicowane są też koszty subskrypcji, wahające się od 0,001 dolarów za gigabajt w przypadku zimnych danych do 12 dol. mies. dla wysokowydajnej pamięci masowej SSD używanej do obsługi operacji krytycznych.

Pliki i bloki w chmurze

Pamięć obiektowa miała być alternatywą dla plików, ale okazało się, że te dużo lepiej sprawdzają się w pracy grupowej niż obiekty, ze względu na możliwości w zakresie edycji, modyfikacji czy ustawiania praw dostępu. W zakresie przechowywania plików w chmurze „wielka trójka" ma w miarę zróżnicowaną ofertę. Specyfiką tego segmentu są alianse zawierane między największymi usługodawcami a dostawcami NAS-ów.

Ciekawą grupę tworzą dostawcy oferujący globalne systemy plików: Ctera, Nasuni, Panzura czy Hammerspace. Przy czym większość systemów operacyjnych i aplikacji nie może bezpośrednio odczytywać i zapisywać danych w pamięci obiektowej – konieczny jest dostęp do protokołów sieciowych, takich jak NFS lub SMB, bądź bezpośredni dostęp do pamięci masowej. Wprawdzie dostawcy tworzą różnego rodzaju przejściówki (bramy), jak też pojawiają się aplikacje kompatybilne z pamięcią obiektową, ale to wciąż kropla w morzu potrzeb. Globalny system plików jest – jak na razie – najlepszym sposobem rozwiązania tego problemu, ponieważ łączy takie cechy jak elastyczność i pojemność chmury z prostotą NAS-ów.

– Przykładowo, użytkownik iPhone'a nie musi mieć wiedzy na temat infrastruktury ani tego, gdzie znajdują się dane. Zależy mu tylko na dostępie do informacji w czasie rzeczywistym z dowolnego urządzenia. Globalny system plików zapewnia taką swobodę – tłumaczy Molly Presley, dyrektor marketingu w Hammerspace.

Według IDC w latach 2021–2025 średnia stopa wzrostu ze sprzedaży usług związanych z przechowywaniem plików w chmurze wyniesie 41 proc., aby w 2025 r. osiągnąć wartość 4 mld dol. W przypadku pamięci obiektowej prognozy mówią o 21-proc. wzroście w tym samym czasie, aczkolwiek wielkość obrotów będzie wyraźnie wyższa niż w segmencie przechowywania plików.

Jednym z najtrudniejszym obszarów dla dostawców usług chmurowych jest blokowa pamięć masowa, która obsługuje aplikacje wymagające minimalnych

Fot. Adobe Stock

opóźnień, jak bazy danych i maszyny wirtualne. Największym wyzwaniem w przypadku środowiska chmurowego jest zagwarantowanie użytkownikom odpowiedniej wydajności. Systemy przechowywania bloków nie najlepiej radzą sobie z danymi rozproszonymi w wielu odległych lokalizacjach, co jest atutem pamięci obiektowej.

Potencjalnych nabywców mogą odstraszać także ceny tego rodzaju usług, na co zwraca uwagę Rob Pankow, współzałożyciel startupu Simplyblock. Młoda firma ma na koncie kilka pilotażowych wdrożeń rozwiązania, które ma być alternatywą dla AWS Elastic Block Storage (EBS). Co ciekawe, w niektórych konfiguracjach jest ono 11 razy tańsze od usługi świadczonej przez Amazon. W tym przypadku dużą barierą jest zaufanie, bo któż odważy się powierzyć realizację operacji krytycznych nieznanemu startupowi z Niemiec? Niemniej jest to sygnał dla potencjalnych usługobiorców, że warto przy wyborze dostawcy kierować się matematyką.

Multicloud dla pamięci masowych

Jeszcze kilka lat temu producenci macierzy dyskowych obawiali się ekspansji dostawców usług chmurowych. Masowa migracja klientów do chmury mogłaby ich pozbawić znacznej części przychodów, ale tak się jednak nie stało.

– *Widać, że słabnie owczy pęd do chmury. Firmy zaczynają podchodzić do tematu bardziej racjonalnie. Takim przykładem jest firma HEY, która stworzyła e-mail nowej generacji. Jej założyciel, David Heinemeier, na swoim blogu klarownie tłumaczy dlaczego chmura nie zawsze jest dobrym rozwiązaniem* – zauważa Łukasz Milic, Business Development Representative w QNAP-ie.

Obecnie trudno znaleźć firmy decydujące się na sygnowanie umów z jednym usługodawcą. Większość wybiera niczym rodzynki z ciasta najbardziej optymalne dla siebie oferty, korzystając z usług chmurowych dwóch lub więcej dostawców. Od niedawna podobna tendencja występuje w grupie pamięci masowych. Przedsiębiorstwa współpracują z kilkoma usługodawcami, umieszczając dane w różnych chmurach.

Pamięć masowa w środowisku lokalnym, chmurze hybrydowej i publicznej

Właściwości	Środowisko lokalne	Chmura hybrydowa	Chmura publiczna
Skalowalność	Ograniczona	Bardzo wysoka	Bardzo wysoka
Bezpieczeństwo	Największy poziom	Wysoki poziom, integracja pozwala wzmocnić ochronę o dodatkowe warstwy	Uzależnione od środków wdrożonych przez dostawcę usługi
Wydajność	Wysoka	Dobra, jeśli aktywne dane są w środowisku lokalnym	Od niskiej do średniej
Niezawodność	Wysoka	Od średniej do wysokiej, jeśli aktywne dane są w środowisku lokalnym, ale uzależniona od jakości połączenia internetowego oraz SLA dostawcy usług	Średnia, zależy od jakości połączenia internetowego oraz SLA dostawcy usług

Przykładowo, można przechowywać zasoby archiwalne w Azure Blob Storage, jeszcze inne na Amazon EFS, a najbardziej wrażliwe informacje w chmurze prywatnej. Ta koncepcja pozwala na niezliczoną liczbę kombinacji, a co za tym idzie oszczędności, aczkolwiek dział IT musi sprawnie poruszać się w tym segmencie usług oraz stawiać czoła zagrożeniom związanym ze złożonością, ochroną i spójnością danych. Czasami można wpaść w pułapkę kosztów, zwłaszcza jeśli administratorzy IT nie monitorują zasobów pod kątem skali ich wykorzystania. Przy czym rynek nie znosi próżni – Broadcom, Cloudera, Cloudian, IBM czy NetApp oferują już narzędzia ułatwiające zarządzanie danymi rozproszonymi w chmurach należących do różnych usługodawców.

Przyszłość pod znakiem AI

Wszyscy dostawcy są zgodni, iż istotny wpływ na budowanie ich oferty będzie miał rozwój sztucznej inteligencji. Z jednej strony oznacza to znaczny przyrost danych, zaś z drugiej umożliwia usługodawcom wprowadzanie różnego rodzaju proaktywnych działań zapobiegających awarii sprzętu czy cyberatakom.

> Słabnie owczy pęd do chmury.

– *W 2023 roku dominującym trendem był dynamiczny rozwój rozwiązań chmurowych bazujących na generatywnej sztucznej inteligencji. Można go porównać z pojawieniem się internetu. Rok 2024 pokaże, czy szum związany z GenAI zrewolucjonizuje obecne modele biznesowe i zmieni nasze życie w takim stopniu jak internet czy urządzenia mobilne* – mówi Marcin Dzienniak, CTO w OChK.

Część ekspertów uważa, że niepośledni wpływ na rynek usług chmurowych może mieć zakup Splunka przez Cisco. Choć transakcja bezpośrednio nie jest związana ze środowiskiem chmurowym, może przynieść nowe możliwości w monitorowaniu i zarządzaniu danymi.

Z kolei Adam Kotecki, CEO Cloudica, nie spodziewa się istotnych przetasowań na rynku. Jego zdaniem wielka trójka nadal będzie nadawać ton, przy czym Amazon może tracić klientów na rzecz Microsoftu. Poza tym istnieje miejsce dla usługodawców oferujących innowacyjne rozwiązania – zarówno dla integratorów, jak i klientów końcowych.

Chmura rośnie mimo przeszkód

Potrzeby biznesowe i nowe technologie, w tym GenAI oraz przetwarzanie brzegowe, stają się stymulatorem innowacyjności dla usług chmurowych. Firmy wciąż jednak doświadczają problemów związanych z finansowaniem obsługi środowisk w chmurze.

• *Krzysztof Jakubik*

Według opublikowanej pod koniec ub.r. prognozy Gartnera światowe wydatki na usługi w chmurze publicznej wzrosną w 2024 r. o 20,4 proc. – do poziomu 678,8 mld dol. (563,6 mld dol. w 2023 r.). Przy czym wzrost ma dotyczyć wszystkich segmentów tego rynku, ale w największym stopniu rozwiązań infrastrukturalnych (26,6 proc.) oraz platformowych (21,5 proc.). Analitycy przewidują też, że do 2027 r. ponad 70 proc. przedsiębiorstw będzie korzystać z branżowych platform chmurowych w celu przyspieszenia swoich inicjatyw biznesowych (w 2023 r. było to mniej niż 15 proc.).

Jednym z głównych motorów tego wzrostu mają być w najbliższym czasie usługi generatywnej sztucznej inteligencji (GenAI). Biorąc pod uwagę skalę wymaganej infrastruktury, przedsiębiorcy będą poszukiwać zdolnych do jej „udźwignięcia" usług chmury publicznej, które zapewnią stabilny rozwój w akceptowalnych ekonomicznie warunkach, a także z zachowaniem aspektów dotyczących bezpieczeństwa. Szczególne zainteresowanie widoczne będzie wśród modeli GenAI dla różnych branż – tu pojawia się olbrzymia szansa dla integratorów specjalizujących się w rynkowych niszach, ponieważ dzięki dobrej znajomości aspektów dotyczących danego rodzaju biznesu, a przede wszystkim wiedzy co do potrzeb swoich klientów, będą w stanie ich profesjonalnie wesprzeć.

Edge computing i chmura

W coraz większej liczbie cyfrowych środowisk, szczególnie tych zaliczanych do kategorii Operational Technologies, zbieranych jest coraz więcej danych. Ich przesyłanie do centrum danych w celu zbiorczego przetworzenia stanowi dla firm niemały koszt, dlatego przez ostatnie lata spopularyzowała się koncepcja przetwarzania brzegowego (edge computing). Promuje ona dokonywanie wstępnych operacji na danych jak najbliżej miejsca, gdzie zostały pozyskane, aby do głównego repozytorium trafiły wyniki tych obliczeń albo wyselekcjonowane dane przeznaczone do dalszej obróbki.

Środowiska tego typu stają się już popularne w krajach wysokorozwiniętych, szczególnie o dużej powierzchni i rozproszonej strukturze (np. posiadających wiele wysp). Korzyści płynące z tych wdrożeń są tak znaczące, że należy liczyć się z wykładniczym wzrostem popularności przetwarzania brzegowego także w innych państwach. To będzie naturalny czynnik wzrostu dla chmury publicznej, bowiem – przy zagwarantowanej minimalizacji ilości zbieranych przez urządzenia OT danych – usługi infrastruktury chmurowej staną się najlepszym, bo stale dostępnym i relatywnie tanim repozytorium.

W trosce o finanse

Tworzenie planów finansowych związanych z migracją do chmury stanowi jednak dla firm niemałe wyzwanie. Według badania przeprowadzonego przez firmę Komprise, przedsiębiorstwa często mają bardzo ograniczony wgląd w dane dotyczące ponoszonych wydatków, co uniemożliwia ich skuteczną optymalizację. Podczas gdy dwa lata temu 27 proc. zbadanych przedsiębiorstw zarządzało co najmniej 10 petabajtami danych w chmurze, w tym roku ich odsetek wzrósł już do 32 proc. Szefowie IT zakładają, że ilość wykupionej pamięci masowej praktycznie nigdy nie jest wystarczająca, robią więc zakupy na zapas. To jednak prowadzi do braku optymalnego wykorzystania przestrzeni, a w szczególności do nieprawidłowego doboru klasy wydajnościowej wybranego repozytorium w chmurze dla różnego rodzaju danych.

Analitycy zakładają, że wkrótce standardem stanie się włączenie operacji finansowych dotyczących kwestii związanych z chmurą do codziennej praktyki firm. Działy IT będą musiały zrozumieć mechanizmy kosztowe związane z przechowywaniem danych, a także analizować wzorce ich wykorzystania przed projektem migracji do chmury i po jego zakończeniu. Konieczne będzie też nauczenie się komunikowania w jasny sposób tych wskaźników kierownictwu wyższego szczebla, bowiem informacje te staną się kluczowym czynnikiem w generowaniu wartości i zwrotu z inwestycji z migracji danych do chmury.

Fot. Adobe Stock

GenAI odmieni podejście **do bezpieczeństwa**

Zanim zespoły ds. bezpieczeństwa w pełni skorzystają z mechanizmów sztucznej inteligencji do obrony infrastruktury i zasobów, będą musiały mierzyć się z nowymi typami ataków, prowadzonych przez cyberprzestępców właśnie z jej użyciem.

Specjaliści Snowflake opracowali dokument „Data + AI Predictions 2024", w którym opisują możliwe kierunki rozwoju cyberprzestępczości w nadchodzących latach, jak też sugerują strategie reagowania na incydenty bezpieczeństwa. Jego treść skupia się na generatywnej sztucznej inteligencji, gdyż po sukcesie serwisu ChatGPT w przedsiębiorstwach zapanował boom na tę właśnie formę AI.

Sztuczna inteligencja w rozwiązaniach ochronnych pozwoli uszczelniać cyfrowe mury, automatyzować procesy wykrywania incydentów i reagowania na nie, będzie też niezastąpiona w zadaniach analizy oraz predykcji zagrożeń. Jednym z największych problemów związanych z bezpieczeństwem IT jest bowiem czas, jaki upływa pomiędzy uzyskaniem przez cyberprzestępców dostępu do firmowych systemów a wykryciem incydentu. W różnych raportach branżowych mediana tego okresu wynosi około dwóch tygodni.

Eksperci Snowflake podkreślają jednak, że wraz z rozpowszechnianiem się otwartych narzędzi AI, cyberprzestępcy nabyli zdolność generowania zupełnie nowych typów ataków, na które działy bezpieczeństwa nie są jeszcze gotowe. Co gorsza, mogą zupełnie dowolnie eksperymentować z AI, bez oglądania się na jakiekolwiek regulacje.

Pomoc w zrozumieniu potencjalnie niebezpiecznego zachowania może stanowić analiza danych behawioralnych. Odchylenia od wzorców dotyczących tego gdzie, kiedy i do jakich systemów określony pracownik uzyskuje dostęp, mogą zostać przypisane osobie posługującej się skradzionymi danymi uwierzytelniającymi lub jakiejkolwiek innej złośliwej działalności. Można spodziewać się, że właśnie GenAI będzie bardzo wydajna w ocenie i wychwytywaniu takiej aktywności.

Programiści na celowniku cyberprzestępców

Z uwagi na rosnącą rolę uczenia maszynowego i automatyzacji w procesach wytwarzania oprogramowania DevOps (a zwłaszcza DevSecOps) zmniejsza się liczba błędów, które może popełnić człowiek, a które – niezauważone – mogą trafić do wersji produkcyjnej aplikacji. Dlatego autorzy dokumentu „Data + AI Predictions 2024" twierdzą, że konsekwencją stosowania mechanizmów sztucznej inteligencji w rozwiązaniach ochronnych będzie zmiana priorytetów atakujących – cyberprzestępcy będą szukać sposobów na przedostanie się do środowisk programistycznych, ponieważ tam szansa na znalezienie i wykorzystanie podatności będzie wyjątkowo duża.

– *Rozwój jest z natury chaotyczny i eksperymentalny, więc zrozumienie tego, co w środowisku programistycznym jest normalne, a co nienormalne, jest bardzo trudne. Dlatego zespołom odpowiedzialnym za bezpieczeństwo trudniej jest bronić się przed atakami, a dla ich dyrektorów ważnym zadaniem staje się tworzenie reguł dla akceptowalnych działań programistycznych* – mówi Grzegorz Kapusta, dyrektor ds. inżynierii i szef warszawskiego biura Snowflake.

Jedną z najskuteczniejszych form cyberataku pozostaje dziś phishing. Według CERT Polska, w 2022 r. stanowił on 2/3 wszystkich obsłużonych przez ten zespół incydentów. Jak wskazują eksperci Snowflake, ataki te, chociaż w swojej istocie nieskomplikowane, mogą za sprawą wykorzystania generatywnej sztucznej inteligencji stać się znacząco trudniejsze do rozpoznania. Łatwo wyobrazić sobie sytuację, gdy atakujący będą za pośrednictwem narzędzi GenAI preparować komunikację firmową, szkoląc modele na przechwyconych wiadomościach wymienianych przez pracowników lub na bazie dostępnej powszechnie wiedzy o profilu i ofercie danej firmy.

Grzegorz Kapusta, *dyrektor ds. inżynierii i szef warszawskiego biura Snowflake*

Firmy podejmują mniej lub bardziej zaawansowane próby wprzęgnięcia GenAI w swoje procesy i działania z dwóch głównych przyczyn: nie chcą pozostać w tyle za konkurencją, a jednocześnie próbują przygotować się na moment, gdy mechanizmy AI osiągną większą dojrzałość. W warunkach dopiero tworzących się wewnętrznych procedur, reguł polityki bezpieczeństwa oraz zewnętrznych, branżowych i prawnych regulacji dotyczących wykorzystania sztucznej inteligencji, inicjatywy te mają często charakter doświadczalny. Tymczasem cyberprzestępcy, którzy też eksperymentują z AI, nie mają takich ograniczeń.

Dodatkowe informacje:
Grzegorz Kapusta, dyrektor ds. inżynierii i szef warszawskiego biura, Snowflake
grzegorz.kapusta@snowflake.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SNOWFLAKE.

Nie ma ucieczki **od hybrydy**

Dostawcy oprogramowania coraz bardziej starają się wykorzystywać w swoich produktach sztuczną inteligencję. Nie inaczej jest w przypadku rozwiązań do backupu.

Wojciech Urbanek

Koncepcja tworzenia kopii zapasowych istnieje niemal tak długo, jak komputery. Praktycznie każdy liczący się dostawca rozwiązań do ochrony danych wchodził na rynek, aby sprostać specyficznym potrzebom użytkowników. I tak, Veritas zaistniał dzięki wprowadzeniu produktów dla środowiska Unix, podczas gdy Commvault utożsamiany jest z Windowsem, a Veeam z VMware'em. W obecnych czasach jednak na znaczeniu zyskują kompleksowe rozwiązania chroniące dane rozproszone w wielu różnych środowiskach.

– *Zauważamy wśród klientów zapotrzebowanie na heterogeniczne narzędzia do backupu i przywracania środowisk do pracy po awarii. Trudno się temu dziwić. W tej chwili na globalnym rynku działa ok. 23 tysięcy dostawców aplikacji SaaS* – zauważa Simon Taylor, prezes HYCU.

Trudno sobie wyobrazić chaos, nie wspominając już o kosztach, jaki powstałby, gdyby jakaś firma musiała wdrożyć osobne rozwiązanie do backupu dla każdej wykorzystywanej usługi SaaS. Zwłaszcza, że według opublikowanego przez BetterCloud raportu „State of SaaSOps 2023", przeciętne przedsiębiorstwo na świecie korzystało w ubiegłym roku średnio ze 130 aplikacji chmurowych.

AI pomoże w wykrywaniu anomalii.

– *Firmy przenoszą wiele operacji do chmur, co wpływa na rosnące zapotrzebowanie na elastyczne i skalowalne rozwiązania do tworzenia kopii zapasowych. Ponadto, rozwinięcie technologii sztucznej inteligencji i analizy danych znacząco wpłynęło na efektywność procesów backupu oraz identyfikowanie potencjalnych zagrożeń* – mówi Paweł Mączka, CTO i wiceprezes Storware'u.

Co istotne, świadomość usługobiorców na temat zabezpieczania danych przetwarzanych przez aplikacje chmurowe cały czas rośnie. W dużym stopniu przyczyniły się do tego cybergangi i... dostawcy usług chmurowych. Te pierwsze z coraz większą ochotą atakują środowiska SaaS (aż 55 proc. firm przyznało, że w ciągu ostatnich dwóch lat doświadczyło incydentu związanego z SaaS, jak wynika z „Annual SaaS Security Survey Report: 2024 Plans & Priorities, Adaptive Shields"), zaś usługodawcy zmagali się w ubiegłym roku z kilkoma awariami (Microsoft 365, Datadog, Google Cloud Identity and Access Management, Salesforce Slack). Nic dziwnego, że część specjalistów dmucha na zimne i rozgląda się za różnymi formami redundancji, które umożliwiają korzystanie z kopii zapasowych nawet w przypadku wystąpienia mniejszych lub większych usterek po stronie dostawcy usług backupu online.

Bez dywersyfikacji ani rusz

Najbardziej popularną i już nie najmłodszą strategią planowania backupu jest tzw. 3-2-1. Użytkownik przechowuje trzy kopie danych na dwóch różnych nośnikach pamięci, przy czym jedna z nich powinna znajdować się poza główną lokalizacją firmy. Dywersyfikacja eliminuje pojedynczy punkt awarii i dodaje nową warstwę bezpieczeństwa. Już od dawna stosują ją chociażby instytucje finansowe. Część firm idących z duchem czasu zdążyło się przestawić na metodę 3-2-1-1-0. Jak łatwo zauważyć pojawiają się tutaj dwie kolejne liczby „1" oraz „0", gdzie pierwsza oznacza przechowywanie jednej kopii w trybie offline (nie jest połączona z infrastrukturą teleinformatyczną), zaś druga codzienny monitoring kopii zapasowych i przeprowadzanie regularnych testów, co przekłada się na „zero niedostępności". Wprawdzie dostawcy usług chmurowych podpisują z klientami umowy SLA określające poziom dostępności, trwałości oraz integralności danych, to jednak mają one pewne ograniczenia. Takie strategie jak 3-2-1-1-0 czy 3-2-1 pozwalają użytkownikowi uniezależnić się od usługodawcy.

Przechowywanie danych zarówno w środowisku chmurowym, jak

Fot. Adobe Stock

i lokalnym, ma swoje mocne i słabe strony, a stawka jest zbyt wysoka, aby zdecydowanie postawić wyłącznie na jedną z opcji. Na przykład odzyskiwanie dużej ilości danych z chmury publicznej może być na tyle uciążliwym procesem, że nie uda się osiągnąć zamierzonego wskaźnika RTO (Recovery Time Objective), który definiuje czas, w jakim system ma powrócić do stanu przed awarii. Natomiast mała firma, korzystająca z zasobów cyfrowych o pojemności kilkunastu terabajtów, może być zadowolona z backupu online ze względu na niższe koszty (brak inwestycji w sprzęt i oprogramowanie) oraz skalowalność. Nie martwi się o też aktualizacje bezpieczeństwa, migracje danych czy starzenie się usług, ponieważ wszystko spoczywa na barkach dostawców.

Generalnie, w przypadku niewielkiej ilości danych łatwiej uzyskać zakładane RTO. Odzyskiwanie w chmurze jest też szybsze i łatwiejsze niż w przypadku kopii zapasowych przechowywanych w bibliotekach taśmowych.

– Usługi typu Backup as a Service będą stanowiły coraz większą część rynku rozwiązań do zabezpieczania danych. Użytkownicy często decydują się na przejście do chmury, ponieważ nie chcą utrzymywać żadnej infrastruktury we własnym zakresie, co dotyczy również infrastruktury do backupu – wyjaśnia Tomasz Krajewski, Senior Technical Sales Director w Veeamie.

Drugim bardzo istotnym wskaźnikiem opisującym skuteczność backupu jest RPO (Recovery Point Objective), definiujący moment oraz częstotliwość z jaką wykonywane są kopie zapasowe. Tutaj wiele zależy od oczekiwań użytkownika: jeśli są one wysokie (jak najmniejsza utrata danych), wymagają większej liczby kopii zapasowych, przestrzeni dyskowej oraz wysokiej wydajności komputerów i przepustowości sieci. Za to wszystko trzeba słono zapłacić, niezależnie do tego czy firma korzysta z backupu tradycyjnego czy online. Dlatego przed wyborem jednej z opcji przydałaby się dokładna analiza finansowa.

Backup i sztuczna inteligencja

Sztuczna inteligencja coraz częściej trafia także do rozwiązań do wykonywania kopii zapasowych. Veritas już w połowie 2022 r. zaprezentował koncepcję autonomicznego backupu, który łączy automatyzację ze sztuczną inteligencją oraz uczeniem maszynowym. Taki system łatwo dostosowuje się do zmieniających się okoliczności i natychmiast reaguje na wszelkie nieprawidłowości.

Jednak dopiero w ubiegłym roku zrobiło się głośno o zastosowaniu generatywnej sztucznej inteligencji w narzędziach do backupu. Dwaj producenci – Cohesity oraz Rubrik – poinformowali o integracji swoich produktów z inteligentnymi chatbotami. Takie rozwiązanie, przynajmniej teoretycznie, umożliwia klientom przeszukiwanie eksabajtów danych w celu uzyskania wglądu we wzorce danych w celu wykrycia zagrożeń, takich jak chociażby ransomware. Współpraca pozwala również na głęboką penetrację danych, żeby znaleźć odpowiedzi na bardzo konkretne pytania lub szybko odzyskać pliki za pomocą wyszukiwania kontekstowego.

Broadcom wywraca stolik?

Jednym z najważniejszych ubiegłorocznych wydarzeń na rynku IT był zakup VMware'a przez Broadcoma. Nowy właściciel, zaraz po oficjalnej finalizacji transakcji, podjął działania, które poważnie zaniepokoiły nie tylko pracowników VMware'a, ale również partnerów tego dostawcy. Zmiany w programie partnerskim oraz wzrost cen postawiły bowiem w trudnej sytuacji integratorów, którzy sprzedają produkty tej marki małym firmom. Zmiany te mogą wpłynąć na cały rynek backupu, gdyż mali i średni integratorzy, pokrzywdzeni przez Broadcoma, prędzej czy później zaczną rozglądać się za alternatywą dla VSphere'a, co dotyczy też narzędzi do backupu. Warto odnotować, że Veeam, znany ze swojego przywiązania do VMware'a, niedawno poinformował o testach z platformą Proxmox i zapowiedział wsparcie dla Oracle Linux KVM. Niewykluczone, że dostawcy rozwiązań do backupu zaczną promować swoje produkty jako te, które ułatwiają wycofanie się ze środowiska VMware'a. Wówczas część klientów chętniej podejmie decyzję o wdrożeniu mniej popularnych, za to tańszych platform wirtualizacyjnych. Wiele wskazuje na taki właśnie scenariusz.

Część ekspertów traktuje tego rodzaju zapowiedzi bardziej jako akcje marketingowe. Chociaż pojawiają się nowe interfejsy, to generatywna sztuczna inteligencja nie zmieniła w znaczący sposób procesów tworzenia kopii zapasowych. Z pewnością potrzeba na to jeszcze trochę czasu. Niewykluczone przy tym, że rozwój tej technologii w systemach do backupu będzie podążać w kierunku wykrywania anomalii. Tym bardziej, że od czasu, kiedy cyberprzestępcy zaczęli szyfrować kopie zapasowe, dostawcy systemów do backupu przejawiają duże zainteresowanie kwestiami bezpieczeństwa. Należy oczekiwać, że będą wprowadzali dodatkowe warstwy zabezpieczeń lub umożliwiali integrację swojego rozwiązania z produktami firm trzecich do ochrony środowisk IT.

Synology: pełna ochrona w jednym serwerze

Sprawne tworzenie kopii zapasowych wszystkich rodzajów danych, jak i obejmowanie ich innymi mechanizmami ochronnymi, zapewniają serwery NAS firmy Synology.

Eksperci zajmujący się backupem danych już ponad dekadę temu wypracowali najlepszą praktykę określaną trzema liczbami: 3-2-1. Oznacza ona, że powinny być wykonywane przynajmniej trzy kopie danych, z czego dwie na różnych rodzajach nośników, a jedna kopia powinna być przechowywana poza fizycznym miejscem produkcyjnego przetwarzania tych danych.

Zrealizowanie praktyki 3-2-1 z powodzeniem umożliwiają serwery NAS firmy Synology. Mogą stanowić repozytorium plików pochodzących ze stacji roboczych, serwerów (w tym innych serwerów NAS), środowisk wirtualnych i aplikacji chmurowych. Zabezpieczanie danych możliwe jest także za pomocą mechanizmu migawek uruchamianych wewnątrz tego samego serwera, który udostępnia dane do produkcyjnego użycia.

Z takiego serwera za pomocą aplikacji **Hyper Backup** można wykonać dodatkową kopię – na kolejny serwer NAS, podłączony przez port USB zewnętrzny zasób dyskowy lub do chmurowego repozytorium (np. do usługi **Synology C2 Storage**). Oprogramowanie Synology umożliwia również szybkie odzyskiwanie danych według założonego wcześniej scenariusza, w tym odtworzenie kopii systemu bare-metal, przywrócenie do systemu plików oraz natychmiastowe uruchomienie maszyny wirtualnej bezpośrednio z jej kopii.

Dla użytkowników pakietów biurowych w postaci usługi chmurowej dostępne są dodatkowe przygotowane przez Synology 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 Drive, Contacts i Calendar.

Zapisz tylko raz

Istnieje wiele powodów, dla których warto rozważyć wdrożenie mechanizmu uniemożliwiającego modyfikację lub skasowanie raz zapisanych danych. Jednym z nich jest rosnąca liczba regulacji prawnych stawiających wymóg przechowywania informacji w sposób gwarantujący ich niezmienność. Kolejnym zaś może być wola menedżerów, którzy w ten sposób chcą sobie zagwarantować, że część firmowych danych będzie mogła być bez żadnych wątpliwości wykorzystana w procesach sądowych. Nadrzędną przyczyną jest jednak działalność cyberprzestępców – dzięki blokadzie modyfikacji danych nie zostaną one zaszyfrowane podczas ataku ransomware. Wdrożenie takiego rozwiązania neutralizuje też próbę sabotażu podjętego chociażby przez niezadowolonego pracownika firmy, który otrzymał wypowiedzenie.

Mechanizm gwarantujący niezmienność danych nazywa się WORM (Write Once, Read Many) i od ponad roku jest dostępny w systemie DiskStation Manager 7.2 (DSM 7.2) pod nazwą **WriteOnce** w niemal 50 modelach serwerów NAS Synology (także poprzednich generacji, od serii 20 wzwyż oraz w urządzeniach z serii SA, FS i HD). Umożliwia on objęcie ochroną przed modyfikacją wskazanych przez administratora folderów z plikami przez określony czas lub trwale.

25 kwietnia br. Synology organizuje webinar, podczas którego eksperci producenta przedstawią szczegóły dotyczące funkcjonowania mechanizmu WriteOnce.

Synology®

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

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ SYNOLOGY.

Rubrik: **ransomware nam niestraszny**

Rubrik zaprojektował rozwiązanie do backupu z funkcją gwarantującą ochronę zabezpieczanych danych przed zewnętrznymi zagrożeniami.

Rubrik stworzył rozwiązanie, które – dzięki zniesieniu ograniczeń w architekturze – zmieniło zasady gry w zakresie tworzenia kopii zapasowych. Jednym z głównych filarów było założenie, że nowy system ma być nie tylko odpowiedzialny za backup, ale powinien sam być przedmiotem nieustannych ataków. Tym samym musi być wyposażony w niezawodne mechanizmy ochronne.

W efekcie powstała platforma, która nie wykorzystuje otwartej architektury ani komercyjnych systemów operacyjnych, zawierających wiele znanych oraz nieznanych jeszcze luk w systemach zabezpieczeń. Rozwiązanie Rubrika zbudowane zostało na utwardzonym jądrze Linuksa, z aktualizacjami nie wymagającymi restartu urządzenia, na którym jest zainstalowane. Zastosowany w nim system plików Atlas został stworzony od podstaw i jest używany wyłącznie przez Rubrik. Jego skalowalna architektura zapewnia brak ograniczeń wydajności, która rośnie liniowo wraz z dodawaniem do systemu kolejnych węzłów (urządzeń).

Rozwiązanie do backupu firmy Rubrik dostępne jest dla klientów w trzech postaciach – oprogramowania, appliance'u sprzętowego oraz usługi w chmurze publicznej. Dzięki temu można je wykorzystać do zabezpieczenia danych we wszystkich występujących w przedsiębiorstwach scenariuszach. Urządzenia z preinstalowanym oprogramowaniem Rubrik dostępne są jako system z architekturą wysokiej dostępności, składającą się z 4-węzłowego klastra ze zintegrowanym deduplikatorem i przestrzenią dyskową do przechowywania danych. Twórcy systemu wyeliminowali pojedyncze punkty awarii oraz zapewnili użytkownikom nadmiarową moc obliczeniową na wypadek konieczności przywrócenia danych do sytuacji sprzed awarii.

Bezpieczeństwo przede wszystkim

Dane w kopiach zapasowych są indeksowane i zarządzane centralnie, dzięki czemu można je przeszukiwać i przywracać z jednego miejsca. Są chronione przed atakami ransomware dzięki mechanizmowi galwanicznej separacji danych, przez co wyeliminowano ryzyko zaszyfrowania ich w trakcie ataku.

Wśród dodatkowych mechanizmów zabezpieczeń znajduje się też wymuszenie stosowania uwierzytelniania wieloskładnikowego lub jednorazowych haseł, co eliminuje ryzyko uszkodzenia kopii zapasowej z wykorzystaniem ataku na konto uprzywilejowane administratora backupu. System Atlas używa też własnego protokołu komunikacji i nie można go wykryć w sieci za pomocą mechanizmów śledzenia standardowych protokołów komunikacji lub routingu. Dodatkowo, funkcja „retention lock" uniemożliwia skrócenie czasu retencji kopii zapasowych. Metoda ta bywa wykorzystywana podczas ataków ransomware, w trakcie której usuwane są stare kopie danych, a najnowsza zawiera już tylko zaszyfrowane dane.

Unikalną cechą rozwiązania Rubrik jest też blokada przed atakami na usługę zegara sieciowego NTP. To niestety popularna metoda niszczenia kopii zapasowych, która polega na zaatakowaniu serwera usługi NTP i zmianie ustawień zegara oraz daty na odległą w przyszłości. W rezultacie serwer backupu, który cyklicznie sprawdza i synchronizuje swój zegar systemowy w usłudze Windows z serwerem NTP, sam kasuje starsze kopie zapasowe jako niepotrzebne, ponieważ miał przechowywać kopię tylko przez określoną liczbę dni.

Rubrik jest tak pewien niezawodności swojego rozwiązania, że jako jedyna firma daje pisemną gwarancję dostępności danych. Jeżeli nie udałoby się ich odzyskać, w ramach gwarancji producent zobowiązuje się do wypłaty odszkodowania w wysokości do 10 mln dol. Jednak, jak przekonują menedżerowie producenta, żaden spośród ponad 5 tys. jego klientów na świecie nie stracił swoich danych i nie musiał płacić okupu w przypadku ataku ransomware. Co więcej, wszyscy klienci odzyskali 100 proc. swoich danych w ciągu kilku do kilkunastu godzin po ataku. Do ich całodobowej dyspozycji jest też zespół Ransomware Response Team, którego jedynym zadaniem jest pomoc ofierze ataku w jak najszybszym przywróceniu systemów do pracy.

rubrik

INGRAM MICRO

Dodatkowe informacje:
Paweł Zaręba, Business Development Manager Security, Ingram Micro
pawel.zareba@ingrammicro.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI RUBRIK I INGRAM MICRO.

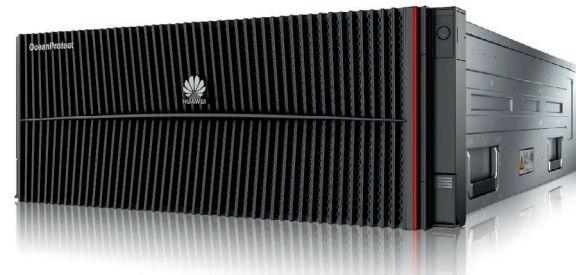
Backup nadzieją na walkę z atakami ransomware

W styczniu br. firma Veeam opublikowała doroczny dokument „Data Protection Trends Report 2024", w którym przedstawiła wyniki przeprowadzonego w ostatnim czasie badania preferencji 1200 klientów dotyczących środowisk zabezpieczania danych. Jednym z najważniejszych czynników dla ankietowanych okazało się zapewnienie spójności zabezpieczanych w postaci backupu danych oraz niezawodność tego środowiska. Firmy deklarują też chęć rozbudowania go o możliwość wykonywania kopii zapasowych do i z usług chmurowych – zarówno w ramach usług Backup as a Service (BaaS), jak też Disaster Recovery as a Service (DRaaS).

Najczęstszą i najbardziej dotkliwą przyczyną utraty danych pozostaje ransomware. Z tego powodu firmy poszukują rozwiązań zdolnych do przeciwdziałania temu rodzajowi cyberzagrożeń. Ale pozostają świadome, że utrata dostępu do informacji może nastąpić też z powodu takiej katastrofy jak pożar czy zalanie, jak też w wyniku błędów użytkowników.

Źródło: „Data Protection Trends Report", Veeam, styczeń 2024

Backup na nośniki flash to (już) nie utopia



Huawei ma w ofercie innowacyjne rozwiązanie do backupu danych, przeznaczone dla firm oczekujących wyjątkowej trwałości i wydajności systemu ochrony informacji. Jego unikalną cechą jest możliwość wyboru pamięci SSD jako wyłącznego nośnika kopii zapasowych.

Przedsiębiorstwa coraz rzadziej postrzegają backup wyłącznie jako koszt związany z koniecznością posiadania ubezpieczenia, ale widzą w tej procedurze dodatkowe szanse na usprawnienie działalności biznesowej. Kopie danych mogą być wykorzystywane na różne sposoby, w tym do prowadzenia analiz bez obciążania środowiska produkcyjnego, czy uczenia mechanizmów generatywnej sztucznej inteligencji. Zwiększone oczekiwania wobec systemów backupu coraz częściej zgłaszają podmioty z sektora publicznego, branży finansowej i telekomunikacyjnej, placówki ochrony zdrowia, firmy produkcyjne.

Rosną też oczekiwania wobec samych środowisk backupu. Gdy dochodzi do awarii macierzy obsługującej maszyny wirtualne, administratorzy liczą na możliwość uruchomienia ich kopii bezpośrednio z repozytorium backupu. Zapewni to jak najkrótszą przerwę w działalności biznesowej, a jednocześnie da czas administratorom na spokojne przywrócenie podstawowego środowiska. Zagwarantowanie tak dużej wydajności jest jednak niemożliwe przy zastosowaniu mechanicznych twardych dysków. **Dlatego Huawei doprowadził do przełomu – jest pierwszym producentem, który jako nośniki do backupu zastosował pamięci flash.**

Wydajnie i bezpiecznie

Rozwiązanie Huawei OceanProtect umożliwia stworzenie środowiska backupu w modelu flash-to-flash-to-anything (F2F2X) – jako alternatywę do popularnego od lat modelu disk-to-disk-to-tape (D2D2T). Dostępne są cztery modele tego rozwiązania – trzy (X6000, X8000 i X9000) opcjonalnie można wyposażyć wyłącznie w dyski SSD SAS, co gwarantuje bardzo wysoką prędkość zapisu i odczytu danych (rzędu kilkuset terabajtów lub nawet kilku petabajtów na godzinę), zaś dla firm, które nie potrzebują tak dużej wydajności, zachowano też możliwość skorzystania z tradycyjnych mechanicznych napędów NL-SAS. W czwartym modelu – X3000 – podstawowym nośnikiem danych są dyski HDD, zaś SSD dostępne są jako cache (dzięki temu skrócone zostało okno backupowe). **To jedyne tego typu rozwiązanie w klasie entry level, w którym zastosowano dwa kontrolery, a przez to wyeliminowano pojedynczy punkt awarii.**

Przyspieszenie pracy systemu Huawei OceanProtect uzyskano dzięki uwolnieniu zasobów procesora w kontrolerze za pomocą silnika Direct TCP/IP Offload Engine (DTOE), a także grupowaniu rdzeni procesora, łączeniu kilku sekwencyjnych strumieni danych oraz partycjonowaniu zadań. Dostępny jest również mechanizm deduplikacji danych na urządzeniu źródłowym, dzięki któremu zmniejszona zostaje ilość danych przesyłanych przez sieć i skrócony zostaje czas tworzenia kopii zapasowych (współczynnik redukcji danych może wynieść nawet do 72:1). Zgromadzone informacje poddawane są też innym procesom zapewniającym jak najbardziej oszczędne wykorzystanie nośników, w tym kompresji i kompaktowaniu na poziomie bajtów.

Deduplikator Huawei OceanProtect współpracuje ze wszystkimi popularnymi narzędziami do backupu. Jego konstruktorzy wzięli pod uwagę także kwestie bezpieczeństwa danych gromadzonych w repozytorium – ochronę przed wyciekiem zapewnia szyfrowanie podczas przesyłania i przechowywania. Z kolei przed utratą kopii zapasowych chroni mechanizm bezpiecznych migawek (secure snapshots). Natomiast zaszyfrowanie danych podczas ataku ransomware nie powiedzie się dzięki zastosowanej technologii fizycznego odseparowania nośników od środowiska produkcyjnego (air gap).

Warto również podkreślić, że zgodność z regulacjami prawnymi, które nakazują zapewnienie niezmienności danych, umożliwia mechanizm blokujący ich skasowanie lub zmodyfikowanie (Write Once Read Many, WORM). Wysoką dostępność rozwiązania zagwarantują natomiast redundantne kontrolery pracujące w trybie active-active, co przyczyniło się do uzyskania niezawodności całego systemu na poziomie 99,9999 proc.

Dodatkowe informacje:
Marcin Kostrzewa
Product Manager, Arrow
Marcin.Kostrzewa@arrow.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI HUAWEI I ARROW.

NAKIVO: niezawodny backup bez inwestowania w nowy sprzęt

Bezpieczeństwo środowisk IT często postrzegane jest jako koszt, co prowokuje do poszukiwania oszczędności w tym obszarze. Podobnie jest z kwestiami dotyczącymi backupu danych. Świadoma tej sytuacji firma NAKIVO opracowała rozwiązanie, które zapewnia bardzo bogatą funkcjonalność, ale jednocześnie minimalizuje koszty jego wdrożenia i obsługi.

Założona w 2012 r. firma NAKIVO to amerykański producent narzędzi do backupu, jeden z najszybciej rozwijających się w branży oprogramowania do ochrony danych. Na przestrzeni lat wiele zainwestowała w europejską kadrę i biuro na Ukrainie, w Kijowie. Od 2017 r. wyłącznym dystrybutorem NAKIVO w Polsce jest poznańskie Konsorcjum FEN, wieloletni lider sprzedaży dystrybucyjnej serwerów NAS.

Obecnie NAKIVO zapewnia niezawodne rozwiązanie typu „wszystko w jednym" do backupu środowisk wirtualnych, fizycznych, chmurowych i SaaS – NAKIVO Backup & Replication. Jego możliwości obejmują tworzenie kopii zapasowych, replikację, natychmiastowe odzyskiwanie, odzyskiwanie po awarii, a także ochronę przed atakami ransomware i monitorowanie zasobów IT. Wszystkie te funkcje są dostępne w przystępnym modelu cenowym, który jest o prawie 50 proc. niższy niż w przypadku konkurentów.

Na całym świecie producentowi zaufało już ponad 27 tys. klientów w 182 krajach. Referencje wystawiły mu tak wielkie marki, jak Coca-Cola, Honda, Siemens i Cisco. Także w Polsce jest wielu zadowolonych klientów z różnych branż – medycznej, górniczej, produkcyjnej czy edukacyjnej. Jedno z największych lokalnych wdrożeń obejmuje prawie 200 procesorów, z centralnym zarządzaniem w Poznaniu i rozproszoną instalacją na 34 placówki medyczne.

NAKIVO może pochwalić się pięciogwiazdkowymi recenzjami i wskaźnikiem zadowolenia klientów na poziomie 98 proc. Na przestrzeni lat producent otrzymał wiele nagród oraz wyróżnień od ekspertów branżowych i mediów w dziedzinie tworzenia kopii zapasowych i odzyskiwania danych (w tym niedawne wyróżnienie w raporcie „Gartner Peer Insights: Voice of the Customer for Enterprise Backup and Recovery Software Solutions 2024").

Duża funkcjonalność przy małych wymaganiach

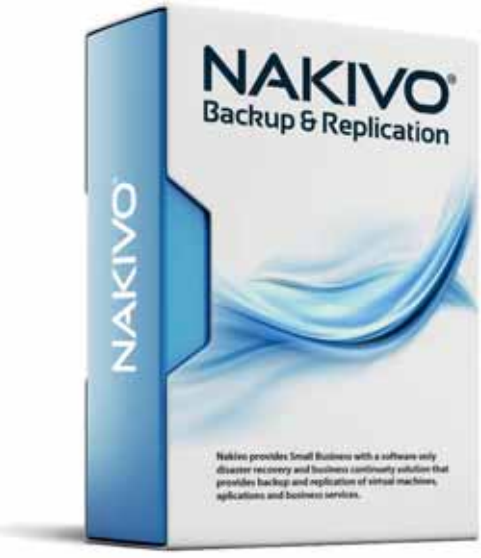
Rozwiązanie NAKIVO Backup & Replication jest bardzo intuicyjne i łatwe w użyciu. Klienci nie potrzebują tracenia wielu godzin na lekturę samouczków, aby skonfigurować i uruchomić pierwsze zadania backupowe (co jest charakterystyczne dla rozwiązań konkurencyjnych). Internetowy interfejs pozwala łatwo konfigurować zadania tworzenia kopii zapasowych i odzyskiwania danych z dowolnego urządzenia lub lokalizacji oraz zarządzać nimi. Aby usprawnić proces, pulpit kalendarza upraszcza planowanie i przeglądanie przepływów pracy, a automatyzacja bazująca na regułach umożliwia automatyczne tworzenie kopii zapasowych i replikację.

Bogata funkcjonalność NAKIVO Backup & Replication zapewnia niezawodną ochronę danych w wielu środowiskach, takich jak VMware vSphere, Microsoft Hyper-V, Nutanix AHV, AWS EC2, Microsoft 365, serwery i stacje robocze Windows/Linux, re-

Główne zalety współpracy partnerskiej z NAKIVO

- Przejrzysty program partnerski, prosto liczone rabaty, gwarancja zarobku przy każdym projekcie
- Możliwość zarabiania również na odnowieniach (**brak „drugich" cen**)
- Przejrzyste licencjonowanie – licencje wieczyste, subskrypcyjne oraz możliwość rozliczania w trybie miesięcznym
- Zniżki do 35 proc., promocje i dodatkowe korzyści dla różnych poziomów partnerstwa
- Dostęp do zweryfikowanych leadów sprzedażowych i gotowych do użycia materiałów informacyjnych
- Częściowy zwrot kosztów związanych z działaniami marketingowymi
- Ciągłe szkolenia, certyfikacja i webinaria przeznaczone dla personelu technicznego oraz sprzedażowego
- Portal partnerski umożliwiający wygodne zarządzanie licencjami, dostęp do licencji NFR, cen i materiałów szkoleniowych
- Menedżerowie kanału zapewniający wsparcie regionalnych liderów i promocję rozwoju biznesu
- Całoroczny marketing, a także możliwości co-brandingu

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI NAKIVO I KONSORCJUM FEN.



pozytoria plików i bazy danych Oracle. Wszystko to z jednego ujednoliconego panelu zarządzania – bez potrzeby stosowania oddzielnych rozwiązań i wielu interfejsów, co upraszcza zarządzanie ochroną danych i zmniejsza koszty.

Rozwiązanie to oferuje również elastyczne opcje wdrażania, w tym instalacje lokalne, urządzenia wirtualne i wdrożenia w chmurze, które pozwalają klientom wybrać najlepszą opcję dla ich konkretnych potrzeb. Użytkownicy NAKIVO Backup & Replication cenią sobie również to, że konsolę tego rozwiązania można zainstalować na niemal dowolnym cyfrowym urządzeniu. Wymagania sprzętowe są tak niewielkie, że działa ona nawet na Raspberry Pi. Natomiast ponad 80 proc. polskich klientów ma zainstalowaną konsolę NAKIVO na serwerze NAS, który już posiadają w firmie. Do konsoli podłączane są lokalne oraz w pełni szyfrowane zdalne repozytoria – wszystko w cenie licencji.

Unikalny model cenowy rozwiązania NAKIVO Backup & Replication został zaprojektowany tak, aby był przystępny i przejrzysty, bez żadnych ukrytych opłat lub dodatkowych kosztów. Oprogramowanie to jest dostarczane z licencją wieczystą lub subskrypcyjną – w zależności od platformy, która ma być chroniona i wymagań przedsiębiorstwa w zakresie zabezpieczania danych.

Trzy pytania do...

Antona Shelepchuka, dyrektora sprzedaży w NAKIVO

Co najbardziej cenią sobie partnerzy we współpracy z NAKIVO?

Przede wszystkim to, że jako zorientowana na kanał firma programistyczna z ponad dziesięcioletnim doświadczeniem w branży ochrony danych, zapewniamy nieustanny rozwój swojego produktu i usług. Dbamy o to, abyśmy wspólnie byli gotowi na zmiany potrzeb nowoczesnych przedsiębiorstw w tym zakresie, wynikające zarówno z ich rozwoju technicznego, jak też sytuacji związanej z bezpieczeństwem danych, w tym wzrostu popularności ataków ransomware. Partnerzy handlowi oczekują długoterminowej perspektywy przychodów, jasnej wizji współpracy i otwartej, proaktywnej komunikacji ze swoimi dostawcami. I właśnie to im zapewniamy, wraz z konkurencyjnymi cenami, dzieleniem się informacjami o potencjalnych klientach, wczesnymi informacjami o produktach, szkoleniami technicznymi/sprzedażowymi oraz całodobową dostępnością zespołu wsparcia.

Które funkcje rozwiązań NAKIVO są najbardziej doceniane przez klientów?

Otrzymują wszystko czego potrzebują w jednym rozwiązaniu: tworzenie kopii zapasowych, replikację, natychmiastowe odzyskiwanie danych, ochronę przed skutkami ataku ransomware, przywracanie środowisk po awarii oraz monitorowanie infrastruktury IT. Wraz z prostotą obsługi ma to zasadnicze znaczenie dla budowania lojalności i satysfakcji klientów. Warto też wspomnieć o dostępności wielu typów licencji, w tym typ wieczysty licencjonowany per gniazdo procesora, który większość dostawców wyeliminowała. Korzystniejsze o nawet 50 proc. niż w przypadku konkurencji są też ceny, przystosowane do możliwości zarówno małych firm, jak również dużych przedsiębiorstw.

NAKIVO może pochwalić się bardzo wysokim wskaźnikiem odnowień oraz poleceń oprogramowania do backupu innym potencjalnym klientom. Co jest tego główną przyczyną?

Rozumiemy, że usatysfakcjonowani klienci są bardziej lojalni – dlatego nie zadowalamy się podejściem „to po prostu działa", lecz staramy się wykraczać poza to, czego oczekują od nas użytkownicy. Tak wysoki wskaźnik odnowień to efekt połączenia wszystkich wymienionych wcześniej korzyści: zapewnienia konkurencyjnych cen, elastycznego modelu licencyjnego oraz łatwości użytkowania i zaawansowanej funkcjonalności rozwiązania NAKIVO Backup & Replication. Partnerzy mają również ogromny wkład w ten wynik – mając **rabaty partnerskie na wyłączność przy odnowieniach** chętniej pilnują klienta, aby odnowił wsparcie. Dodatkowo ogromne znaczenie ma wysiłek włożony w nieustanne podnoszenie poziomu obsługi klientów. Nasz zespół ekspertów jest gotowy przez całą dobę do zorganizowania zdalnej sesji, aby szybko i skutecznie zająć się problemami klientów, dzięki czemu wskaźnik ich zadowolenia wynosi 98 proc.

Inżynierowie FEN – w ramach projektu Akademia NAKIVO – nagrali serię krótkich instruktażowych filmów, w których dzielą się wiedzą na temat najlepszych praktyk w zakresie konfiguracji oprogramowania tego producenta.

NAKIVO®

FEN

Dodatkowe informacje:
Mateusz Łuka, Product Manager Backup & Storage, Konsorcjum FEN
Mateusz.Luka@fen.pl
tel. 510 044 710

Cyfrowe archiwa pękają w szwach

Firmy natrafiają na coraz większe trudności związane z zarządzaniem cyfrowymi zasobami. Jednym z największych wyzwań jest archiwizacja dużych zbiorów danych.

Wojciech Urbanek

Przedsiębiorstwa gromadzą dane, wychodząc z założenia, że zawsze mogą się do czegoś przydać. Zresztą w taki sam sposób postępują użytkownicy indywidualni. Jednak o ile ci ostatni na swoich komputerach czy domowych NAS-ach przechowują maksymalnie kilka terabajtów danych, o tyle średnie i duże firmy zgłaszają zapotrzebowanie na przestrzeń liczoną w petabajtach, a nawet eksabajtach. Najwięcej danych generują urządzenia w sieci IoT, aplikacje naukowe oraz inżynieryjne, media, monitoring wizyjny czy modele sztucznej inteligencji. W tych obszarach ilość danych rośnie niemal w tempie wykładniczym, co obciąża firmowe repozytoria, a tym samym budżety IT.

Jeszcze do niedawna pod pojęciem cyfrowej archiwizacji kryło się przechowywanie danych przez okres od kilku miesięcy do kilkunastu lat. Na ogół były to nikomu niepotrzebne zasoby, które musiały znaleźć się w cyfrowym archiwum ze względu na regulacje i rozporządzenia prawne. Dlatego od lat funkcjonuje podział na dane gorące i zimne. Gorące znajdują się bardzo blisko „ciepła", a więc obracających się dysków i procesorów, zaś zimne spoczywają na tych dyskach lub taśmach, które są ukryte gdzieś daleko na półce.

– *Szybki dostęp do zarchiwizowanych danych był często czynnikiem drugoplanowym. Dlatego w przypadku rozwiązań archiwizacyjnych dopuszczano wykorzystywanie nośników off-line, takich jak taśmy magnetyczne. Dzisiaj kwestie szybkiego wyszukiwania danych oraz dostępu stają się coraz bardziej istotne, a to w dużym stopniu zależy od procesu i sposobu ich archiwizacji* – tłumaczy Krzysztof Lorant, Pure Storage Business Development Manager w TD Synnex.

W rezultacie proste i czytelne podziały zaczynają się nieco zacierać. Gorące dane to takie, do których potrzebny jest szybki dostęp (w przeciwieństwie do chłodnych). Jednak, jak do tej pory, nie doczekano się standardowej definicji określających „ciepło" i „zimno".

Segregacja danych

Według klasycznej szkoły w ciągu pierwszego miesiąca od utworzenia danych, aż 80 proc. z nich jest używana sporadycznie lub w ogóle. Dlatego zaleca się zachowanie 20 proc. aktywnych danych na nośnikach flash, zaś resztę na HDD lub taśmach. Niestety, tendencje szybko się zmieniają, bowiem firmy wykorzystują dane do analiz w czasie rzeczywistym czy zasilania nimi systemów AI.

Najczęstszym sposobem określenia czy zbiór danych jest wystarczający, jest zastosowanie reguły 10-krotności. Zasada ta oznacza, że ilość danych wejściowych (czyli liczba przykładów) powinna być dziesięciokrotnie większa niż liczba parametrów w zestawie danych. Przykładowo, jeśli algorytm ma odróżniać obrazy ryb od krokodyli na podstawie tysiąca parametrów, do wytrenowania modelu potrzeba dziesięć tysięcy zdjęć.

– *Dostępne rozwiązania w zdecydowanej większości zapewniają na etapie archiwizacji odpowiednią klasyfikację treści, a także bazujące na AI i ML obudowywanie plików w odpowiednie metadane oraz słowa kluczowe. Nie wystarczy już wyłącznie platforma sprzętowa do przechowywania odpowiedniej ilości danych. Musi być dostarczana w komplecie z odpowiednim oprogramowaniem* – wyjaśnia Krzysztof Lorant.

Fot. Adobe Stock

Klasyfikacja danych w systemach produkcyjnych i przeznaczonych do archiwizacji

	Gorące dane	Ciepłe dane	Zimne dane
Lokalizacja danych	Jak najbliżej miejsca przetwarzania	Łatwo dostępne w pobliżu	Poza siedzibą przetwarzania
Dostęp do danych	Szybki i częsty	Wolniejszy i rzadszy	Najwolniejszy i sporadyczny
Rodzaj pamięci masowej	Macierze SAN oraz zoptymalizowana pamięć masowa w chmurze	Serwery NAS i repozytoria chmurowe	Wolne macierze dyskowe i biblioteki taśmowe

Na rynku nie brakuje produktów przeznaczonych do zarządzania danymi znajdującymi się na różnych urządzeniach, najczęściej serwerach NAS. Systemy takie identyfikują dane, a następnie przenoszą je na bardziej ekonomiczną platformę, która może znajdować się w środowisku chmury publicznej. Wraz z przyrostem zasobów cyfrowych, firmy popełniają kardynalne błędy polegające na kupowaniu przestrzeni dyskowej bądź traktowaniu jej jako taniej szafki do magazynowania plików.

Ruch w dwie strony

W chmurze publicznej może być obecnie przechowywana nawet połowa wszystkich danych biznesowych. Najwięksi hiperskalerzy co roku notują przyrosty zarówno pod względem przychodów, jak i ilości przechowywanych informacji. Jednak ruch nie odbywa się wyłącznie w jedną stronę, gdyż część firm decyduje się na rozwiązania hybrydowe, gdzie dane znajdują się także w środowisku lokalnym. Z danych firmy konsultingowej Aptum wynika, że 77 proc. firm korzysta z chmury publicznej, zaś 86 proc. planuje czerpać korzyści z usług hybrydowych lub wielochmurowych.

– *Znaczenie obu tych środowisk rośnie równolegle. Zaczęły być wobec siebie komplementarne, a nie – jak dotychczas – konkurencyjne. Myślę, że to nie pojemność decyduje o opłacalności chmury w archiwizacji, a tempo przyrostu danych, ich rodzaj i częstotliwość dostępu do nich* – mówi Jakub Bala, Product Manager w Stovarisie.

W przypadku archiwizacji chłodnych danych chmura publiczna może być dość dobrą opcją. Aplikacje do archiwizacji bądź tworzenia kopii zapasowych pracują w tle, więc jakiekolwiek problemy z wydajnością nie powinny mieć negatywnego wpływu na pracę użytkowników. Niemniej jest i druga strona medalu – menedżerowie IT, którzy spodziewają się oszczędności wynikających z przesuwania zasobów do chmury, mogą wpaść w pułapkę kosztów. Usługodawcy komplikują swoje cenniki, stosując różne stawki i dodatkowe opłaty. Szczególnie uciążliwe dla usługobiorców są koszty związane z pobieraniem danych z chmury. Czasami klienci przechowują zasoby cyfrowe przez dłuższy czas na droższych warstwach, zamiast w archiwach.

– *Pięć lat przechowywania petabajta danych w chmurze publicznej kosztuje od 1,2 do 1,5 miliona dolarów. Jesteśmy zazwyczaj tańsi, a takim punktem przełomowym jest 100 TB. Poniżej tej pojemności bardziej opłaca się korzystać z dostawców usług chmurowych, zaś od 100 TB do 400 TB dużo korzystniej wybrać środowisko lokalne* – przekonuje Philip Storey, CEO Xen Data.

Ważnym trendem jest rosnąca popularność modelu Storage as a Service. Najwięksi dostawcy macierzy dyskowych dostarczają swój sprzęt, aczkolwiek użytkownik nie płaci za urządzenie, lecz rozliczany jest okresowo za wykorzystanie pojemności.

– *W takim scenariuszu klient zobowiązany jest tylko do uiszczania okresowych opłat wynikających wprost z wykorzystanej przestrzeni. Z jednej strony mamy tutaj do czynienia z rozwiązaniem lokalnym, znajdującym się pod pełną kontrolą klienta, zaś z drugiej korzystamy z niego jak z przestrzeni w chmurze* – tłumaczy Krzysztof Lorant.

Dysk czy taśma?

Jedną z kluczowych kwestii podczas projektowania cyfrowego archiwum jest dobór odpowiednich nośników. Producenci pamięci masowych podsuwają różne rozwiązania. Najbardziej radykalna jest koncepcja amerykańskiego startupu VAST Data. Jego platforma typu SDS (Software Defined Storage) bazuje na połączeniu pamięci SCM (Storage Class Memory) i QLC, czyli najtańszych nośników SSD. Architektura opracowana przez VAST Data powoduje, że można osiągnąć wysoką wydajność systemu all-flash w cenie zbliżonej do macierzy z dyskami mechanicznymi. Takie rozwiązanie pozwala uniknąć tworzenia kilku warstw w puli pamięci masowej.

Jednak, jak na razie, wciąż najpopularniejszym nośnikiem w cyfrowych archiwach są dyski twarde. Ich producenci nie składają broni, co najlepiej pokazują ostatnie premiery napędów WD oraz Seagate, zapewniających maks. pojemność odpowiednio 26 TB i 30 TB.

– *Jednym z ubiegłorocznych trendów jest renesans bibliotek taśmowych. Wynika to głównie z bezpieczeństwa jakie oferuje taśma, a także dyrektyw europejskich NIS2 oraz RCE* – zauważa Jakub Bala.

Do innych atrybutów taśm należą niskie koszty przechowywania danych i niewielkie zużycie energii elektrycznej,

> Dyrektywy europejskie sprzyjają renesansowi bibliotek taśmowych.

co jest atutem w czasach, kiedy wszyscy mówią o potrzebie zrównoważonego rozwoju. Co istotne, rozwój technologii taśmowych nie stoi w miejscu, co pokazują przykłady IBM-a, który w ubiegłym roku wprowadził na rynek nośnik o pojemności 150 TB po kompresji. Natomiast konkurencyjny format LTO-9 oferuje 45 TB skompresowanej pojemności.

Warto dodać, że w obecnych czasach nie postrzega się taśmy jako pojedynczego nośnika, lecz wdrażane są zautomatyzowane biblioteki przechowujące petabajty danych. Co nie zmienia faktu, iż ten rodzaj nośnika ma pewne mankamenty, takie jak zbyt wolny dostęp do danych, problemy z kompatybilnością wsteczną w przypadku formatu LTO, czy potrzeba zapewnienia klimatyzacji oraz trudności związane z eksploatacją w wilgotnym środowisku.

Nowym motywatorem prawo i sztuczna inteligencja

Firmy coraz bardziej przekonują się do elektronicznego obiegu dokumentów. Dla nieprzekonanych zaś skutecznym impulsem mogą być regulacje prawne.

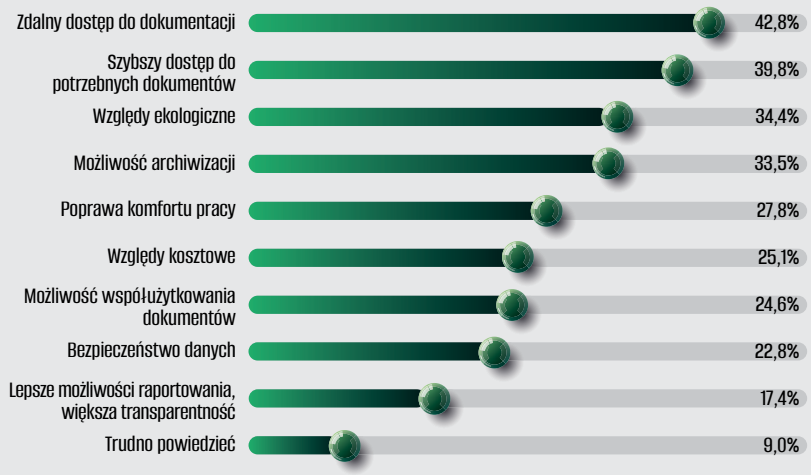
Andrzej Gontarz

Jednym ze skutków globalnych zawirowań związanych z pandemią w latach 2020–21 oraz koniecznością wprowadzenia pracy zdalnej było wzmożone, skokowe zainteresowanie wdrożeniami systemów elektronicznego obiegu dokumentów i zarządzania nimi. Jednak w kluczowych obszarach działania dużych podmiotów nastąpiło nasycenie nimi. Z kolei wiele małych firm nie dostrzegło realnych korzyści z ich wdrożenia lub nie dysponuje odpowiednim budżetem na ich zakup lub wynajem. Dlatego ubiegły rok nie obfitował już w tak silne bodźce do inwestowania w tego rodzaju oprogramowanie, jak w latach poprzednich.

Wdrażaniu lub rozwojowi systemów elektronicznego obiegu dokumentów może jednak obecnie sprzyjać rosnące zainteresowanie wykorzystaniem narzędzi bazujących na mechanizmach sztucznej inteligencji i nastawienie na automatyzację różnych obszarów działalności biznesowej. Przebadane przez EY firmy z całego świata, także z Polski, w najbliższych latach chcą inwestować głównie w: robotykę i automatykę, analitykę i sztuczną inteligencję oraz przetwarzanie brzegowe. Do poprawy warunków pracy zdalnej i optymalizacji procesów oraz systemów mają im też służyć sieci 5G, które znalazły się na piątym miejscu wśród deklarowanych priorytetów inwestycyjnych.

Według analiz IDC wydatkom na IT sprzyjać będą obecnie głównie inwestycje w automatyzację, platformy AI, oprogramowanie zabezpieczające i narzędzia programowe. Wśród najważniejszych czynników wzrostu znalazła się także postępująca migracja do chmury.

Największe przewagi elektronicznego obiegu dokumentów nad papierowym



Źródło: Webcon, 2023

Klucz do większej efektywności

Jak wynika z ubiegłorocznego raportu Quocirca, nawet te firmy, które wciąż w dużej mierze bazują na obiegu papierowym, zrozumiały, że digitalizacja jest kluczem do większej efektywności działania i odporności w obliczu możliwych zakłóceń funkcjonowania. Poza tym łatwość zestawiania i analizy dostępnych danych cyfrowych pozwala przedsiębiorstwom uzyskać lepszy, bardziej czytelny wgląd w swoje przewagi konkurencyjne i wykorzystywać je zgodnie z sytuacją na rynku.

Warto podkreślić, że 61 proc. uczestniczących w światowym badaniu osób odpowiedzialnych za inwestycje w IT przyznało się do przyspieszenia digitalizacji procesów bazujących na obiegu papierowym. Wśród głównych wskazanych motywacji do podjęcia działań w tym zakresie znalazła się możliwość poprawy efektywności kosztowej, jak też konieczność zapewnienia warunków do zrównoważonego rozwoju. Przedsiębiorcy szukają optymalnych rozwiązań w tym zakresie w odpowiedzi na wymagania wynikające z regulacji prawnych dotyczących sfery ESG (environmental, social and corporate governance) oraz w obliczu konieczności ścisłej kontroli kosztów w szybko zmieniającym się środowisku ekonomicznym.

Fot. Adobe Stock

Przyspieszenie sprzyjających osiąganiu tych celów inicjatyw w zakresie transformacji cyfrowej nie oznacza przy tym całkowitej rezygnacji z posługiwania się dokumentami papierowymi. Chodzi raczej o stworzenie jednolitego, cyfrowego systemu zarządzania posiadanymi zasobami. Warto też zauważyć, że 38 proc. respondentów Quocirca uważa, iż mimo przyspieszenia procesów digitalizacji wykorzystanie papieru w ich firmach się zwiększy.

Brak wiary w korzyści

Opublikowane w ubiegłym roku badanie firmy Webcon ujawniło, że w Polsce elektroniczny obieg dokumentów wykorzystuje w codziennej pracy ogółem 59 proc. przedsiębiorstw. Systemy EOD najbardziej popularne są w dużych podmiotach (82 proc.) oraz w średnich (76 proc.). Natomiast takim rozwiązaniem zainteresowanych jest tylko 29 proc. polskich mikroprzedsiębiorstw (tzn. zatrudniających do dziewięciu pracowników).

Wykorzystanie papierowych dokumentów rośnie, mimo postępującej cyfryzacji.

Branża z potencjałem

Postępuje cyfryzacja obsługi procesów administracyjnych w budownictwie. Z początkiem 2023 r. została uruchomiona oficjalna aplikacja c-KOB do elektronicznego prowadzenia książki obiektu budowlanego. W połowie roku oddano do użytku system EDB, czyli Elektroniczny Dziennik Budowy. Rozpoczęły się też prace nad Systemem Obsługi Postępowań Administracyjnych w Budownictwie.

W większości przypadków cyfryzacja nie obejmuje jednak całości przedsiębiorstwa – przeprowadzana jest raczej wyspowo. Jedynie 27 proc. polskich firm zdigitalizowało wszystkie obszary swojej aktywności biznesowej i korzysta z elektronicznego obiegu dokumentów do pełnej kontroli prowadzonych działań operacyjnych. Z kolei 16 proc. respondentów przyznało, że nadal używa wyłącznie poczty elektronicznej i dokumentacji papierowej do działań związanych z marketingiem i sprzedażą, zaś 11 proc. do procesów kadrowych, podczas gdy 7 proc. do zadań finansowych (np. akceptacji faktur).

Największą przeszkodą w digitalizacji, jak pokazuje raport Webconu, okazuje się być brak wiary kadry zarządzającej w to, że cyfrowe techniki poprawią efektywność operacyjną przedsiębiorstwa. Aż 54 proc. uczestników badania nie widzi potrzeby wdrożenia elektronicznego obiegu dokumentów. W sumie 28 proc. respondentów obawia się zbyt wysokich kosztów wdrożenia, a 17 proc. sądzi, że ich firma nie posiada odpowiednich zasobów IT, które pozwalałyby na implementację takich rozwiązań.

Z mocy prawa

Co zatem może stanowić w obecnych warunkach impuls do wzrostu zainteresowania wdrożeniami systemów elektronicznego zarządzania obiegiem dokumentów na polskim rynku? Z pewnością, jak zawsze, wiele będzie zależało od umiejętności edukowania potencjalnych klientów o faktycznych korzyściach biznesowych wynikających z zastosowania tego rodzaju oprogramowania. Oczywiście najlepiej, jeśli argumenty będą uwzględniały realia konkretnej firmy, a nie bazowały tylko na ogólnikach.

Z drugiej strony, zastosowaniu systemów EOD mogą pomóc rysujące się na horyzoncie wymagania związane z wejściem w życie przepisów dotyczących e-faktur i e-doręczeń. Integracja tych rozwiązań z systemami elektronicznego obiegu dokumentów w firmach wydaje się być najbardziej racjonalnym i efektywnym sposobem sprostania ustawowym wymogom. Może też skutkować uporządkowaniem procesów biznesowych bazujących na przepływach dokumentów poprzez ich automatyzację i uproszczenie zarządzania nimi.

Problem w tym, że do końca nie wiadomo od kiedy ostatecznie zaczną obowiązywać wspomniane przepisy. Ich wprowadzenie w życie jest co jakiś czas odkładane na późniejszy termin. Jeszcze pod koniec ubiegłego roku harmonogram wdrażania Krajowego Systemu e-Faktur ustalał obowiązek ich wystawiania przy użyciu KSeF na 1 lipca 2024 r. Jednak w styczniu br. minister finansów odłożył termin wdrożenia systemu na bliżej nieokreśloną przyszłość.

Termin wejścia w życie wymogów związanych z uruchomieniem usług elektronicznych doręczeń również był przekładany pod koniec ubiegłego roku. Tutaj, na dodatek, różne grupy użytkowników będą zobowiązane do zakładania skrzynek do e-doręczeń w różnym czasie. Jak wynika z informacji na stronie biznes.gov.pl, na przykład przedsiębiorcy zarejestrowani w CEIDG do końca 2024 r. będą do tego zobligowani do końca września 2026 r. Administracja publiczna zacznie posługiwać się e-doręczeniami od 1 października 2024 r.

Poza tym, od 1 stycznia 2026 r. wszystkie urzędy oraz podległe im jednostki będą zobowiązane do korzystania z systemu Elektronicznego Zarządzania Dokumentami oraz prowadzenia w nim wszystkich działań związanych z zarządzaniem dokumentacją. Będą mogły wdrożyć w tym celu oferowany im bezpłatnie system EZD PUW lub wybrać oprogramowanie dostępne na rynku.

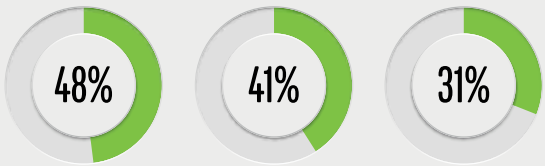
Rośnie zainteresowanie skanowaniem dokumentów

Na zlecenie firmy PFU (Ricoh), agencja badawcza Quocirca przeprowadziła badanie dotyczące digitalizacji dokumentów w kontekście cyfrowej transformacji, w którym udział wzięło ponad 500 europejskich przedsiębiorstw. 22 proc. z nich przyznało, że ma zdefiniowany cel dotyczący ograniczenia liczby papierowych dokumentów w realizowanych przez siebie procesach biznesowych. Tak niewielka liczba nie oznacza jednak, że zainteresowanie skanowaniem jest niewielkie – 68 proc. firm twierdzi, że ma fundusze na rozwój projektów digitalizacyjnych, zaś 77 proc. deklaruje, iż skanuje większość lub wszystkie trafiające do nich dokumenty.

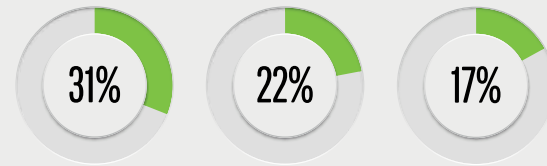
Na stronie firmy badawczej Quocirca dostępna jest pełna wersja raportu „Scanning as an enabler for digital transformation".

Jaki typ dokumentów przetwarzany jest w procesach biznesowych przedsiębiorstwa?

Wyłącznie cyfrowo

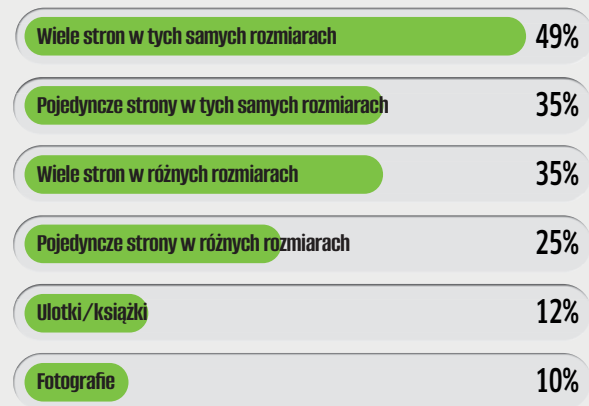


Wyłącznie na papierze

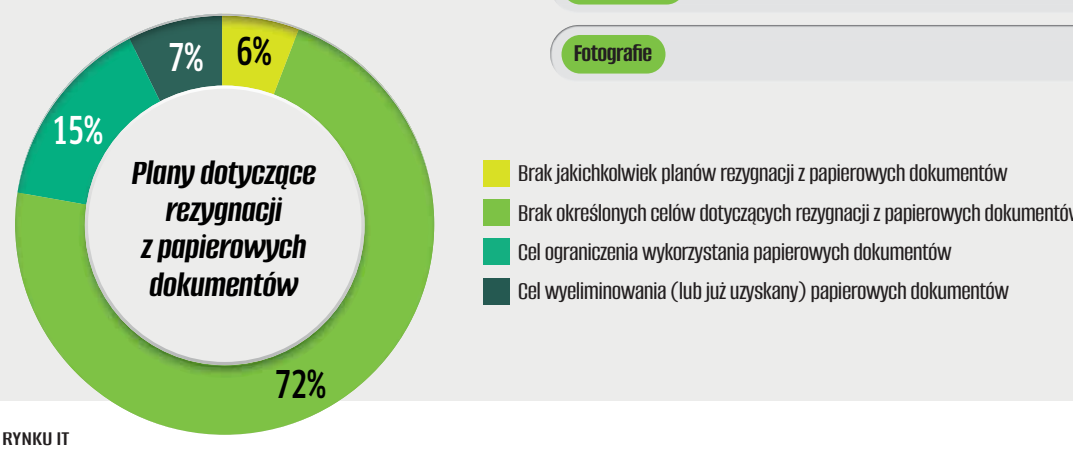


Jakie są główne przyczyny kontynuowania przetwarzania papierowych dokumentów?

Najczęściej skanowane obiekty



Plany dotyczące rezygnacji z papierowych dokumentów



Źródło: Raport „Scanning as an enabler for digital transformation", Quocirca, wrzesień 2022 r.

Zarządzanie informacją **dla małych i dużych**

ABBYY dysponuje bogatym portfolio produktów, dzięki którym resellerzy mogą zaspokajać potrzeby małych i średnich przedsiębiorstw w zakresie zarządzania dokumentami, zaś integratorzy wdrażać w większych korporacjach rozbudowane systemy obiegu informacji.

Zarządzanie danymi w firmach to wielowątkowe zagadnienie, w którym konieczne jest określenie procesów, jak i zapewnienie narzędzi umożliwiających ich realizację. Bogatą ofertę w tym zakresie ma ABBYY – lider rynku rozwiązań przetwarzania danych z dokumentów, którego od lat na polskim rynku reprezentuje AutoID Polska, generalny przedstawiciel producenta. Przedsiębiorstwom, organizacjom publicznym oraz instytucjom państwowym ABBYY oferuje wiele produktów do przetwarzania dokumentów. Od aplikacji desktopowych po narzędzia dla najbardziej wymagających podmiotów, które potrzebują zindywidualizowanych rozwiązań.

W wielu instytucjach przetwarzających dokumenty zastosowanie znajduje **FineReader PDF**. Z narzędzia tego mogą korzystać pojedynczy użytkownicy potrzebujący rozwiązania do rozpoznawania znaków (OCR) lub usprawnienia pracy z formatem PDF (tu sprawdzi się wersja Standard), jak też bardziej wymagające osoby potrzebujące funkcji porównywania dokumentów (również w różnych formatach) oraz automatycznego przetwarzania – to zapewnia wersja Corporate. FineReader PDF sprawdzi się także w rozbudowanych przedsiębiorstwach, w których liczba i różnorodność procesów jest na tyle duża, że zasadne staje się udostępnienie rozwiązania na zasadach zmienności (licencja określa maksymalną liczbę stanowisk, na których jednocześnie aktywne jest oprogramowanie, ale pozwala też na instalację go na ich dowolnej liczbie).

W ostatnim czasie dla użytkowników istotne stały się takie funkcje jak: edycja pliku PDF, możliwość przetworzenia w celu długoterminowego przechowywania, anonimizacja czy szyfrowanie, dlatego zostały udostępnione w obu wersjach oprogramowania FineReader PDF.

Inteligentne przetwarzanie na masową skalę

Dla przedsiębiorstw, które potrzebują automatyzacji rozpoznawania i przetwarzania większej liczby dokumentów o powtarzalnej strukturze, przeznaczone jest oprogramowanie **FineReader Server**. Istnieje możliwość zintegrowania tego rozwiązania z systemami zarządzania dokumentami jak DMS oraz innymi narzędziami stosowanymi w przedsiębiorstwie. Administrator może też wykorzystać to oprogramowanie do zarządzania innymi wybranymi procesami przetwarzania dokumentów.

Dla firm, w których przetwarzanie danych z dokumentów wiąże się z koniecznością zasilania nimi systemów zewnętrznych, a ich pobieranie powinno odbywać się w sposób selektywny, ABBYY oferuje rozwiązanie **Flexi Capture**. Służy ono do automatyzacji procesów związanych z gromadzeniem, klasyfikacją i ekstrakcją informacji z dokumentów. Zaś dzięki eliminacji ręcznych prac związanych z ich przetwarzaniem pozwala na zwiększenie wydajności pracowników.

Nowością w ofercie producenta jest **ABBYY Vantage**, czyli kompleksowe rozwiązanie do inteligentnego przetwarzania dokumentów, wykorzystujące sztuczną inteligencję i zaawansowane mechanizmy przetwarzania języka naturalnego. Służy przede wszystkim, ale nie tylko, do ekstrakcji danych, klasyfikacji dokumentów i rozpoznawania pól.

Kolejną grupą produktów udostępnianych przez dystrybutora ABBYY są narzędzia programistyczne – silniki **FineReader Engine**, na bazie których deweloperzy mogą tworzyć rozwiązania dopasowane do indywidualnych potrzeb i wymagań klientów. Zawierają one zestaw narzędzi programistycznych, dzięki którym możliwe jest zbudowanie rozwiązań np. dla kancelarii podatkowych, biur księgowych, w tym zautomatyzowanie procesu rozpoznawania i archiwizacji dokumentów przez maszyny MFP. Na bazie silników powstają również rozwiązania, które świetnie sprawdzają się w branży medycznej, dzięki czemu informacja o aktualnym stanie zdrowia pacjenta może być natychmiast dostępna tam, gdzie w danej chwili jest potrzebna.

ABBYY

AutoID

Dodatkowe informacje:
Jacek Wójcik,
dyrektor handlowy dystrybucji, AutoID Polska
dystrybucja@autoid.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMAMI ABBYY I AUTOID POLSKA.

Druk punktem wyjścia do cyfryzacji biznesu

Drukarki i skanery mogą stanowić dobry punkt wyjścia do rozwoju szerszej oferty usług z zakresu automatyzacji procesów i zarządzania informacją.

Andrzej Gontarz

Rozwój rynku urządzeń do druku i skanowania będzie w dużej mierze zależał od sytuacji na rynku pracy, a przede wszystkim od tego jak będą rozkładały się relacje między pracą zdalną, hybrydową i stacjonarną w biurze. Każdy z tych modeli wiąże się z innym zapotrzebowaniem na poszczególne rodzaje sprzętu i systemu wspomagającego obieg firmowych dokumentów.

Kwestia ewentualnego masowego powrotu pracowników do biur wciąż nie jest jednoznacznie rozstrzygnięta. Tym bardziej, że większość pracodawców deklaruje obecnie wybór modelu hybrydowego. Jak jednak zauważają specjaliści od HR, na zmiennym rynku pracy może jeszcze wiele się wydarzyć, i to w najbliższym czasie.

Według badania przeprowadzonego w połowie 2023 r. przez Resume Builder, 90 proc. firm dysponujących własnymi przestrzeniami biurowymi chce wrócić do modelu stacjonarnego do końca 2024 r. Z kolei 8 proc. pracodawców chciałoby powrotu wszystkich pracowników do biur w 2025 r. lub później. Jedynie 2 proc. badanych nie zamierza wymagać od swoich pracowników wykonywania obowiązków w modelu stacjonarnym.

Zdaniem ekspertów, nawet jeśli większość przedsiębiorstw wróci do pracy w biurach, to stała praca w siedzibie firmy będzie już nie do obrony. Wielu menedżerów otrzymuje od swoich pracowników, którzy w większości preferują pracę zdalną, głosy sprzeciwu przed powrotem do biur. Upodobali ją sobie szczególnie przedstawiciele pokolenia Z, które zaczyna odgrywać coraz bardziej znaczącą rolę na rynku zatrudnienia.

Duzi kupują więcej

Wzrost zainteresowania pracodawców przywróceniem pracowników do pracy w biurach dał się zauważyć na rynku IT już w ubiegłym roku. Widać to chociażby po strukturze sprzedaży urządzeń drukujących. Według danych Contextu już w pierwszej połowie 2023 r. spadła znacznie sprzedaż drukarek atramentowych kupowanych przez nabywców indywidualnych do użytku domowego. Wzrosła natomiast, w porównaniu z tym samym okresem 2022 r., sprzedaż urządzeń laserowych, głównie wielofunkcyjnych, kupowanych do wykorzystania w siedzibach firm.

Przedsiębiorcy postanowili uzupełnić po pandemii część wyposażenia biur i zaczęli wymieniać sprzęt na nowy, bardziej dostosowany do realiów pracy hybrydowej niż w pełni zdalnej czy stacjonarnej. Według IDC, do wzrostu zapotrzebowania na urządzenia drukujące i skanujące w ubiegłym roku przyczynili się głównie klienci korporacyjni. Ten trend będzie prawdopodobnie zauważalny również w roku bieżącym, gdyż w sektorze MSP nastąpiło w trakcie lockdownów nasycenie tym sprzętem i przedsiębiorcy będą powoli przymierzać się do jego wymiany w miarę zużycia.

Na co zwracają uwagę kupujący? Dla użytkowników domowych i przedsiębiorców prowadzących małe firmy najważniejszym kryterium przy wyborze urządzeń drukujących są niskie koszty eksploatacji, ważniejszym nawet nieco niż jakość wydruków. Duże firmy preferują z kolei wydajność i stabilność działania. Liczy się także cena zakupu urządzenia oraz doświadczenia z dotychczasowego użytkowania sprzętu danej marki.

Dla coraz większej grupy użytkowników ważne stają się też kwestie ekologiczne. Chodzi tu głównie o oszczędne zużycie energii, efektywne wykorzystanie tonerów, czy wykonanie niektórych części z materiałów uzyskanych

Konieczność zapewnienia cyberbezpieczeństwa stwarza okazję do poszerzenia oferty usług.

Fot. Adobe Stock

w procesie recyklingu. Przygotowując ofertę sprzedaży warto zatem obecnie brać pod uwagę ten aspekt.

Zdalnie, wygodnie, bezpiecznie

Potrzeba dostosowania sprzętu drukującego i skanującego do realiów pracy hybrydowej powoduje konieczność wyposażenia go w systemy bądź aplikacje umożliwiające zdalne administrowanie całym środowiskiem druku, jak i zarządzanie na odległość każdym urządzeniem z osobna. Producenci wyposażają wypuszczany na rynek sprzęt we własne oprogramowanie tego typu lub umożliwiają podłączenie swojej drukarki czy skanera do zewnętrznego, stosowanego już w firmie systemu.

Coraz większym atutem staje się też wyposażenie urządzeń drukująco-skanujących w mechanizmy wspomagające zarządzanie obiegiem dokumentów w firmie. Chodzi o to, by zeskanowany dokument mógł być poddany od razu obróbce OCR i odpowiednio zindeksowany trafiał automatycznie do właściwego katalogu w firmowych zasobach obsługiwanych przez stosowne systemy zarządzania treścią. W wielu przypadkach może to się odbywać już bez potrzeby podłączania urządzenia do zewnętrznego komputera. Jak zauważają specjaliści, w systemach wspomagających zarządzanie obiegiem dokumentów coraz większego znaczenia będą nabierać rozwiązania z elementami sztucznej inteligencji.

Ważnym aspektem decyzji zakupowych stają się kwestie cyberbezpieczeństwa. W firmach rośnie świadomość potencjalnych zagrożeń związanych ze stosowaniem urządzeń drukujących i skanujących, które coraz częściej stają się celem ataków hakerskich. W związku z tym klienci oczekują od dostawców rozwiązań, które wyposażone są w zaawansowane zabezpieczenia. Mogą to być mechanizmy kontroli dostępu do sprzętu drukującego bądź narzędzia do konfigurowania kont użytkowników. To stwarza firmom integratorskim okazję do oferowania nowych, dodatkowych usług konsultacyjnych i wdrożeniowych.

O nowych trendach w obszarze druku firmowego świadczy też obserwowany wzrost zainteresowania przenoszeniem systemów drukowania do chmury. Krok taki ma umożliwiać lepsze zarządzanie środowiskiem druku, łatwiejsze administrowanie poszczególnymi jego elementami i urządzeniami (np. zdalny monitoring materiałów eksploatacyjnych, zdalna aktualizacja firmware'u, dostęp do raportów z wykorzystania urządzeń itp.), jak również zwiększać bezpieczeństwo stosowanych rozwiązań. Dzięki chmurze ma być też zapewniony łatwiejszy dostęp do sprzętu dla użytkowników pracujących w modelu hybrydowym (żeby można było np. zlecić wydruk dokumentu na dowolnie wybranej drukarce bezpośrednio z konta poczty elektronicznej, czy ze smartfona). Rośnie przy tym zainteresowanie przenoszeniem systemów zarządzania drukiem do chmury.

Szansa na rozwój biznesu

Na wykorzystanie urządzeń drukujących w firmach trzeba dzisiaj już w dużej mierze patrzeć przez pryzmat postępujących procesów cyfryzacji. Chociaż digitalizacja zasobów przedsiębiorstwa nie wyprze całkowicie z użytku wydruków, to drukarki, skanery i urządzenia wielofunkcyjne trzeba traktować już jako elementy cyfrowego systemu zarządzania obiegiem dokumentów i informacji. Tam, gdzie takich systemów jeszcze nie ma, drukarki oraz skanery mogą stać dobrym punktem wyjścia do ich wdrożenia. Tym bardziej, że wielu producentów umożliwia wiele opcji zarządzania dokumentami bezpośrednio z urządzenia.

Dostawcy sprzętu drukująco-skanującego nie powinni zatem ograniczać swoich ofert tylko do samych urządzeń. Powinny być one obecnie bardziej kompleksowe, dotyczyć w dużej mierze usług zarządzania informacją i obiegiem dokumentów bez względu na ich formę – papierową czy elektroniczną. Druk długo jeszcze będzie funkcjonował równolegle z cyfrowym obiegiem dokumentów, ale procesy digitalizacji postępują i trzeba je brać pod uwagę przy planowaniu działań biznesowych. To bowiem może być szansa na rozwój nowych obszarów działalności oraz zdobycie nowych klientów.

MPS popularyzatorem cyfryzacji

Coraz większą popularność, także w Polsce, zyskują usługi zarządzania drukiem (MPS – Managed Print Services). Jak wynika z raportu Quocirca, ich dostawcy mogą wziąć na siebie proces digitalizacji w firmach, wykraczając poza same kwestie dotyczące druku (w wielu miejscach już tak się dzieje). Zdaniem analityków, 69 proc. przedsiębiorstw korzystających z MPS przyspiesza swoje plany cyfryzacji biznesu. W przypadku tych, które nie mają wdrożonego tego modelu, chęć jego implementacji deklaruje 40 proc. respondentów. Co ciekawe, 65 proc. osób decyzyjnych w zakresie IT przyznało, że ich dostawca usług zarządzania drukiem może w znacznym stopniu pomóc w automatyzacji wszystkich procesów biznesowych. Eksperci Quocirca wskazują cztery podstawowe kwestie niezbędne do odniesienia sukcesu w segmencie usług druku. Radzą oni takim podmiotom, żeby: myślały szeroko (zdefiniowały na nowo granice obszaru papierowego i cyfrowego); wybierały podejście „mniej papieru" zamiast „biuro bez papieru"; jasno, klarownie i odpowiedzialnie informowały o kwestiach zrównoważonego rozwoju; używały digitalizacji jako trampoliny do dostarczania szerszego wachlarza usług.

Zero Trust stymulatorem rynku

Brak zaufania wobec użytkowników infrastruktury IT staje się kluczową i docelową strategią zapewniającą ochronę przed wyciekami danych, do których może dochodzić w wyniku zewnętrznych ataków oraz incydentów wewnątrz firm.

Tomasz Janoś

Od 2020 r., gdy globalna pandemia sprawiła, że pracownicy zostali wysłani do pracy zdalnej, a transformacja cyfrowa przyspieszyła (co w dużej mierze polegało na wzroście wykorzystania chmury), specjaliści ds. bezpieczeństwa zostali zmuszeni do przemyślenia wdrożenia strategii Zero Trust. Wymaga ona weryfikacji i ochrony tożsamości każdego obiektu korzystającego z cyfrowych zasobów (użytkownika, sprzętu, oprogramowania), potwierdzania właściwego stanu zabezpieczeń urządzeń i aplikacji, egzekwowania zasady najmniejszych z możliwych uprawnień dostępu, a także zbierania i analizowania telemetrii w celu lepszego zabezpieczenia środowiska IT. Zgodnie z tym założeniem każde żądanie dostępu jest dokładnie weryfikowane.

Wobec stale ewoluującego i rosnącego zagrożenia model Zero Trust wprowadza kompleksowe, a jednocześnie dynamiczne podejście do ochrony, integrujące zaawansowane technologie, ścisłą kontrolę dostępu oraz ciągłą edukację użytkowników. Oznacza to bardziej proaktywną postawę wobec cyberzagrożeń, co ma na celu ochronę danych, reputacji, no i – rzecz jasna – pieniędzy.

Analitycy Gartnera prognozują, że do 2025 r. ponad 60 proc. przedsiębiorstw zrezygnuje z sieci VPN na rzecz dostępu opartego na Zero Trust, a więc wprowadzającego zasadę „nigdy nie ufać, zawsze weryfikować". Trend ten wynika z coraz większej świadomości, że w obliczu zaawansowanych cyberzagrożeń modele bezpieczeństwa bazujące na ochronie brzegu sieci nie są już wystarczające.

Kluczowym elementem architektury Zero Trust jednak zawsze pozostanie człowiek, dlatego firmy będą więcej inwestować w edukację pracowników w zakresie najlepszych praktyk cyberbezpieczeństwa. Regularne programy szkoleń oraz budowania świadomości będą odgrywać niezwykle istotną rolę w zapobieganiu atakom socjotechnicznym i zapewnianiu, że pracownicy rozumieją swoją rolę w utrzymaniu kultury bezpieczeństwa. Cybersecurity Ventures prognozuje, że globalne wydatki na szkolenia pracowników w tym zakresie wzrosną w ciągu najbliższych trzech lat do 10 mld dol. (1 mld dol. w 2014 r.).

Brak standardów i instrukcji wdrażania

Gdyby ktoś zapytał, czy istnieją certyfikaty i standardy Zero Trust, odpowiedź byłaby krótka: nie istnieją. Nie znaczy to jednak, że poruszać się trzeba po omacku. Na szczęście są wytyczne tworzone chociażby przez National Institute of Standards and Technology (NIST), organizację powstałą w 1901 r., która obecnie stanowi część Departamentu Handlu Stanów Zjednoczonych.

NIST tworzy standardy dla komunikacji, technologii i praktyk związanych z cyberbezpieczeństwem. I choć jeszcze nie przygotował standardów ani certyfikacji dla Zero Trust, to opracował tzw. publikację specjalną (Special Publication), która omawia cele tej architektury. Abstrakt dokumentu opisuje podejście w następujący sposób: „Zero Trust to termin określający ewoluujący zestaw paradygmatów z zakresu cyberbezpieczeństwa, które przenoszą obronę ze statycznych, opartych na sieci obwodów na użytkowników, sprzęt i zasoby".

Wobec tak zasadniczej zmiany paradygmatów praktycznie wszystkie implementacje Zero Trust będą procesem. W początkowej fazie firmy będą starać się utrzymywać pewną równowagę między podejściem polegającym na braku zaufania, a bezpieczeństwem skupionym na brzegu sieci, stopniowo wdrażając zmiany. Dlatego wprowadzenie kompletnej architektury Zero Trust i osiągnięcie celu mogą trwać lata, obejmując szereg cząstkowych projektów. Co więcej, tego celu nie będzie można nigdy nazwać ostatecznym, bo będzie on zakładał nieustanne wdrażanie i egzekwowanie kolejnych elementów strategii Zero Trust, uwzględniających przyszłe zmiany w biznesie i infrastrukturze.

MFA ma stać się w najbliższej przyszłości normą, a nie wyjątkiem.

MFA: ważny element Zero Trust

Wieloskładnikowe uwierzytelnianie (Multi-Factor Authentication, MFA) to

Fot. Adobe Stock

jeden z kluczowych elementów modelu Zero Trust, wprowadzający dodatkową warstwę ochrony poprzez wymaganie wielu form weryfikacji przed udzieleniem dostępu do zasobów. Ogranicza to ryzyko nieautoryzowanego dostępu nawet w przypadku kompromitacji jednego ze składników uwierzytelniania.

Wdrożenie MFA w architekturze Zero Trust wymaga podejścia strategicznego. Trzeba zacząć od zidentyfikowania danych, systemów i aplikacji wymagających zwiększonej ochrony i krok ten jest kluczowy w określeniu, gdzie powinno być zastosowane MFA. Jak wynika z badań Google'a, mechanizm ten może zapobiec aż 99 proc. ataków bazujących na masowym phishingu, a atakom wykorzystującym automatyczne boty aż w 100 proc. Ze względu na wyjątkową skuteczność w zapobieganiu nieautoryzowanemu dostępowi, MFA już należy do najczęściej wybieranych rozwiązań w dziedzinie cyberbezpieczeństwa i zdaniem rynkowych analityków w najbliższej przyszłości stanie się normą, a nie wyjątkiem.

Przedsiębiorstwa wprowadzające MFA będą w celu weryfikacji tożsamości korzystać także z bardziej zaawansowanych metod uwierzytelniania, takich jak biometria i analiza behawioralna. Wsparte przez MFA systemy zarządzania tożsamością (Identity and Access Management, IAM) staną się podstawą zarządzania dostępem do zasobów i gwarantowania, że dostęp do wrażliwych danych mogą uzyskać tylko uprawnione osoby.

Rynek IAM ma wzrosnąć z 12,3 mld dol. w 2020 r. do 24,1 mld w roku 2025, przy średnim rocznym tempie wzrostu wynoszącym 14,4 proc. (prognoza MarketsandMarkets). Taki niemal stuprocentowy wzrost jest wyrazem rosnącego znaczenia zaawansowanych rozwiązań IAM wykorzystywanych w architekturach Zero Trust.

Zdalna izolacja przeglądarki

Obok uwierzytelniania wieloskładnikowego bardzo skutecznym – choć jeszcze nie tak popularnym – zabezpieczeniem przed atakami i wyciekami danych, a także potencjalnym elementem wdrażanego podejścia Zero Trust jest mechanizm Remote Browser Isolation (RBI). Ponieważ przeglądarki internetowe pozostają głównym wektorem cyberataków, jest duża szansa, że RBI – uruchamiający przeglądarkę internetową w zdalnym, odizolowanym środowisku (zazwyczaj na serwerze lub w chmurze) – zostanie zaakceptowane jako sposób na wprowadzenie zasad Zero Trust bezpośrednio w punkcie dostępu do sieci. Po wdrożeniu RBI jakikolwiek złośliwy kod, z którym można się zetknąć podczas przeglądania stron WWW, pozostanie w tym izolowanym środowisku, nie docierając do urządzenia użytkownika i sieci korporacyjnej.

Przyjęcie RBI oznaczałoby proaktywny krok w kierunku zminimalizowania powierzchni ataków, zwłaszcza w przypadku przedsiębiorstw, które zatrudniają dużą liczbę osób pracujących zdalnie. Integrując izolację przeglądarek w ramach architektury Zero Trust, firmy mogą zabezpieczyć nie tylko swoje sieci, ale także zapewnić bezpieczną i bezproblemową obsługę użytkowników. Według analityków z Global Market Insights rynek RBI ma w latach 2020–2026 szansę na wzrost o ponad 40 proc.

W tym kontekście w najbliższej przyszłości będzie rosło także wykorzystanie uczenia maszynowego i sztucznej inteligencji, które mają wzmocnić ochronę przed atakami, a w przypadku wystąpienia incydentu i szkód umożliwiać szybsze odbudowanie infrastruktury i zasobów. Mechanizmy te pomogą w realizacji będących częścią wdrożenia Zero Trust procesów automatyzujących rutynowe zadania, takich jak przydzielanie zasobów, przeglądy dostępu i zarządzanie poświadczeniami. Wobec zalewu powiadomień o zagrożeniach i alertów, trafiających dzisiaj do centrum operacji bezpieczeństwa (SOC), automatyzacja stanie się w zarządzaniu środowiskiem cyfrowym czymś niezbędnym i kluczowym. Nie oznacza to jednak wyeliminowania z cyberbezpieczeństwa czynnika ludzkiego.

Trzy podstawowe zasady Zero Trust

- **Kompleksowa weryfikacja** – decyzje dotyczące bezpieczeństwa powinny być podejmowane z wykorzystaniem wszystkich dostępnych źródeł informacji, w tym tożsamości, lokalizacji, stanu urządzenia, zasobów, klasyfikacji danych i anomalii.
- **Najmniejsze z koniecznych uprawnienia dostępu** – dostęp jest przydzielany tylko wtedy, gdy jest konieczny (JIT - just-in-time), i jedynie na tyle, na ile jest potrzebny (JEA – just-enough-access), przy zastosowaniu reguł polityki bezpieczeństwa dostosowanych do poziomu ryzyka.
- **Wzmacnianie obrony przed atakiem** – minimalizacja obszaru ataku dzięki mikrosegmentacji, szyfrowaniu end-to-end, ciągłemu monitorowaniu oraz zautomatyzowanemu wykrywaniu zagrożenia i reagowaniu na nie.

Fudo Security: VPN już nie wystarcza

W dobie bardzo rygorystycznych przepisów wymuszających ochronę danych wrażliwych konieczne staje się m.in. ścisłe zarządzanie dostępem do nich w odniesieniu do użytkowników, ale też do osób z wyższymi uprawnieniami, np. administratorów.

Wyższy poziom bezpieczeństwa niż łącza VPN zapewniają rozwiązania do zarządzania dostępem uprzywilejowanym (Privileged Access Management, PAM). Fudo Security ma w ofercie dwa takie produkty: Fudo Enterprise oraz jego odmiana Fudo One o skalowalności dopasowanej do potrzeb małych i średnich firm oraz startupów. Zapewniają one użytkownikom bezpieczny dostęp do serwerów, baz danych, aplikacji internetowych i urządzeń sieciowych/OT. Narzędzia te działają zgodnie z regułami polityki Zero Trust, czyli umożliwiają łączenie się z aplikacjami i kontami tylko wtedy, gdy istnieje uzasadniony powód. Aktywność jest stale monitorowana, zaś w przypadku zaobserwowania podejrzanego zachowania sesja może być przerwana, a administrator poinformowany.

Do korzystania z rozwiązań Fudo Security nie jest wymagane instalowanie aplikacji agentów (nie potrzeba instalować środowiska bazodanowego oraz systemów operacyjnych). Do wykonania zdalnego połączenia można użyć natywnych klientów, jak terminale Unix, Putty czy Microsoft Remote Desktop Client, albo przeglądarki internetowej. Fudo umożliwia też skorzystanie ze standardu OpenID Connect i uruchomienie modułu jednokrotnego logowania firmy trzeciej (Single Sign On).

Rozwiązanie Fudo One obsługuje trzy protokoły (SSH, RDP i VNC), zaś Fudo Enterprise – aż 11 (w tym HTTPS, MySQL, TCP i Telnet). W wersji Enterprise wdrożono mechanizm optycznego rozpoznawania znaków (OCR) z nagranej sesji, co umożliwia identyfikowanie i indeksowanie tekstu oraz jego późniejsze przeglądanie i wyszukiwanie.

AI chroni przed zagrożeniami

Wyróżnikiem konkurencyjnym rozwiązania Fudo Enterprise jest wykorzystanie mechanizmów sztucznej inteligencji do analizy danych przesyłanych za pomocą protokołów SSH i RDP w celu wykrywania zagrożeń oraz nietypowego zachowania użytkowników. Dla sesji RDP przygotowano specjalizowane modele, w ramach których analizowany jest sposób korzystania z myszy i klawiatury (i porównywany z wcześniej zaobserwowanymi wzorcami), zaś dla sesji SSH dostępny jest model analizujący treść komend wprowadzanych z klawiatury.

W sytuacji, gdy dany moduł jest wybrany jako podstawa polityki, rozwiązanie Fudo Enterprise reaguje w zależności od oceny stopnia zagrożenia, na przykład poprzez wstrzymanie połączenia lub zablokowanie użytkownika. To funkcja szczególnie ważna dla placówek ochrony zdrowia i każdej firmy operującej na danych wrażliwych, posiadającej unikalne zasoby lub zarządzającej infrastrukturą krytyczną. Dzięki tej funkcji możliwe jest też spełnienie wymogów dyrektywy NIS2.

Fudo Enterprise zapewnia też możliwość analizy jakości pracy użytkowników i okresów ich bezczynności w określonym przedziale czasowym (Analizator Efektywności / Efficiency Analyzer). Mechanizm do tego wykorzystywany identyfikuje te sesje, które nie spełniają wymaganego poziomu aktywności, co pozwala na podejmowanie lepszych decyzji optymalizacyjnych. Jest to też świetne narzędzie do monitorowania i oceny pracy podwykonawców, kontraktorów oraz firm korzystających z outsourcingu zasobów i usług.

Informacje dla partnerów dostępne są na stronie www.fudosecurity.com/pl/zostan-partnerem. Bezpłatną konsultację z ekspertem można zamówić pod adresem www.fudosecurity.com.

Główne funkcje rozwiązań Fudo Security

1. Zarządzanie dostępem uprzywilejowanym – możliwość modyfikowania haseł dla wielu systemów, urządzeń i aplikacji oraz tworzenia własnych wtyczek modyfikujących hasła.

2. Ochrona przed celowymi lub niezamierzonymi nadużyciami dokonanymi przez użytkowników zdalnych.

3. Bezpieczny zdalny dostęp dla wszystkich użytkowników łączących się z firmową infrastrukturą IT.

4. Współpraca wielu administratorów podczas jednej sesji oraz przekazywanie sesji.

5. Alternatywa, ale też niezbędne uzupełnienie dla VPN – scentralizowany dostęp, monitorowanie sesji oraz zapobieganie naruszeniom.

6. Analiza powłamaniowa i identyfikacja obiektów lub osób naruszających procedury bezpieczeństwa dzięki funkcji nagrywania sesji (możliwe jest znakowanie czasem – asygnowanie sesji certyfikatem, co stanowi niepodważalność dowodu z sesji).

7. Wykorzystanie nagranych sesji w celach szkoleniowych.

Doradztwo i sprzedaż:
Katarzyna Zaorska,
Sales Director, Fudo Security
k.zaorska@fudosecurity.com

Współpraca partnerska:
Maciej Kotowicz
Channel Manager EMEA, Fudo Security
m.kotowicz@fudosecurity.com

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ FUDO SECURITY.

G DATA: szkolenia zamiast krytyki

Faktem jest, że użytkownicy stanowią najsłabsze ogniwo w systemie bezpieczeństwa IT, ale na ich usprawiedliwienie przemawia to, iż bardzo rzadko są szkoleni pod tym kątem we właściwy sposób. Wyzwanie polegające na zmianie tej sytuacji podjęła G DATA.

W ostatnich latach cyberprzestępcy rozpoczęli wykorzystywanie na masową skalę sztucznej inteligencji do generowania fałszywych treści, w tym manipulowania tekstami, obrazami i głosem. W szczególności wzrasta jakość phishingowych wiadomości e-mail, a wraz z nią ich skuteczność. Hakerzy szybko i łatwo przyswoili ChatGPT, a nawet opracowali nielegalne chatboty – WormGPT czy FraudGPT, przeznaczone między innymi do tworzenia wiadomości phishingowych. W rezultacie oszust pochodzący z zagranicy jest w stanie wygenerować tekst w języku polskim, bez błędów ortograficznych i gramatycznych.

Jakość mechanizmów sztucznej inteligencji stale rośnie, należy więc założyć, że znacząco wzrośnie liczba fałszerstw we wszystkich znanych formach. W nieodległej przyszłości zaś trudno będzie odróżnić e-maile phishingowe lub fałszywe obrazy od oryginałów. Zaobserwowano już ataki bazujące na oszustwach telefonicznych, w których przestępcy podszywali się pod członków rodziny lub służby medyczne, aby wyłudzić dane osobowe i finansowe. To oznacza, że do zdemaskowania takich manipulacji potrzeba będzie nie tylko więcej czasu, ale także większej wiedzy.

Tymczasem coraz częściej można zauważyć antagonizowanie pomiędzy działami IT i pracownikami firm. Popełnianie błędów przez tych drugich jest nagminnie krytykowane, ale faktem jest, że mało przedsiębiorstw choćby w niewielkim stopniu podejmuje w tym zakresie działania szkoleniowe. Nie jest to jednak jedyny powód, dla którego konieczne jest zwiększanie świadomości użytkowników. Wprowadzona przez UE nowa dyrektywa NIS2 wymaga podniesienia poziomu bezpieczeństwa IT w firmach, między innymi poprzez wprowadzenie programu szkoleń. W Polsce realizowany jest też program Cyberbezpieczny Samorząd, który spowodował wzrost popytu na szkolenia dla urzędników.

Teoria i praktyka

W reakcji na te wyzwania G DATA uruchomiła e-learningową platformę szkoleniową Security Awareness Training, z której mogą korzystać zarówno klienci, jak też partnerzy do rozbudowy portfolio swoich usług związanych z bezpieczeństwem. Jej celem jest nie tylko przekazywanie wiedzy technicznej, ale także promowanie świadomości bezpieczeństwa IT w zakresie aktualnych cyberzagrożeń i możliwych scenariuszy ataków. Przedstawiane są konkretne instrukcje działania i najlepsze praktyki, umożliwia ona także prowadzenie regularnych ćwiczeń i symulacji dotyczących bezpieczeństwa. Ponadto, kluczowym aspektem jest zachęcanie firm do wprowadzenia polityki dotyczącej zgłaszania błędów, w ramach której pracownicy będą mogli swobodnie raportować swoje obawy dotyczące bezpieczeństwa oraz podejrzane zachowania, nie obawiając się negatywnych konsekwencji.

Platforma zawiera kilkadziesiąt 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. Obsługa platformy jest zautomatyzowana i nie wymaga bieżącego zaangażowania ze strony administratorów. Szkolenia oraz warsztaty są dostępne przez cały czas trwania licencji (rok lub dwa lata), zaś ich uczestnikom wystawiane są certyfikaty.

Platforma Security Awareness Training cieszy się zainteresowaniem ze strony partnerów, ponieważ dzięki niej mogą rozszerzyć swoją ofertę, a także zaoferować szkolenia klientom, którzy dotychczas nie korzystali z oprogramowania G DATA. 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 na stronie gdata.pl/szkolenia.

Tematyka szkoleń

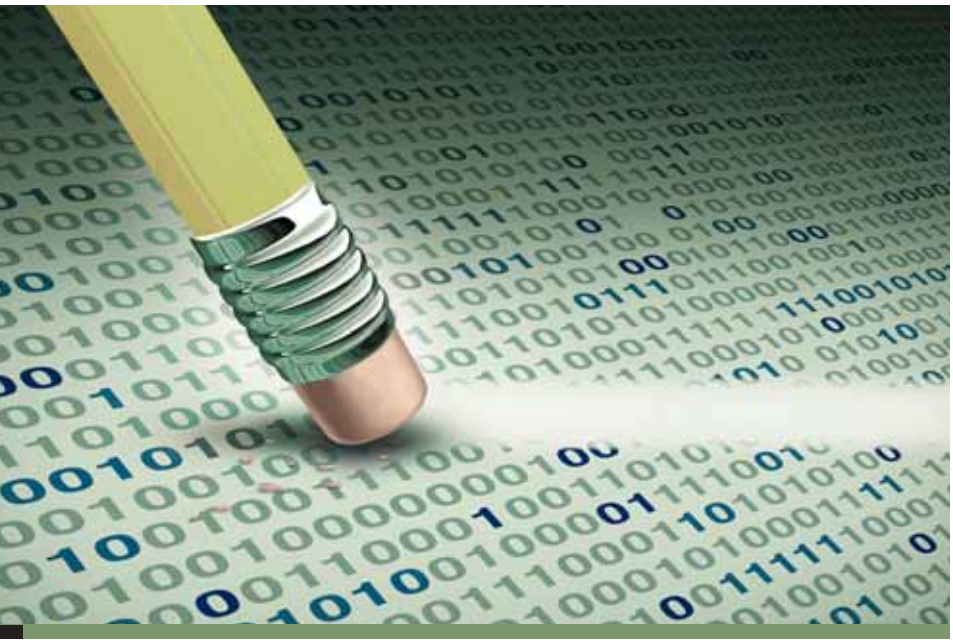
G DATA Security Awareness Training

- Bezpieczna praca poza biurem i w miejscach publicznych
- Zarządzanie ryzykiem i hasłami
- Phishing & malware – demaskowanie złośliwego oprogramowania i prób wyłudzenia danych
- Sposoby i przyczyny klasyfikacji informacji
- Media społecznościowe i praca w chmurze
- Incydenty zagrażające bezpieczeństwu i kontrola dostępu
- Socjotechnika
- Prawidłowe użytkowanie urządzeń mobilnych w pracy
- RODO i prywatność

Dodatkowe informacje:
Dział Handlowy G DATA Software,
tel. (94) 37-29-669 (pn-pt, 8.00-16.00)
sales@gdata.pl

ARTYKUŁ POWSTAŁ WE WSPÓŁPRACY Z FIRMĄ G DATA SOFTWARE.

Regulacje zagwarantują zyski



W ostatnich latach rynek rozwiązań do usuwania danych odnotował znaczny wzrost, co wynika z narastających obaw dotyczących ich prywatności, bezpieczeństwa oraz konieczności zachowania zgodności z przepisami.

Tomasz Janoś

IDC przewiduje, że tzw. datasfera, czyli zbiór wszystkich danych na świecie, urośnie do 221 zettabajtów w 2026 r., co oznacza roczny przyrost średnio o 21 proc. Ta trudna do wyobrażenia liczba (1 zettabajt to bilion gigabajtów) i obserwowane „tsunami danych" stanowi, po pierwsze, ogromne wyzwanie w obszarze przechowywania informacji, a po drugie generuje problem ze skutecznym ich usuwaniem. Zwłaszcza że nośniki danych trzeba zabezpieczyć podczas całego cyklu ich życia, a więc także na jego końcu. A gdy dane są wówczas „na dobre" kasowane, zachowanie zgodności z krajowymi i międzynarodowymi przepisami o ochronie danych oraz ich prywatności może wymagać przedstawienia certyfikowanych raportów o ich zniszczeniu – potwierdzających, że każdy nośnik pamięci został bezpiecznie wyczyszczony i jest wolny od podatności na ewentualne „pośmiertne" wycieki.

Bezpowrotne usuwanie danych to istotny, choć nierzadko zaniedbywany element bezpieczeństwa informacyjnego, którego celem jest ochrona wrażliwych danych przed dostaniem się w niepowołane ręce. Obecnie stosuje się kilka metod ich usuwania, z których każda ma swoje zalety i wady.

Jedną z tych powszechnie stosowanych jest fizyczne niszczenie, które obejmuje mechaniczne uszkodzenie nośnika, aby uczynić go nieczytelnym. Może to być osiągnięte poprzez kruszenie lub miażdżenie urządzeń. Metoda ta, choć skuteczna, może być czasochłonna i przez to nie nadawać się do masowego niszczenia danych. Inną powszechnie stosowaną metodą jest degaussing, który polega na wystawieniu nośnika na działanie silnego pole magnetycznego, aby wymazać przechowywane dane. Ta metoda jest szybka i efektywna w przypadku dysków i taśm, ale nie będzie skuteczna wobec powszechnie już stosowanych pamięci SSD.

Alternatywnym podejściem do fizycznego niszczenia danych są metody wykorzystujące do tego celu oprogramowanie. Specjalistyczna aplikacja wielokrotnie nadpisuje istniejące dane nic nieznaczącymi informacjami, co czyni oryginalne dane praktycznie niemożliwymi do odzyskania. Metody te mogą jednak nie być odpowiednie dla wszystkich rodzajów mediów oraz wymagają właściwej implementacji w celu zagwarantowania skutecznego usunięcia informacji. Są też czasochłonne, ale ich główną zaletą jest możliwość ponownego wykorzystania nośnika.

Nowe trendy

Jednym z nowych trendów jest wzrost popularności usług usuwania danych znajdujących się w chmurze. Trudno jednak wciąż wyrokować o ich skuteczności ze względu na brak możliwości weryfikacji tego aspektu – brak dostępu do danych nie oznacza, że operator nie dysponuje ich kopiami zapasowymi. Rośnie też wykorzystanie sztucznej inteligencji w procesach usuwania danych. Algorytmy oparte na AI mogą analizować duże ilości informacji i identyfikować potencjalne ryzyka bezpieczeństwa lub podatności, ułatwiając przedsiębiorstwom proaktywne zabezpieczanie swoich zasobów.

Innym obiecującym trendem, który być może zrewolucjonizuje podejście do niszczenia danych, jest usuwanie danych bazujące na technologii blockchain. W tym zdecentralizowanym i transparentnym procesie wykorzystywany jest niezmienny rejestr potwierdzający kiedy i w jaki sposób informacje zostały zniszczone.

Fot. Adobe Stock

Szansę na postęp dają także techniki szyfrowania, które mogą odgrywać istotną rolę w doskonaleniu metod usuwania danych. Bezpieczne wymazywanie przy użyciu zaawansowanego szyfrowania sprawia, że usunięte pliki są praktycznie niemożliwe do odzyskania.

Coraz istotniejsze staje się usuwanie danych, które ma być jednocześnie przyjazne dla środowiska. Ekologiczne metody, takie jak rozdrabnianie dysków twardych na materiały do recyklingu lub ich przeznaczanie do innych celów, pomagają zminimalizować ilość elektrośmieci przy jednoczesnym zapewnieniu gwarancji bezpieczeństwa informacji.

Usuwanie danych w serwerowniach

Na potrzebę zautomatyzowanego i audytowalnego sposobu usuwania danych zgromadzonych w firmowych serwerowniach wpływa kilka trendów. Składają się na nie wzrost ilości cyfrowych informacji w chmurze, konsolidacja centrów danych, potrzeba zapewnienia zrównoważonego rozwoju oraz przepisy regulujące bezpieczeństwo informacji. Usuwanie danych jest szczególnie istotne w kontekście ich ochrony przed wyciekami, gdy dane i aplikacje są migrowane lub w sytuacji, gdy sprzęt posiadany przez centrum danych zmienia właścicieli.

Profesjonalne oprogramowanie do usuwania danych spełnia wymagania dotyczące bezpieczeństwa centrów danych, automatyzując procesy usuwania dla różnych nośników danych i konfiguracji, zarówno w aktywnych, będących w użytku systemach, jak i takich, które już wycofano z użytku. Certyfikowane, zgodne ze wszystkimi najważniejszymi międzynarodowymi standardami usuwania oprogramowanie chroni wrażliwe dane klientów, umożliwiając jednocześnie zachowanie zgodności z przepisami dzięki dostarczaniu audytowalnych raportów z procesu usuwania. Bezpieczna i ekonomiczna technologia umożliwia zarówno wycofywanie sprzętu po zakończeniu jego okresu użytkowania, jak i jego ponowne wykorzystanie.

Rośnie znaczenie usług usuwania danych w chmurze.

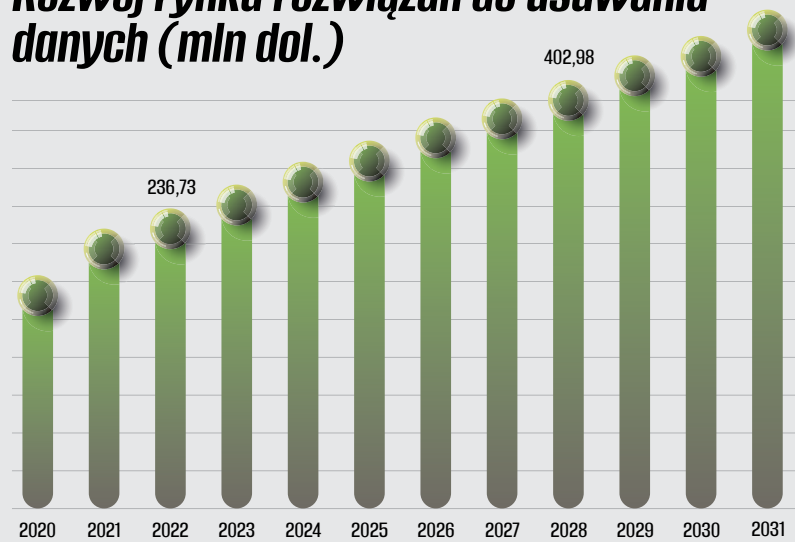
Usługi odzyskiwania danych

Chociaż praktyka posiadania kopii zapasowych ważnych danych na szczęście się już upowszechniła, stając się standardem, to wciąż nie brakuje klientów gotowych zapłacić za usługi odzyskiwania skasowanych i nadpisanych danych bądź takich, które znajdują się na uszkodzonych nośnikach. Dla tych, którzy chcieliby rozpocząć działalność w tej branży, kluczowe powinno być pozyskanie profesjonalnych narzędzi umożliwiających odzyskiwanie większej ilości danych w takich przypadkach, jak częściowo uszkodzone dyski, w tym nośniki ze „złymi sektorami".

Jeśli ktoś nastawi się na obsługę użytkowników domowych, musi się liczyć z najniższymi stawkami. Dane, które ci klienci chcą odzyskać, mają niską wartość, więc są oni gotowi zapłacić niewielką kwotę, zazwyczaj kilkaset złotych za proste usługi odzyskiwania danych. Z drugiej strony to w tej grupie klientów będzie najwięcej przypadków braku kopii zapasowej, więc także okazji do łatwiejszego zarobku.

Więcej można zarobić w przypadku małego biznesu. Ci klienci cenią swoje dane i są skłonni zapłacić więcej, zazwyczaj kilka tysięcy, za bardziej złożone usługi odzyskiwania danych. Z kolei specjalistyczne firmy odzyskiwania danych obsługują duże podmioty, których działalność bez odzyskanych danych mogłaby być poważnie zakłócona. Dlatego tacy klienci są gotowi płacić znaczne sumy za wysokiej jakości usługi odzyskiwania. Gdy chodzi o rozwój takiego specjalistycznego biznesu, strategią powinno być pozyskanie najnowocześniejszych narzędzi do odzyskiwania danych i zaawansowanej wiedzy, aby radzić sobie z najbardziej skomplikowanymi przypadkami. Warto zaznaczyć, że takie placówki chętnie współpracują z firmami partnerskimi, oferując im zarobek w postaci prowizji od zleconych przypadków odzyskania danych.

Rozwój rynku rozwiązań do usuwania danych (mln dol.)



Firma analityczna Business Research Insights opracowała raport podsumowujący globalny rynek rozwiązań do bezpiecznego usuwania danych oraz prognozy jego rozwoju. Wynika z niego, że w 2022 r. na świecie sprzedano tego typu usługi oraz umożliwiające je świadczenie sprzęt i oprogramowanie za 236,7 mln dol. W 2028 r. wartość tego rynku ma wynieść 403 mln dol., co oznacza średni roczny wzrost o 9,27 proc. Jako główną przyczynę rozwoju tego rynku analitycy wskazują rosnące obawy dotyczące prywatności danych, ich bezpieczeństwa i zgodności metod przechowywania z regulacjami, takimi jak RODO.

Prawo stwarza szansę dla integratorów

Przedsiębiorcy zgłaszają potrzebę i chęć współpracy z zewnętrznymi zaufanymi ekspertami, aby pokonać bariery i wdrożyć szyfrowanie w kluczowych dla swojego funkcjonowania obszarach.

Tomasz Janoś

Jak pokazują od lat różne badania, najpoważniejszym zagrożeniem dla wrażliwych danych są niezmiennie błędy popełniane przez pracowników. Dlatego jak najbardziej uzasadnione są te obawy firm, które dotyczą nieumyślnego wycieku wynikającego z pomyłek bądź zaniedbań personelu albo awarii systemów. Przeważają one znacząco nad obawami dotyczącymi złośliwych incydentów, za którymi stoją tymczasowi bądź kontraktowi pracownicy lub cyberprzestępcy.

Tworzone w latach 2021 i 2022 dla Entrust raporty Ponemon Institute stwierdzały, że decydenci w procesie wyboru wdrażanych rozwiązań do szyfrowania nie preferowali żadnych konkretnych rozwiązań. Niemniej większość badanych priorytetowo traktuje szyfrowanie danych w spoczynku (data-at-rest) i szyfrowanie w chmurze publicznej.

Największą przeszkodą stała się niemożność stwierdzenia, gdzie znajdują się wrażliwe dane.

Dobrą wiadomością jest to, że respondenci zwracają uwagę na przyszłościowe trendy w szyfrowaniu i przynajmniej częściowo rozpoczęli wdrażanie ochrony w takich obszarach, jak Internet Rzeczy. Dynamiczny rozwój IoT sprawia, że gromadzone są ogromne ilości danych. Często są one poufne, więc szyfrowanie staje się kluczowe. Gwarantuje ono, że dane pozostaną bezpieczne nawet podczas przenoszenia między różnymi urządzeniami i systemami IoT.

Tym, co może być uznane za nowy trend, który w kolejnych latach zapewne będzie narastać, jest migracja wrażliwych danych do chmury. Jak wynika z badania „Global Encryption Trends 2023" (autorstwa Encryption Consulting) w przypadku chmury firmy wybierają szyfrowanie pozostających tam danych w spoczynku w jednej z kilku opcji. Pierwsza zakłada szyfrowanie wykonane on-premise przed przesłaniem danych do chmury przy użyciu kluczy generowanych i zarządzanych przez ich administratorów. Druga to szyfrowanie w pełni powierzone dostawcom usług chmurowych, w ramach czego dostawcy wprowadzają silniejsze algorytmy szyfrowania, takie jak AES-256, aby zapewnić bezpieczeństwo danym (chronione są wtedy nie tylko dane w spoczynku, ale także podczas ich przesyłania). Ostatnim podejściem jest Bring Your Own Key (BYOK), czyli skonfigurowanie dzierżawy przy użyciu własnego klucza, zamiast stosowania klucza domyślnego wygenerowanego przez dostawcę chmury.

Obawa przed potężnymi karami

Jeśli chodzi o typ najchętniej szyfrowanych danych to niezmiennie w firmach i instytucjach dominuje ochrona danych osobowych. Stoi za tym obawa przed utratą reputacji w przypadku wycieku takich danych, ale także konieczność dostosowania się do przepisów i regulacji (w przypadku Unii Europejskiej to oczywiście RODO).

Firmy zdają sobie sprawę, że naruszenie tych regulacji w przypadku wycieku danych może skutkować bardzo poważnymi karami finansowymi. Dlatego zgodność z przepisami jest kluczowym motywem biznesowym dla wdrożenia szyfrowania, które jest jednym z fundamentalnych wymagań tego rodzaju regulacji (dotyczy zarówno danych w ruchu, jak i w spoczynku). Szyfrowanie jest jedną z metod spełniania takich przepisów, ponieważ może zapobiec nieautoryzowanemu dostępowi, ujawnianiu lub modyfikacji danych. W kontekście regulacji także samo szyfrowanie danych musi podlegać odpowiednim ramom prawnym, uwzględniając takie aspekty, jak lokalizacja danych, przesyłanie ich za granicę czy zarządzanie kluczami szyfrowania.

– *Z naszego wieloletniego doświadczenia wynika, że największy wzrost zainteresowania szyfrowaniem ma miejsce wtedy, gdy wchodzi w życie regulacja stanowiąca o konieczności stosowania adekwatnych do ryzyka środków technicznych. Poza tymi okresami zainteresowanie wyraźnie spada, a firmy wdrażające u siebie te mechanizmy powołują się na konieczność spełnienia regulacji. Niestety, firmy idą na skróty i rzadko kiedy dokonują rzetelnej analizy zagrożeń, najczęściej powołując się wprost na RODO. A przecież, jak czytamy w samym rozporządzeniu w art. 32 ust. 1, należy dobrać odpowiednie środki techniczne i organizacyjne właśnie na*

Fot. Adobe Stock

podstawie analizy ryzyka. Takie podejście jest w końcowym rozrachunku bardziej korzystne – mówi Dawid Zięcina, dyrektor działu technicznego w Dagmie.

Jak wynika z badania Entrust, własność intelektualna, dane pracownicze/HR oraz dokumenty finansowe to najpoważniejsi „kandydaci" do zaszyfrowania. Znacznie rzadziej wybieranym przez firmy rodzajem danych do zaszyfrowania są informacje związane ze zdrowiem i informacje niefinansowe, co może być zaskakującym wynikiem, biorąc pod uwagę wrażliwość informacji dotyczących zdrowia.

Bardziej optymistycznie przedstawia się badanie „Bezpieczeństwo IT w sektorze ochrony zdrowia", wykonane przez Biostat na zlecenie Fortinetu w lipcu 2022 r. Wskazywało ono, że decydenci w Polsce zdają sobie jednak sprawę z wagi zabezpieczania cyfrowych zasobów oraz konieczności dalszych inwestycji.

– *Najczęściej zgłaszaną potrzebą, bo przez co czwartą placówkę, było stworzenie środowiska i procedur gwarantujących ochronę danych przed utratą. Tylko 10 procent badanych nie miało planów dotyczących wdrażania kolejnych typów systemów zabezpieczania danych* – stwierdza Robert Dąbrowski, szef zespołu inżynierów w polskim oddziale Fortinetu.

Jak znaleźć dane do zaszyfrowania?

Największą przeszkodą w stworzeniu udanej strategii szyfrowania stała się niemożność odkrycia, gdzie znajdują się wrażliwe dane w firmie, a także ich klasyfikowanie. Kolejną barierą są ograniczenia budżetowe, a następną – trudności we wdrażaniu i zarządzaniu rozwiązaniem szyfrowania. W przypadku tej ostatniej bariery najbardziej wymagającą czynnością okazuje się zarządzanie kluczami. Jest ono bolesne dla wielu przedsiębiorstw ze względu na brak jasnego planu posiadania i przechowywania kluczy, a także brak wykwalifikowanego personelu.

Pewne cechy szyfrowania są uważane za bardziej krytyczne niż inne. Zgodnie z wynikami badania Entrust, do trzech najważniejszych atrybutów należą: wydajność systemu (i co za tym idzie wprowadzane przez szyfrowanie opóźnienia), zarządzanie kluczami, a także egzekwowanie polityki szyfrowania.

Jeśli chodzi o wydajność systemu i związane z tym opóźnienia, jasne jest, że czas potrzebny do zaszyfrowania danych rośnie wraz z ich ilością. W praktyce wiele baz danych to setki gigabajtów, a nawet terabajty. W rezultacie przerwy wymagane do zaszyfrowania uruchomionego obciążenia mogą być znaczne, potencjalnie trwając nawet kilka dni. Co ważne, również podczas okresowej operacji zmiany klucza, przerwa może trwać równie długo, jak przy początkowym szyfrowaniu. Warto zwrócić na to uwagę użytkowników.

Najpopularniejsze techniki szyfrowania

➤ **Szyfrowanie homomorficzne** (homomorphic encryption)
Pozwala na wykonywanie obliczeń na zaszyfrowanych danych bez ich wcześniejszego odszyfrowania. Oznacza to, że dane mogą być przetwarzane i analizowane w sposób bezpieczny i chroniący prywatność, bez ich narażania na potencjalne ryzyka i naruszenia. Nadaje się do zastosowania w chmurze obliczeniowej, w uczeniu maszynowym (ML) i analityce danych, gdzie dane mogą być przekazywane stronom trzecim bez narażania ich poufności czy integralności.

➤ **Szyfrowanie oparte na atrybutach** (attribute-based encryption)
Pozwala na szyfrowanie i deszyfrowanie danych na podstawie atrybutów użytkowników, a nie ich tożsamości czy kluczy. Może być wykorzystywane do kontroli dostępu, udostępniania danych i zarządzania nimi. Ułatwia też zwiększanie prywatności i bezpieczeństwa danych, ponieważ może ograniczać ekspozycję poufnych informacji oraz ryzyko ich wycieku.

➤ **Szyfrowanie o zerowej wiedzy** (zero-knowledge encryption)
Dane są szyfrowane w trybie end-to-end w taki sposób, że nawet dostawca usługi lub platforma zarządzająca danymi nie może uzyskać dostępu do tekstu jawnego. W systemie o zerowej wiedzy jedynie właściciel danych posiada klucze szyfrowania, co zapewnia wyższy poziom prywatności i bezpieczeństwa. Ten trend jest szczególnie istotny w branżach, gdzie poufne informacje muszą być chronione przed dostępem stron trzecich, takich jak opieka zdrowotna, finanse i usługi komunikacyjne.

➤ **Szyfrowanie kwantowe** (quantum encryption)
Wykorzystuje zasady fizyki kwantowej do generowania i dystrybucji kluczy kryptograficznych. Może zapewnić wyższy poziom bezpieczeństwa i prywatności niż konwencjonalne szyfrowanie, ponieważ wykrywa próby przechwycenia lub manipulowania kluczami i zapobiega im. Uważa się je za praktycznie nie do złamania, ponieważ każda próba podsłuchania klucza kwantowego zmienia jego stan, informując o tym strony zaangażowane w komunikację. To istotne między innymi w kontekście rozwoju komputerów kwantowych, które potencjalnie mogą łamać tradycyjne metody szyfrowania.

SASE to przyszłość łączności i bezpieczeństwa

Odpowiedzią na postępujące rozproszenie danych i aplikacji, znajdujących się obecnie nie tylko w firmowej serwerowni, ale także w różnych usługach chmurowych, jest połączenie sieci i aspektów dotyczących bezpieczeństwa w pakiet rozwiązań o wspólnej nazwie SASE.

Tomasz Janoś

Coraz więcej przedsiębiorstw używa zarówno infrastruktury lokalnej, jak i chmurowej, korzystając z rozwiązań SaaS, IaaS i PaaS. W sytuacji, gdy brzeg firmowej sieci ulega rozmyciu, a tradycyjne podejście do jego spójnej ochrony przestaje być skuteczne, konieczne staje się zastosowanie nowej architektury bezpieczeństwa. Takiej, która została zaprojektowana specjalnie dla środowiska wielochmurowego i która w dużej mierze na chmurze bazuje. Takim właśnie rodzajem architektury jest SASE (Secure Access Service Edge).

Stworzony przez analityków Gartnera termin SASE odwołuje się do pięciu kluczowych funkcji: sieci SD-WAN (Software-Defined WAN), bramy SGW (Secure Web Gateway), brokera CASB (Cloud Access Security Broker), zapory sieciowej nowej generacji (Next-Gen Firewall) oraz dostępu do zasobów w modelu ZTNA (Zero Trust Network Access). Wszystko to połączone razem daje, jak to zgrabnie ujmują specjaliści: „bazujący na zerowym zaufaniu dostęp, który wykorzystuje tożsamość urządzenia lub użytkownika w połączeniu z ustalanym w czasie rzeczywistym kontekstem oraz politykami bezpieczeństwa i zgodności". Krótko mówiąc, SASE ma zapewniać bezpieczny dostęp niezależnie od tego, czy pracownicy są w biurze, czy pracują zdalnie.

– *Firmy analityczne uwielbiają tworzyć nowe i chwytliwe akronimy, ale w tym przypadku nie można odmówić słuszności Gartnerowi, wskazującemu na różne nowe potrzeby przedsiębiorstw. Wszyscy stoimy przed koniecznością zapewnienia bezpieczeństwa w środowiskach hybrydowych, łączących zarówno systemy on-premise, jak i pochodzące często od wielu dostawców usługi chmurowe oraz aplikacje SaaS* – mówi Michał Jarski, Business Development and Sales Leadership w Forcepoint.

Zgodność na pierwszym miejscu

Zdaniem analityków Gartnera w kolejnych latach będziemy obserwowali przechodzenie przedsiębiorstw z sieci VPN (obsługiwanych za pomocą klasycznych routerów dostępowych i firewalli) na pakiety rozwiązań znacznie lepiej zabezpieczających środowiska wielochmurowe. Jak zwykle w przypadku bezpieczeństwa, na pierwszym miejscu wśród kluczowych czynników rozwoju rynku SASE jest konieczność uzyskania zgodności z regulacjami dotyczącymi ochrony wrażliwych danych (utrzymanie standardów RODO, PCI DSS czy HIPAA w środowisku wielochmurowym staje się jeszcze bardziej złożone). Wzrost stymulować będzie także rosnący popyt na rozwiązania zabezpieczeń bazujące na chmurze wśród mniejszych i średnich przedsiębiorstw oraz wysoki koszt samodzielnego zarządzania cyberbezpieczeństwem w firmach i związanym z tym ryzykiem.

Dell'Oro Group prognozuje duży wzrost sprzedaży SASE.

Wraz z popularyzacją pracy hybrydowej i coraz większym uzależnieniem od aplikacji chmurowych platformy SASE oferują firmom bezpieczniejsze i łatwiejsze w zarządzaniu rozwiązanie dostępowe. Pozwalają im zastąpić mało elastyczne wobec dzisiejszych potrzeb rozwiązania VPN systemami zdalnego dostępu opartymi na zasadach zerowego zaufania (Zero Trust), do których cyberprzestępcom dużo trudniej jest się włamać.

Dlatego nawet w niepewnych ekonomicznie czasach dostawcy rozwiązań ochronnych SASE wydają się należeć do tych firm z branży IT, które dzięki zestawowi nowych produktów potrafią skłonić klientów do sięgnięcia po portfele. W ostatnim roku wielu producentów wprowadziło nowe rozwiązania i funkcje SASE do swoich platform, co często polegało na integracji brakujących technologii zdobywanych drogą przejmowania mniejszych producentów. Pięciu największych dostawców SASE to obecnie: Zscaler, Cisco, Palo Alto Networks, Broadcom (Symantec) i Fortinet.

Fot. Adobe Stock

Przewidywane szybkie wzrosty

Według niedawno opublikowanego raportu Dell'Oro Group, rynek SASE czeka spory wzrost, który do 2028 r. wyniesie sprzedaż takich rozwiązań na poziom 16 mld dol. Oznacza to średnio 12-procentowy przyrost rocznie, a rozwój rynku napędzać będzie rosnące zapotrzebowanie na zintegrowane rozwiązania sieci i bezpieczeństwa, dostosowane do środowiska pracy hybrydowej.

– *Rynek SASE rośnie, ponieważ zmienia podejście przedsiębiorstw do architektury sieciowej i bezpieczeństwa. W miarę dostosowywania się firm do nowej normalności, czyli pracy hybrydowej oraz rozproszonych aplikacji, priorytetem staje się integrowanie sieci i zabezpieczeń w spójne rozwiązanie zorientowane na chmurę. SASE to nie tylko trend, to przyszłość łączności i bezpieczeństwa w firmach. Szybko porzucają one tradycyjne modele na rzecz efektywności, skalowalności i bezpieczeństwa zapewnianych przez SASE* – twierdzi Mauricio Sanchez, dyrektor ds. bezpieczeństwa i sieci w Dell'Oro Group.

Rynkowe trendy pokazują, że użytkownicy preferują SASE od jednego dostawcy. Wybieranie najlepszych rozwiązań danego rodzaju od różnych producentów i następnie ich integrowanie jest postrzegane za zbyt złożone zarówno we wdrażaniu, jak i późniejszym zarządzaniu. Pakiet już zintegrowanych rozwiązań od jednego dostawcy może ograniczać powierzchnię potencjalnego ataku i zmniejszać opóźnienia. Jeszcze większą zaletą może być skonsolidowane w jednej konsoli narzędzie zarządzania, co upraszcza administrowanie daną platformą.

W rezultacie rynek pakietów SASE nabywanych od jednego dostawcy ma rozwijać się dwa razy szybciej niż pakietów SASE złożonych z rozwiązań od różnych producentów (średnio 17 proc. rocznie w porównaniu z 9 proc. we wspomnianej już prognozie Dell'Oro Group). Zgodnie z tym trendem wielu większych producentów specjalizujących się w sieciach i cyberbezpieczeństwie przejmuje mniejsze firmy i startupy, aby uzupełnić swoje platformy SASE o brakujące elementy SD-WAN czy SSE (Security Service Edge).

Nowe modele dostarczania i wyceniania SASE

Dalszy rozwój SASE, napędzany pracą zdalną, migracjami do chmury i przetwarzaniem brzegowym, będzie w tym roku postępować w stosunkowo szybkim tempie. To efekt modelu Zero Trust i takiego zapobiegania atakom, które stanie się de facto schematem w przypadku bezpieczeństwa każdego nowego „brzegu" firmowej sieci. Co więcej, szerszy dostęp do zintegrowanych usług SASE umożliwią uproszczone modele ich dostarczania i wyceniania.

O ile bowiem wczesne usługi SASE obejmowały złożone modele z indywidualną wyceną, o tyle teraz usługi się standaryzują. Powszechne staną się subskrypcje bazujące na liczbie stanowisk lub zużyciu przepustowości sieciowej. Przyjęcie SASE powinno ponadto przyspieszyć fakturowanie oparte na konsumpcji. Dostawcy usług zarządzanych (MSP) będą również oferować platformy tego typu i pakiety dostosowane do potrzeb małych i średnich przedsiębiorstw. Ujednolicona oferta SASE dostępna za pośrednictwem jednego pulpitu nawigacyjnego będzie przyciągać firmy, które nie mają własnych specjalistów ds. bezpieczeństwa.

SASE jako usługa

Integracja sieci i bezpieczeństwa umożliwia globalne stosowanie spójnych reguł polityki, a chmurowa architektura SASE pozwala na tworzenie usług sieciowych i bezpieczeństwa dla rozproszonych po świecie czy kraju lokalizacji z jednego miejsca. Dostarczanie SASE w formie usługi chmurowej zapewnia większą skalowalność, elastyczność i wydajność. Dla użytkowników oznacza też brak konieczności inwestycji kapitałowych. Firma może subskrybować bazujące na chmurze usługi SASE i natychmiast rozpocząć korzystanie z nich. Wydatki kapitałowe zamieniają się przy tym w łatwiejsze do zarządzania koszty operacyjne.

Tego typu usługowe platformy SASE zwykle zapewniają takie elementy jak bezpieczna brama internetowa (SWG – Secure Web Gateway) do kontroli ruchu, inspekcji treści i filtrowania URL, co chroni przed phishingiem, ransomware'em i innymi zagrożeniami. Kolejną zaletą jest chmurowa zapora sieciowa jako usługa (FWaaS – Firewall as a Service), która chroni infrastrukturę w środowiskach on-premise oraz Software as a Service. Ważnym elementem jest broker bezpiecznego dostępu do chmury (CASB – Cloud Access Security Broker), chroniący przed wyciekiem danych, występowaniem zjawiska shadow IT oraz nieautoryzowanym dostępem do zasobów. Natomiast dodatkowy mechanizm bezpieczeństwa DNS ogranicza dostęp do złośliwych domen.

Indeks firm

CRN
VADEMECUM RYNKU IT

DODATEK SPECJALNY DO MIESIĘCZNIKA
CRN POLSKA
www.CRN.pl

marzec 2024
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.

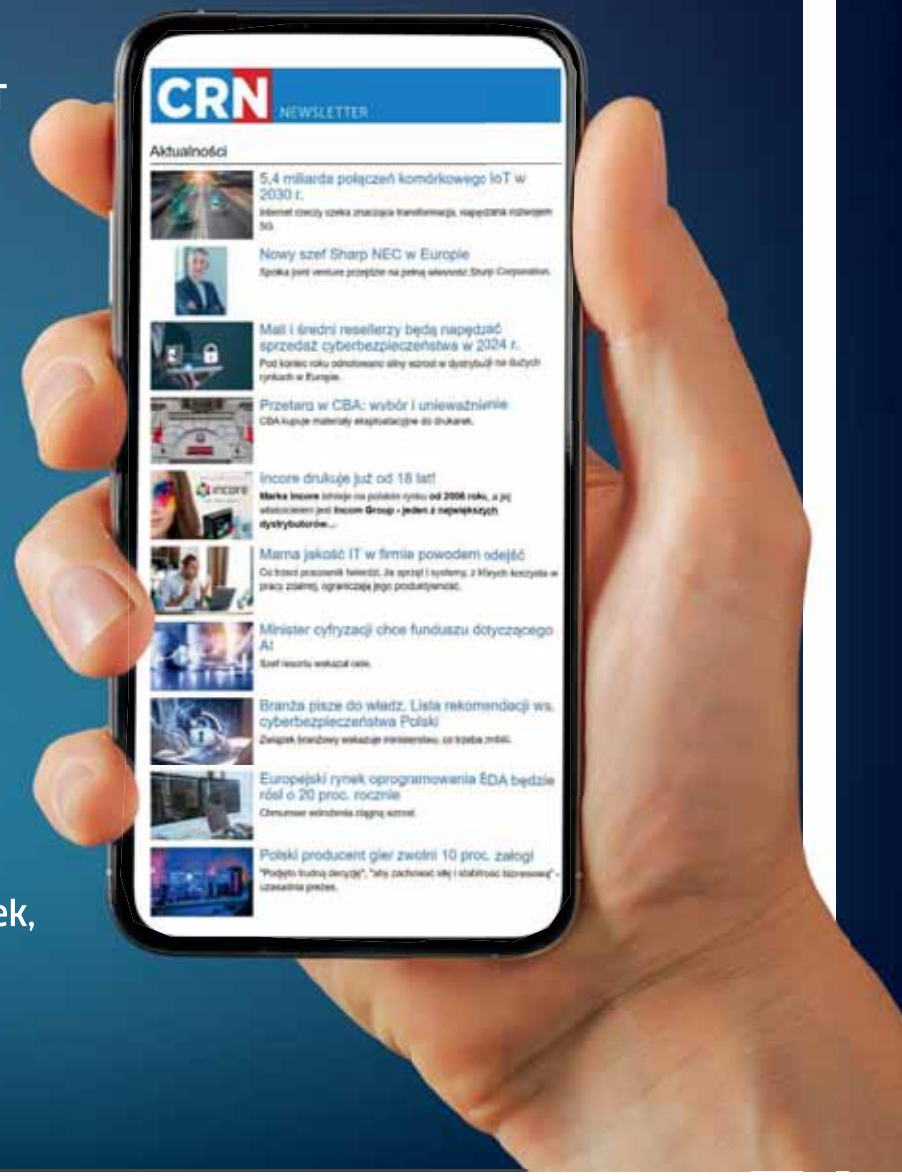
Nie przegap informacji ważnych dla Twojego biznesu!

Chcesz być na bieżąco z tym co najważniejsze w branży IT w Polsce i nie tylko?

Możesz dostawać trzy razy w tygodniu newsletter CRN, z którego szybko dowiesz się o ważnych wydarzeniach i nowościach z ostatnich 48 godzin.

- **wejścia na rynek,**
- **fuzje i przejęcia,**
- **kluczowe newsy z branży,**
- **zmiany personalne,**
- **skróty najważniejszych raportów**

– to wszystko trafi do Ciebie mejlem, w każdy poniedziałek, środę i piątek.



Masz konto na CRN.pl?

Włącz wysyłkę newslettera CRN na stronie **CRN.pl/prenumerata** (wymagane wcześniejsze zalogowanie na CRN.pl/logowanie).

Nie masz jeszcze konta na CRN.pl?

Załóż je na stronie **CRN.pl/rejestracja**

QNAP®

WORLD BACKUP DAY
MARCH 31ST

Kompleksowe rozwiązanie do backupu

multiplatformowe bezpieczne darmowe

Hyper Data Protector 2.0
zabezpiecz maszyny wirtualne w VMware, Microsoft Hyper-V oraz maszyny fizyczne z Microsoft Windows 10 i 11 oraz Server 2016, 2019 i 2022.

Boxafe 2.0
Wykonaj backup całej zawartości środowiska Microsoft 365 oraz Google Workspace.

Hybrid Backup Sync 3
Wyślij kopie danych i backupów z NAS do innej lokalizacji lub do chmury myQNAPcloud storage.

myQNAPcloud storage
Bezpieczna przestrzeń w chmurze QNAP. Wybierz preferowaną lokalizację oraz wymaganą przestrzeń. Bez ukrytych opłat!

QNAP SYSTEMS, INC.

www.qnap.com

O szczegóły zapytaj dystrybutorów QNAP: