BUSINESS INSIDER

RAPORT

Zarządzaj ryzykiem, nie kryzysem.

Przewodnik po skutecznym cyberbezpieczeństwie dla firm

We współpracy komercyjnej:

PZU

Cyberbezpieczeństwo 2024

SPIS TREŚCI

Kliknij w tytuł, aby przejść do danej sekcji

BUSINESS INSIDER

W dobiegającym końca, burzliwym 2024 r. sektor cyberbezpieczeństwa odnotował jedne z najbardziej dotkliwych naruszeń danych w historii.

Skala ataków oraz ich konsekwencje przeszły oczekiwania ekspertów. Liczba skradzionych rekordów przekroczyła miliard.

Spektakularnym przykładem są naruszenia danych AT&T, która w 2024 r. doświadczyła dwóch poważnych ataków. W lipcu wykradziono dane dotyczące połączeń i numerów telefonów niemal wszystkich klientów amerykańskiego operatora. Choć nie obejmowały one treści rozmów, mogą stanowić zagrożenie dla osób narażonych, jak ofiary przemocy domowej. W marcu z kolei wyciekły jeszcze dane 73 mln klientów AT&T, w tym hasła, które były zaszyfrowane, lecz łatwe do odkodowania.

Jeszcze poważniejszy atak dotknął platformę Change Healthcare, gdzie skradziono dane medyczne i rozliczeniowe dużej części populacji USA. Konsekwencje mogą być nieodwracalne, a poszkodowani odczuwać je będą przez lata.

Nie tylko sektor zdrowotny w USA padł ofiarą hakerów. W czerwcu brytyjskie laboratorium Synnovis padło ofiarą cyberataku, który doprowadził do odwołania tysięcy operacji. Dane 300 mln pacjentów zostały skradzione i częściowo opublikowane.

Innym przykładem może być Snowflake, który został zaatakowany całą serią włamań do systemu, i w efekcie dane setek milionów klientów, w tym Ticketmaster i Neiman Marcus, wyciekły. Skutki dopiero zaczynają wychodzić na jaw.

Te i wiele innych przypadków sytuacji krytycznych pokazują, jak fundamentalnym wyzwaniem jest dziś bezpieczeństwo danych. Naruszenia narażają firmy na straty finansowe i wizerunkowe oraz wpływają na prywatność poszkodowanych. Bez wątpienia każda firma powinna priorytetowo traktować cyberbezpieczeństwo, inwestując adekwatne do skali biznesu środki w technologie ochrony i szkolenia pracowników. Tylko tak uzbrojeni możemy stanąć do cyfrowej walki.

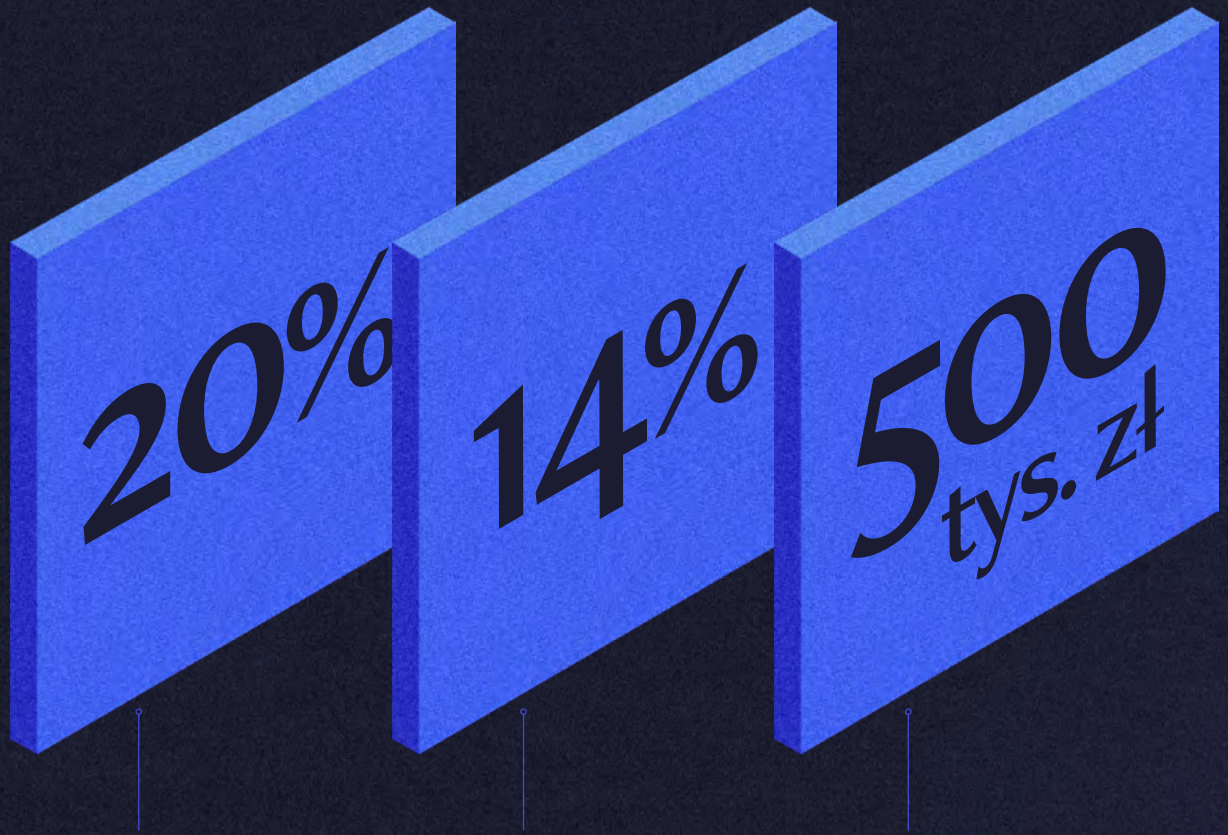
Mikołaj Kunica,
redaktor naczelny
Business Insider

1

Znaczenie cyberbezpieczeństwa dla biznesu

PZU

BUSINESS INSIDER



Już co piąta firma w Polsce padła ofiarą ataku ransomware, a niemal 40 proc. z nich zdecydowało się na zapłacenie okupu, by nie stracić danych.

Tylko 14 proc. firm, które zdecydowały się na zapłacenie okupu, odzyskało wszystkie dane po ataku ransomware. 56 proc. organizacji odzyskało dostęp do maksymalnie połowy danych, a 6 proc. ofiar po przelaniu pieniędzy do cyberprzestępców i tak straciło wszystkie dane.

Tyle wynosi strata spowodowana atakiem ransomware w co trzeciej firmie w Polsce w 2023 r. Z kolei w 8 proc. przypadków to aż ponad 5 mln zł.

Źródło: Badanie „Ransomware w Polsce 2024” firmy Sophos

Sektory krytyczne, takie jak transport, energetyka, zdrowie i finanse, stają się w swojej podstawowej działalności coraz bardziej zależne od technologii cyfrowych. Cyfryzacja stwarza duże możliwości i pomaga rozwiązać wiele problemów, przed którymi staje Europa, ale wystawia też gospodarkę i społeczeństwo na cyberzagrożenia.

Cyberataki i cyberprzestępczość stają się w całej Europie coraz częstsze i bardziej wyrafinowane. Tendencja ta będzie się w przyszłości nasilać. Według prognoz Unii Europejskiej, w 2025 r. aż 41 mld urządzeń na całym świecie będzie podłączonych do Internetu rzeczy.

Zdecydowane działania na rzecz cyberbezpieczeństwa, budujące otwartą i bezpieczną cyberprzestrzeń, mogą zwiększyć wiarygodność narzędzi i usług cyfrowych.

Znaczenie cyberbezpieczeństwa dla biznesu

Każda organizacja staje dziś przed poważnym wyzwaniem ochrony swoich zasobów. Zaledwie kilka minut nieaktualnego oprogramowania czy luki w zabezpieczeniach mogą doprowadzić do nieodwracalnych szkód — od utraty danych po finansową katastrofę. Cyberprzestępczość przestaje być problemem tylko dla dużych firm i staje się codzienną rzeczywistością także dla mniejszych graczy. W miarę jak technologia rozwija się w zawrotnym tempie, tak samo wzrastają umiejętności i możliwości hakerów, co wymaga od organizacji nieustannego podnoszenia standardów cyberbezpieczeństwa.

Obecnie nowe cyberzagrożenia pojawiają się co godzinę, każdego dnia. Połączenie z internetem otwiera możliwość ataku hakera na każdą organizację. Cyberprzestępczość staje się dużym biznesem, a zagrożenia stanowią przedmiot zainteresowania organizacji i rządów na całym świecie. Ryzyko utraty reputacji i pieniędzy jest bardzo wysokie, jeśli organizacje nie mają odpowiedniego planu bezpieczeństwa.

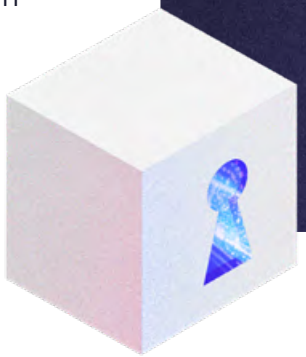
Z raportu Hiscox Cyber Readiness z 2023 r. wynika, że cyberataki nieprzerwanie rosną od czterech kolejnych lat i nic nie wskazuje, aby w tym i kolejnych latach miało być inaczej. Zauważalny jest też wzrost ataków na mniejsze firmy, sięgający nawet 36 proc. Z kolei według Statista sektor produkcyjny doświadczył największego udziału cyberataków w porównaniu z innymi branżami w ostatnich latach, a tuż za nim znalazły się finanse i ubezpieczenia. Ostatnie przypadki dotyczyły kradzieży poufnych informacji, co spowodowało znaczne straty finansowe dla dotkniętych nimi firm.

— Rozwój technologii sprawia, że liczba ataków i ich poziom skomplikowania rosną, co widać szczególnie w atakach na infrastrukturę krytyczną. Może to prowadzić do katastrofalnych społecznie skutków — mówi Tomasz Żelski, dyrektor zarządzający ds. IT i digitalizacji w Grupie PZU. — Musimy zwrócić też uwagę na udział AI w atakach. Sztuczna Inteligencja umożliwia większą precyzję i skalę działań. Organizacje często nie nadążają z aktualizacją i patchowaniem systemów, co pozwala cyberprzestępcom na wykorzystanie luk, zwłaszcza w kontekście nowych technologii, np. Internetu rzeczy.

Ważną kwestią jest też zarządzanie tożsamością i dostępem do danych. Staje się on coraz trudniejszy ze względu na rosnący poziom złożoności rozwiązań IT wykorzystujących równocześnie chmurę prywatną i chmury publiczne, ze względu na możliwość nieautoryzowanego dostępu — dodaje.

Cyberbezpieczeństwo nigdy nie było ważniejsze

Istnieje kilka podstawowych sposobów, w jaki kwestie cyberbezpieczeństwa mogą wpłynąć na organizację i jej reputację. Po pierwsze jest ryzyko, że haker może uzyskać poufne informacje, takie jak dane konta bankowego lub karty kredytowej. W sieci znajdziemy otwarte rynki dla takich informacji w tzw. dark webie. Jeśli inni uzyskają dostęp do takich poufnych informacji, organizacja może odkryć, że jej usługi bankowe lub karty kredytowe zostały wycofane lub naruszone zostały przepisy o ochronie prywatności. Każdego miesiąca na całym świecie zgłaszane są głośne naruszenia bezpieczeństwa wpływające na dane osobowe.



Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to upewnienie się, że dane twojej organizacji są bezpieczne przed atakami zarówno osób działających z wewnątrz, jak i zewnątrz. Może obejmować zbiór technologii, procesów, struktur i praktyk stosowanych w celu ochrony sieci, komputerów, programów i danych przed nieautoryzowanym dostępem lub uszkodzeniem. Celem każdej strategii cyberbezpieczeństwa jest zapewnienie poufności, integralności danych i dostępności.

Popularne cyberzagrożenia

Phishing – ataki polegające na podszywaniu się pod zaufane instytucje w celu wyłudzenia poufnych danych, takich jak hasła czy informacje finansowe.

Ransomware – złośliwe oprogramowanie, które szyfruje dane ofiary, żądając okupu za ich odblokowanie.

Malware – ogólna nazwa dla różnego rodzaju złośliwego oprogramowania, które niszczy, kradnie lub zakłóca działanie systemów komputerowych.

DDoS (Distributed Denial of Service) – ataki polegające na przeciążeniu serwera ogromną liczbą zapytań, co prowadzi do jego niedostępności.

Man-in-the-Middle (MitM) – atak, w którym cyberprzestępca przechwytuje komunikację między dwoma stronami, aby uzyskać poufne informacje.

SQL Injection – atak polegający na wstrzyknięciu złośliwego kodu SQL do aplikacji, w celu uzyskania dostępu do bazy danych.

Zero-day Exploits – wykorzystywanie niewykrytych wcześniej luk w oprogramowaniu przed tym, jak zostaną naprawione przez producenta.

Brute Force Attack – próba uzyskania dostępu do konta poprzez automatyczne, wielokrotne próby odgadnięcia hasła.

Spyware – oprogramowanie szpiegujące, które gromadzi dane użytkownika bez jego wiedzy i zgody.

Adware – złośliwe oprogramowanie wyświetlające niechciane reklamy, które mogą prowadzić do instalacji innych szkodliwych aplikacji.

Najbardziej alarmującym aspektem cyberbezpieczeństwa, który powoduje znaczne problemy dla organizacji, jest ransomware.

Drugim, ale powiązanym problemem jest to, że gdy haker uzyska poufne informacje o organizacji, może to doprowadzić do zrujnowania jej reputacji. Niewiele organizacji jest natomiast w stanie przetrwać szkody dla swojej reputacji, jakie mogą spowodować utracone poufne dane — zwłaszcza gdy chodzi o firmy z sektora MŚP. Szkody dla reputacji mogą być bardziej paraliżujące niż sama utrata danych.

Najbardziej alarmującym aspektem cyberbezpieczeństwa, który powoduje znaczne problemy dla organizacji, jest ransomware. W wielu przypadkach fragment złośliwego oprogramowania jest ukrywany i osadzony w innym typie dokumentu, czekając tylko na działanie ze strony użytkownika docelowego. Po uruchomieniu danego programu czy pliku złośliwe oprogramowanie może zaszyfrować dane organizacji tajnym, nawet 2048-bitowym kluczem szyfrującym lub komunikować się z centralnym serwerem poleceń i kontroli, aby oczekiwać na instrukcje wykonywane przez cyberprzestępcę. Po zainfekowaniu dane organizacji pozostają niedostępne. Gdy wszystkie dostępne dane zostaną zaszyfrowane — w tym w wielu przypadkach dane i systemy kopii zapasowej — organizacja otrzyma instrukcje dotyczące sposobu zapłaty okupu w ciągu kilku dni. W przeciwnym razie atakujący usunie klucz szyfrowania, a dane zostaną utracone. Cyberprzestępcą przetrzymuje więc dane dla okupu. Klucz szyfrowania jest wystarczająco silny, aby złamanie klucza zamiast zapłacenia okupu było nieopłacalne — niektórzy szacują, że przeciętny komputer stacjonarny potrzebowałby pięciu kwadrylionów lat, aby odszyfrować dane bez dostępu do klucza.

Ważna edukacja personelu

Organizacje mogą wprowadzać odpowiednie zabezpieczenia cyfrowe, niemniej równie ważna jest edukacja pracowników. Eksperci wskazują, że zwiększanie świadomości zagrożeń wśród pracowników to konieczność do obrony przed cyberatakami. — Edukacja w zakresie rozpoznawania phishingu, inżynierii społecznej czy korzystanie z silnych haseł oraz MFA (Multi-factor authentication) minimalizuje ryzyko błędów. Większość naruszeń bezpieczeństwa wynika bowiem z ludzkich niedopatrzeń, takich jak np. kliknięcie w złośliwy link — zauważa Tomasz Żelski.

Dlatego regularne szkolenia pracowników tworzą kulturę cyberbezpieczeństwa. Świadomość zagrożeń sprawia, że organizacja staje się mniej podatna na ataki. — Nowoczesne technologie, takie jak AI, machine learning, big data czy cloud, użyte w konkretnych rozwiązaniach, przyczyniają się do poprawy poziomu bezpieczeństwa. Za ich pomocą możemy nie tylko przyśpieszać wykrywanie zagrożeń czy lepiej chronić dane, jesteśmy też w stanie przewidywać ataki, co wspiera proaktywne podejście do bezpieczeństwa firmy. Musimy jednak pamiętać, że technologia automatyzuje i wspiera procesy, ale ludzie muszą umieć ją wykorzystać oraz dostosować do zmieniających się zagrożeń — podkreśla ekspert Grupy PZU. Synergia nowoczesnych technologii i przeszkolonych pracowników pozwala firmom skutecznie reagować na dynamicznie zmieniający się krajobraz zagrożeń cybernetycznych. ■

Firm korzysta z outsourcingu przynajmniej jednej funkcji cyberbezpieczeństwa. Ma to związek z tym, że brakuje na rynku specjalistów ds. bezpieczeństwa IT i są trudności z rekrutacją i utrzymaniem wykwalifikowanych pracowników.

Mniej niż połowa organizacji przekonuje, że są bardzo dobrze lub dobrze przygotowane do zmieniających się regulacji w kontekście cyberbezpieczeństwa, ochrony danych i prywatności.

Niezmiennie od lat głównym zagrożeniem w sieci jest kradzież danych poprzez phishing.

Źródło: „Barometr cyberbezpieczeństwa 2024", KPMG w Polsce

Grupy stanowiące realne zagrożenie dla organizacji. Kogo obawiają się przedsiębiorstwa w 2024 r.?

Źródło: KPMG w Polsce na podstawie badania ankietowego

Strategie i rozwiązania w cyberbezpieczeństwie

Strategie zależą od potrzeb organizacji, natomiast istnieje szereg praktyk, które możemy uznać za niezbędne. Kluczowym działaniem jest implementacja procesu Patch Management, którego celem jest eliminacja luk w zabezpieczeniach poprzez regularne aktualizacje oprogramowania i systemów. Wartościowe jest również wdrożenie systemów automatycznej aktualizacji, które instalują krytyczne poprawki bezpieczeństwa.

Kolejną istotną kwestią jest segmentacja sieci, czyli izolowanie krytycznych zasobów. Przykładem jest oddzielenie systemów finansowych od sieci ogólnodostępnych.

Z kolei w obszarze monitorowania rekomenduje się zastosowanie rozwiązań IPS/IDS, które wykrywają i zapobiegają atakom w czasie rzeczywistym. Monitorowanie logów pozwala na szybkie reagowanie na podejrzane działania.

Ważne jest również regularne tworzenie kopii zapasowych danych oraz testowanie procedur ich odzyskiwania w razie ataków. W celu ochrony przed ransomware należy przechowywać kopie zapasowe w wersji offline lub w odizolowanej sieci — konieczne jest również wdrożenie rozwiązań typu EDR.

Coraz szerzej rynek stosuje też podejście do bezpieczeństwa w modelu Zero Trust Architecture oraz bezpieczną konfigurację chmurową w celu kompleksowej ochrony danych. Podstawową praktyką powinno natomiast stać się edukowanie pracowników w zakresie zagrożeń cyberbezpieczeństwa. ■

Tomasz Żelski, dyrektor zarządzający ds. IT i digitalizacji w Grupie PZU

Polska znajduje się na 4. miejscu wśród państw europejskich najczęściej atakowanych przez cyberprzestępców. Przed nami są tylko Ukraina, Wielka Brytania i Francja.

Tyle prób cyberataków wykrywają każdego dnia chmurowe mechanizmy Microsoftu, wspierane sztuczną inteligencją. Dane dotyczą 2024 r.

Źródło: Microsoft Digital Defense Report 2024

Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji

Źródło: „Barometr cyberbezpieczeństwa 2024", KPMG w Polsce

Największym wyzwaniem dla firm w osiągnięciu odpowiedniego poziomu zabezpieczeń nie są budżety, lecz przede wszystkim trudności związane z rekrutacją i utrzymaniem wykwalifikowanych pracowników.

2

Najczęstsze zagrożenia cybernetyczne

Tyle incydentów cybernetycznych odnotowano w Polsce w 2023 r. To dwukrotny wzrost w porównaniu do roku 2022.

O tyle proc. według World Economic Forum wzrośnie liczba ataków na sektor zdrowia w 2024 r.

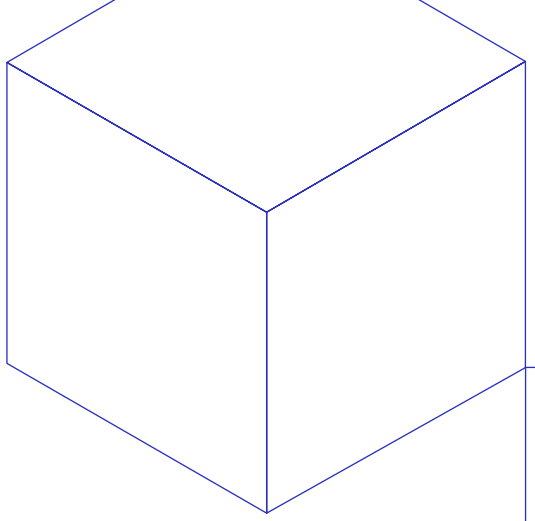
Eksperci z World Economic Forum podkreślają, że szybko rośnie liczba ataków z użyciem sztucznej inteligencji do przeprowadzania wyrafinowanych ataków socjotechnicznych.

Źródło: Raport „Global Cybersecurity Outlook 2024" World Economic Forum

Wzrost liczby cyberataków jest widoczny również w kontekście Internetu rzeczy (IoT), gdzie urządzenia często nie są wystarczająco zabezpieczone. W 2024 r. przewiduje się, że ataki na urządzenia IoT będą rosnąć, co może prowadzić do poważnych naruszeń bezpieczeństwa danych. W Polsce 58 proc. firm zgłosiło przynajmniej jeden incydent związany z naruszeniem bezpieczeństwa, co podkreśla potrzebę zwiększenia inwestycji w cyberbezpieczeństwo.

W nadchodzących latach niezbędne dla firm będzie nie tylko wdrażanie skutecznych strategii ochrony przed cyberzagrożeniami, ale także edukacja pracowników oraz współpraca międzysektorowa w celu zwiększenia odporności na ataki.

Najczęstsze zagrożenia cybernetyczne dla firm



Zagrożenia dla firm stają się coraz bardziej złożone i wyrafinowane. W 2024 r. przewiduje się, że głównymi zagrożeniami będą ataki ransomware, phishingowe oraz złośliwe oprogramowanie.

Ransomware, czyli oprogramowanie wymuszające okup za dostęp do danych, pozostaje jednym z najpoważniejszych zagrożeń. Według raportu Bitdefender grupy zajmujące się tym rodzajem ataków **nadal będą celować w organizacje, które często nie aktualizują swojego oprogramowania w sposób wystarczający**.

Phishing, w tym szczególnie ataki Business Email Compromise (BEC), to kolejne istotne zagrożenie. Ataki te wykorzystują ludzkie słabości, co czyni je niezwykle niebezpiecznymi. W 2022 r. straty związane z atakami BEC wyniosły 2,7 miliarda dolarów, a ich liczba wzrosła o 81 proc. w porównaniu do roku poprzedniego. Firmy są szczególnie narażone na te ataki ze względu na niską świadomość pracowników oraz brak odpowiednich zabezpieczeń.

Co więcej, **rozwój sztucznej inteligencji przyczynia się do ewolucji metod ataków**. To sprawia, że hakerzy mogą przeprowadzać bardziej skomplikowane operacje. Wzrost liczby cyberataków jest również związany z przejściem na pracę zdalną, co zwiększa podatność firm na ataki ze względu na używanie niezabezpieczonych urządzeń oraz niewystarczające procedury zabezpieczeń.

Poważne zagrożenia w Polsce

W Polsce już 70 proc. firm doświadczyło sytuacji zagrażającej bezpieczeństwu danych. Koszty związane z cyberatakami mogą przekraczać milion złotych, a ich wpływ na działalność przedsiębiorstw często jest trudny do oszacowania. Warto zauważyć, że **na świecie niemal dwie trzecie małych i średnich przedsiębiorstw, które padły ofiarą cyberataku, upada w ciągu sześciu miesięcy od incydentu** — wynika z raportu National Cyber Security Alliance.

Na świecie niemal dwie trzecie małych i średnich przedsiębiorstw, które padły ofiarą cyberataku, upada w ciągu sześciu miesięcy od incydentu.

W obliczu rosnących zagrożeń cybernetycznych firmy powinny inwestować w odpowiednie zabezpieczenia oraz edukację pracowników. Wskazane, czy wręcz konieczne jest wdrażanie polityk ochrony danych oraz regularne aktualizowanie systemów IT, aby zminimalizować ryzyko skutków ataków.

W firmach bardzo ważne są szkolenia i edukacja personelu z zakresu cyberbezpieczeństwa. — Bezpieczny pracownik to świadomy pracownik, dlatego nie zatrzymujemy się na przekazywaniu pracownikom wewnętrznych procedur — realizujemy szereg działań edukacyjnych — mówi Bartosz Zbyszewski, dyrektor ds. ryzyka i bezpieczeństwa IT w Grupie PZU. — **Podstawową formą przekazania wiedzy są e-learningi. Każdy pracownik ma obowiązek przejść szkolenie z najważniejszymi zasadami cyberbezpieczeństwa.** Udostępniamy również dodatkowe materiały w formie quizów, animacji, filmików, a także nowoczesnej aplikacji VR, w której można przeżyć wirtualną przygodę, próbując uratować świat przed cyberzagładą. Prowadzimy kampanie wewnętrzne, w których staramy się chwytliwymi hasłami, aktualnościami i ciekawostkami zainteresować pracowników tematyką cyberbezpieczeństwa. Realizujemy także kampanie antyphingowe, których celem jest uświadomienie pracownikom tego rodzaju zagrożenia, oraz sprawdzenie podatności organizacji na tego typu ataki — wymienia.

Jeśli pracownicy będą wiedzieć, dlaczego tak ważne jest stosowanie bezpiecznego hasła, dbanie o aktualizację oprogramowania, znajomość socjotechnik czy sztuczek przestępców — nie tylko organizacja będzie bezpieczniejsza, ale także oni i ich bliscy. ■

3

Zarządzanie ryzykiem cybernetycznym

PZU

BUSINESS INSIDER

Zarządzanie ryzykiem cybernetycznym

Ocena ryzyka cybernetycznego dla firm jest procesem, który pozwala na identyfikację, analizę i zarządzanie zagrożeniami związanymi z bezpieczeństwem informacji. Istnieje wiele metod, które można zastosować w tym zakresie, a każda z nich ma swoje unikalne cechy i zastosowania.

Ocena ryzyka cybernetycznego to wieloaspektowy proces wymagający zastosowania różnych metod i narzędzi, które łączą analizę danych z praktycznymi strategiami ochrony przed zagrożeniami. W miarę jak cyberzagrożenia stają się coraz bardziej zaawansowane, **ciągłe doskonalenie metod oceny ryzyka staje się niezbędne dla zapewnienia bezpieczeństwa organizacji**.

Jednocześnie wiele firm popełnia błędy przy ocenie ryzyka cybernetycznego. — Największe zdarzenia cybernetyczne ostatniej dekady były spowodowane cyberatakami, a nie błędem ludzkim czy awarią systemu, dlatego katalog potencjalnych cyberzagrożeń kojarzony jest zazwyczaj niemal wyłącznie jako ataki hakerskie: malware, phishing itp. **Tymczasem do naruszenia bezpieczeństwa danych dojść może również w wyniku błędu — pracownika czy dostawcy**, ponieważ cyberbezpieczeństwo nigdy nie jest tylko problemem technologicznym — zauważa Monika Ściuba, koordynator ds. underwritingu w PZU. — Podobnie jak w przypadku pozostałych ryzyk, główną rolę odgrywają ludzie i procesy. Systemy bezpieczeństwa IT nie zabezpieczą krytycznych informacji i własności intelektualnej, jeśli pracownicy nie będą stosować bezpiecznych praktyk w zakresie cyberbezpieczeństwa — dodaje.

Druga kwestia to ocena ryzyka i rozłożenie akcentów w budowaniu odporności organizacji. Jak zauważa Monika Ściuba, tu widoczna jest przewaga umacniania obrony przed atakami nad strategią zakładającą, że bezpieczeństwo danych zostanie naruszone. — Tylko przy drugim podejściu można mówić o realnej ochronie, czyli przed nieuprawnionym wykorzystaniem informacji i zdolności ich odzyskania po naruszeniu — mówi.

Od cyberataków można się ubezpieczyć

Warto zauważyć, że w obecnych czasach **firmy mogą ubezpieczyć się również od cyberataków. Ubezpieczenie PZU Cyber to ochrona przedsiębiorstw przed stratami finansowymi** (kosztami własnymi, odszkodowaniami), wynikającymi m.in. z naruszenia przepisów prawa polskiego (np. RODO) lub obcego, dotyczących ochrony prywatności. — Bardzo ważnym zakresem ubezpieczenia jest wsparcie w zarządzaniu incydentem i usługi świadczone przez panel specjalistów. W praktyce oznacza to, że w ramach umowy ubezpieczenia zapewniamy organizację i pokrycie kosztów pomocy specjalistów m.in. IT, informatyków śledczych, prawników, agencji PR, biegłych księgowych — podkreśla Monika Ściuba z PZU.

Wsparcie PZU Cyber dotyczy też zawiadomienia Prezesa Urzędu Ochrony Danych i poszkodowanych o zaistniałym incydencie. **Ubezpieczyciel pokrywa też koszty porad prawnych, przygotowania zawiadomień, wysyłki korespondencji czy wsparcia agencji PR.** Pomoc rozpoczyna się wraz ze zgłoszeniem incydentu i może trwać aż do zakończenia postępowania włącznie, więc nawet długo po zakończeniu okresu ubezpieczenia w polisie. ■

Ubezpieczyciel weźmie na siebie część ryzyka

Wymagania określone w regulacji NIS2 dotyczące identyfikacji i ochrony danych krytycznych, planów reagowania i ciągłości działania oraz MFA są od lat podstawowymi informacjami wykorzystywanymi przy ocenie ryzyk cybernetycznych przez ubezpieczycieli.

Wpływając na poprawę bezpieczeństwa przedsiębiorstw regulacja NIS2 przekłada się na dostępność ubezpieczeń cybernetycznych. Warto o tym pamiętać w kontekście tej regulacji, która na przedsiębiorstwa objęte jej zakresem nakłada m.in. obowiązki raportowania incydentów czy zarządzania ryzykiem cybernetycznym. Posiadanie ubezpieczenia od ryzyk cybernetycznych może wesprzeć organizację w realizacji tych wymogów.

Podobnie jak w innych produktach ubezpieczeniowych, w PZU do wyboru mamy różne zakresy ochrony, dopasowane do skali i profilu działalności ubezpieczonego. Począwszy od tych skupiających się wyłącznie na ubezpieczeniu odpowiedzialności z tytułu naruszenia danych osobowych, do rozbudowanych produktów obejmujących ochroną skutki braku dostępu usług, utraty klientów czy utraty zysku w wyniku szkody u usługodawcy.

Myśląc o strategii firmy w zakresie cyberbezpieczeństwa, należy rozważać przeniesienie części ryzyka na ubezpieczyciela. ■

Monika Ściuba, koordynator ds. underwritingu w PZU

4

Podstawowe zasady bezpieczeństwa IT

PZU

BUSINESS INSIDER

Podstawowe zasady bezpieczeństwa IT

Zasady bezpieczeństwa są niezbędne dla ochrony danych i systemów informatycznych przed zagrożeniami. W 2024 roku organizacje powinny skupić się na kilku fundamentalnych zasadach, które mogą znacząco podnieść poziom bezpieczeństwa.

Pierwszą zasadą jest stosowanie silnych haseł. Hasła powinny być długie, unikalne i zawierać kombinację liter, cyfr oraz znaków specjalnych. Regularna ich zmiana jest również istotna, aby zminimalizować ryzyko nieautoryzowanego dostępu do systemów.

Kolejnym elementem jest zarządzanie dostępem. Warto wprowadzić różne role użytkowników w systemach IT, co pozwoli na ograniczenie dostępu do danych tylko do tych pracowników, którzy rzeczywiście go potrzebują. Zasada minimalnych uprawnień, tzw. Zero Trust, powinna być stosowana w każdej organizacji, aby przydzielać pracownikom jedynie te uprawnienia, które są niezbędne do wykonywania ich obowiązków.

Regularne aktualizacje oprogramowania i systemów operacyjnych są niezbędne do ochrony przed znanymi lukami bezpieczeństwa. Firmy powinny wdrożyć procesy aktualizacji oraz instalacji poprawek w sposób ciągły. Ważnym aspektem jest również posiadanie skutecznego oprogramowania antywirusowego oraz zapór sieciowych (firewall), które stanowią pierwszą linię obrony przed złośliwym oprogramowaniem i atakami z sieci.

Nie można zapominać o regularnym tworzeniu kopii zapasowych danych. To zabezpieczenie chroni przed utratą informacji w wyniku awarii systemu lub ataku ransomware. Co więcej, firmy powinny wdrożyć procedury dotyczące dostępu zdalnego, zwłaszcza w kontekście pracy hybrydowej. Odpowiednie zabezpieczenia i polityki muszą być wprowadzone, aby zminimalizować ryzyko związane z dostępem do firmowych zasobów z urządzeń osobistych.

Wszystkie te zasady powinny być częścią szerszej polityki bezpieczeństwa, która określa ramy działania i procedury dotyczące ochrony informacji w organizacji. Polityka ta powinna być regularnie przeglądana i aktualizowana, aby odpowiadała zmieniającym się zagrożeniom i technologiom.

Bardziej zaawansowane podejście

Oczywiście w wielu organizacjach podstawowe zasady nie wystarczą i potrzebne są dodatkowe działania. Grupa PZU może tu posłużyć

za dobry przykład. — Stawiamy na nowoczesne technologie, które nie tylko zwiększają wydajność naszego IT, ale równocześnie zapewniają nam ciągłość działania i ochronę danych. Regularne aktualizacje oprogramowania są kluczowe w naszej strategii IT, ponieważ eliminują luki w zabezpieczeniach, co znacząco obniża ryzyko cyberataków i zwiększa naszą odporność na nowe zagrożenia. Utrzymanie oprogramowania w najnowszej wersji jest również konieczne dla spełnienia wymogów regulacyjnych i standardów branżowych, minimalizuje to ryzyko związane z audytami i zapewnia zgodność z przepisami, m.in. z RODO — podkreśla Sławomir Brzozowski, dyrektor ds. utrzymania usług IT w Grupie PZU.

Jednocześnie rozwiązania chmurowe pozwalają PZU dynamicznie dostosowywać zasoby IT do zmieniających się potrzeb biznesowych. Chmura umożliwia reagowanie na zwiększone obciążenie systemów w czasie rzeczywistym, co jest kluczowe dla utrzymania ciągłości działania. — Rozwiązania chmurowe umożliwiają naszym pracownikom bezpieczny dostęp do zasobów IT z dowolnego miejsca, co w modelu pracy hybrydowej, który posiadamy, jest dla nas bardzo ważne. W PZU chcemy realizować strategię hybrydową, łącząc infrastrukturę chmurową z lokalnymi zasobami IT. Ten model pozwala nam na elastyczne zarządzanie danymi i aplikacjami, optymalizację kosztów oraz szybszą reakcję na zmieniające się potrzeby biznesowe — mówi Sławomir Brzozowski. ■

Zasady bezpieczeństwa a analiza ryzyka. Jak postępować?

Zasady to bezpieczeństwo, natomiast ocena ryzyka jest równie istotna. W jaki sposób sprawdzić możliwość wystąpienia zagrożenia czy też jak opracować strategie obronne? Warto stosować się do tych pięciu kroków:

Analiza prawdopodobieństwa i skutków
Polega ona na ocenie prawdopodobieństwa wystąpienia określonego zagrożenia oraz skutków, jakie mogłoby ono spowodować. Dzięki temu firmy mogą klasyfikować ryzyka i priorytetyzować je w zależności od ich potencjalnego wpływu na działalność.

Analiza historii incydentów
Metoda, która polega na badaniu wcześniejszych incydentów związanych z bezpieczeństwem. Umożliwia to identyfikację wzorców ataków oraz prognozowanie przyszłych ryzyk na podstawie zebranych danych.

Innym podejściem jest metoda Value at Risk (VaR), która szacuje maksymalną stratę, jaką organizacja może ponieść w wyniku incydentu bezpieczeństwa informatycznego. Ta metoda opiera się na analizie rozkładu prawdopodobieństwa strat oraz ustalaniu poziomu ufności dla tych oszacowań.

Modelowanie zagrożeń
Pproces identyfikacji i analizy potencjalnych zagrożeń dla systemów IT. Umożliwia to nie tylko zrozumienie, jakie ataki mogą wystąpić, ale także opracowanie strategii obronnych.

Analiza skuteczności kontroli
Ocenia, jak dobrze istniejące zabezpieczenia chronią przed atakami. Analizując dane dotyczące ataków oraz skuteczność środków obronnych, organizacje mogą dostosować swoje strategie bezpieczeństwa.

Analiza trendów i prognozowanie ryzyka
Pozwala na przewidywanie przyszłych zagrożeń na podstawie analizy danych historycznych i aktualnych trendów w cyberprzestępczości.

Rekomendacje na bezpieczną pracę

Funkcjonuje szereg podstawowych praktyk, które jednocześnie można uznać za priorytet w kontekście bezpieczeństwa danych i ochrony operacji biznesowych. Silne hasła do kont to absolutna podstawa — nowe hasło powinno znacząco różnić się od poprzedniego, a zdania lub frazy warto zamieniać na ciąg inicjałów, cyfr i symboli. W przypadku trudności w zapamiętaniu wielu haseł można skorzystać z programów do zarządzania nimi. Uświadamianie pracowników w zakresie mocy hasła jest kluczowe dla powodzenia tego podstawowego kroku. Ważne jest również uwierzytelnianie wielopoziomowe, które w przypadku próby kradzieży danych może skutecznie ją utrudnić.

Wiele mówi się też o aktualizacjach systemów — to priorytet dla działów cyberbezpieczeństwa również w zakresie bezpieczeństwa danych i ochrony procesów biznesowych. Jeśli chcemy, aby dane, do których dostęp mają pracownicy w czasie ich codziennych zadań, były odpowiednio zabezpieczone, to musimy zadbać o bezpieczeństwo sieci internetowej. Korzystanie z VPN podczas pracy zdalnej to gwarancja szyfrowania ruchu i ograniczenie ryzyka „podsłuchiwania" transmisji danych.

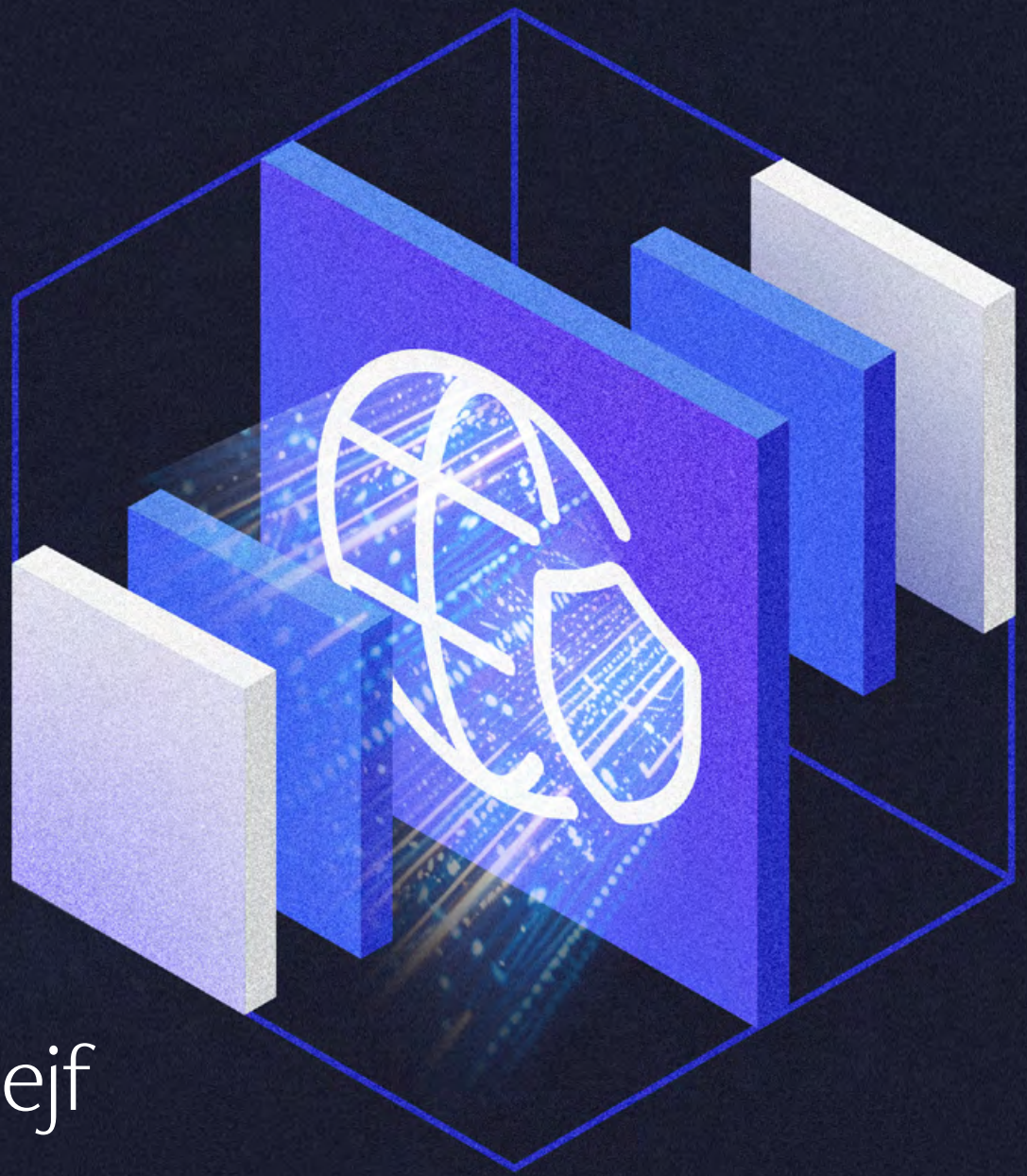
Pracownicy powinni korzystać jedynie ze zweryfikowanych przeglądarek internetowych, które uznajemy za bezpieczne. Warto wspomnieć również o edukacji pracowników w zakresie rozpoznawania oszustw związanych z wyłudzeniem informacji — klikanie w podejrzane linki czy odpowiadanie na prośby podania poufnych informacji może prowadzić do groźnego wycieku danych.

Z kolei do jednej z najbardziej podstawowych — a tak bardzo ważnych praktyk — możemy zaliczyć zasadę blokowania komputera przy opuszczaniu stanowiska pracy, aby niepowołana osoba nie miała dostępu do naszych danych. Przyjęcie tych priorytetowych zasad pomaga w minimalizowaniu ryzyka i tworzeniu bezpiecznego środowiska pracy. ■

Grażyna Maśnica, kierownik zespołu zarządzania ochroną informacji, inspektor ochrony danych w Grupie PZU

5

Firmowa sieć jak najnowocześniejszy sejf



PZU

BUSINESS INSIDER

Firmowa sieć jak najnowocześniejszy sejf

Bezpieczeństwo sieci to niezbędny element funkcjonowania każdej nowoczesnej firmy. Ochrona przed zagrożeniami, takimi jak ataki ransomware, kradzież danych czy sabotaż wewnętrzny, wymaga zastosowania zaawansowanych narzędzi, takich jak firewalle, systemy IDS/IPS oraz SIEM i SOAR. Inwestycja w te technologie to inwestycja w stabilność i bezpieczeństwo firmy.

Bezpieczeństwo sieci to fundament, na którym opiera się funkcjonowanie współczesnych firm. W dobie cyfryzacji, gdzie dane są jednym z najcenniejszych zasobów, ochrona przed zagrożeniami staje się priorytetem. Ataki ransomware, kradzież danych czy sabotaż wewnętrzny mogą prowadzić do ogromnych strat finansowych, utraty zaufania klientów oraz poważnych problemów prawnych. Bezpieczna sieć ma chronić organizację przed atakami tego rodzaju.

W kontekście bezpieczeństwa sieci ważne są systemy wykrywania i zapobiegania włamaniom (IDS/IPS). IDS (Intrusion Detection System) to systemy, które monitorują ruch sieciowy w poszukiwaniu podejrzanych działań. Z kolei IPS (Intrusion Prevention System) idą o krok dalej, nie tylko wykrywając, ale również zapobiegając potencjalnym zagrożeniom.

Zapora sieciowa. Jakie istnieją?

Firewalle to podstawowe narzędzie ochrony sieci, które monitoruje i kontroluje ruch sieciowy. Istnieją różne typy firewalli, które oferują różne poziomy ochrony.

Tradycyjne firewalle: tradycyjne firewalle, takie jak stateless i stateful inspection, działają na poziomie sieciowym. Stateless firewalle analizują każdy pakiet danych niezależnie, podczas gdy stateful inspection firewalle śledzą stan połączeń sieciowych, co pozwala na bardziej zaawansowaną kontrolę ruchu.

Nowoczesne firewalle aplikacyjne (WAF): działają na poziomie aplikacji, co pozwala na ochronę przed bardziej zaawansowanymi zagrożeniami, takimi jak ataki SQL injection czy cross-site scripting (XSS).

Grupa PZU to jedna z organizacji, która stawia na rozległą architekturę i w rezultacie ma wielowarstwowy system ochronny, zgodny z zasadą Defence in Depth. — Podstawowe systemy obronne w zakresie ataków sieciowych to z pewnością NGFW (firewalle), IPS, system antyDDoS. Dodatkowo warto również pamiętać o ochronie DNS i Web Application Firewall, chroniącym systemy udostępnione w internecie. To elementy ochrony zewnętrznej — zauważa Bartosz Zbyszewski, dyrektor ds. ryzyka i bezpieczeństwa IT w Grupie PZU.

Ekspert dodaje przy tym: — Nie możemy zapominać, że wewnątrz firmy również może pojawić się zagrożenie. Podstawowe systemy ochrony wewnętrznej to Proxy, ochrona kanału poczty elektronicznej, zaawansowany system ochrony przed kodem, moduły machine learning, obserwacja zagrożeń i anomalii w segmentach sieci za pomocą systemu klasy Network Detection and Response (NDR). Każdy budynek musi mieć plan i podobnie jest z siecią — kluczowe jest dobre rozplanowanie elementów topologii sieci, eliminujące w miarę możliwości słabe punkty już w fazie projektowania, oraz jej segmentacja. Systemy bezpieczeństwa i sieciowe powinna cechować wysoka dostępność i wydajność.

Zaawansowane technologie ochrony sieci

Jeśli chodzi o zaawansowane technologie w ochronie sieci, sandboxing izoluje aplikacje w kontrolowanym środowisku, aby zapobiec ich potencjalnemu wpływowi na resztę systemu. Dzięki temu, nawet jeśli aplikacja jest zainfekowana złośliwym oprogramowaniem, nie może ono rozprzestrzenić się poza sandbox.

Jednym z głównych zagrożeń związanych z sandboksingiem jest możliwość obejścia izolacji przez zaawansowane złośliwe oprogramowanie. Dlatego ważne jest, aby regularnie aktualizować i monitorować środowiska sandbox.

Idąc dalej, dobrą praktyką jest wdrożenie systemyu IAM (Identity and Access Management), czyli do zarządzania tożsamością i dostępem. Nowoczesne systemy IAM, takie jak Azure AD i Okta, odgrywają ważną rolę w ochronie dostępu do kluczowych zasobów. IAM umożliwia zarządzanie tożsamościami użytkowników oraz kontrolowanie, kto ma dostęp do jakich zasobów.

Zaawansowane techniki autoryzacji wielopoziomowej (MFA) to kolejny element strategii cyberbezpieczeństwa. Wielopoziomowe autoryzacje zwiększają bezpieczeństwo, wymagając od użytkowników

Wirtualna sieć prywatna to konieczność

VPN (Virtual Private Network) to technologia, która zapewnia bezpieczną transmisję danych nawet przez niezabezpieczone sieci publiczne.

VPN szyfruje dane przesyłane między użytkownikiem a siecią, co chroni je przed przechwyceniem przez osoby trzecie. Jest to szczególnie ważne w przypadku pracy zdalnej, gdzie pracownicy łączą się z firmową siecią z różnych lokalizacji.

Tradycyjne technologie VPN, takie jak IPsec, oferują solidne zabezpieczenia, ale mogą być one skomplikowane w konfiguracji. Nowoczesne technologie, oparte na protokole takim jak WireGuard, są prostsze w implementacji i oferują lepszą wydajność.

Przykładowy scenariuszy wykorzystania VPN w korporacjach: zdalny dostęp do zasobów firmowych, bezpieczne połączenia między oddziałami firmy, ochrona przed atakami typu man-in-the-middle.

potwierdzenia tożsamości za pomocą kilku metod, takich jak hasło i kod SMS. Dzięki temu, nawet jeśli jedno z zabezpieczeń zostanie złamane, dostęp do zasobów pozostaje chroniony.

SIEM i SOAR

Systemy zarządzania informacją i zdarzeniami (SIEM — Security Information and Event Management) oraz automatyzacji reakcji (SOAR — Security Orchestration, Automation and Response) są nieodzownymi narzędziami w nowoczesnym zarządzaniu bezpieczeństwem. Narzędzia te umożliwiają zbieranie, analizowanie i reagowanie na zdarzenia w czasie rzeczywistym.

— SIEM i SOAR to systemy cyberbezpieczeństwa, które służą ochronie sieci poprzez zbieranie i korelację danych, a jednocześnie automatycznie reagują na zdarzenia z tego obszaru. SIEM gromadzi dane, które pozwalają wykryć naruszenia bezpieczeństwa, anomalie, a SOAR pomaga w automatyzacji obsługi incydentów bezpieczeństwa za pomocą tzw. playbooków — instrukcji wskazujących, co dokładnie powinno się zadziać w momencie wystąpienia niebezpiecznej sytuacji wykrytej przez SIEM — tłumaczy Bartosz Zbyszewski.

Grupa PZU używa obu klas rozwiązań, które wspomagają analityków SOC (Security Operations Center) w codziennym monitorowaniu cyberbezpieczeństwa. Oczywiście, żaden system nie zastąpi człowieka, ale systemy tego rodzaju znacznie skracają czas odpowiedzi na zagrożenia, pozwalają poprawić ogólny obraz bezpieczeństwa. — Dzięki nim jesteśmy szybsi i skuteczniejsi. PZU za pomocą SOAR wzbogaca kontekst i odciąża SOC z powtarzalnych, cyklicznych czynności, np. sprawdza reputację wielu adresów IP z pomocą kilkudziesięciu serwisów reputacyjnych w ciągu kilkunastu sekund, co znacznie skraca czas weryfikacji. Integracje między SIEM, SOAR i innymi systemami cyberbezpieczeństwa pozwalają na zbudowanie skutecznej reakcji obronnej lub gromadzącej materiał dowodowy, która działa w trybie 24/7. SIEM gromadzi dane, SOAR zaś reaguje i dokonuje zmian, np. przekazuje konkretne adresy IP do zablokowania, w innych systemach bezpieczeństwa z nim zintegrowanych. Holistyczne podejście do cyberbezpieczeństwa pozwala zwiększyć bezpieczeństwo całej organizacji — podkreśla ekspert z PZU.

Zaawansowane technologie ochrony sieci, takie jak sandboxing, IAM, SIEM i SOAR odgrywają bardzo ważną rolę w zabezpieczaniu organizacji przed złośliwym oprogramowaniem i innymi zagrożeniami. Inwestowanie w te technologie oraz ich regularne aktualizowanie i monitorowanie jest niezbędne dla utrzymania wysokiego poziomu bezpieczeństwa. ■

Monitorowanie pasywne vs. aktywne

IDS (Intrusion Detection System) działa w trybie pasywnym, co oznacza, że jedynie monitoruje i raportuje podejrzane działania.

IPS (Intrusion Prevention System) działa w trybie aktywnym, co pozwala na natychmiastowe blokowanie zagrożeń. Popularne narzędzia IDS/IPS to Snort i Suricata.

Bartosz Zbyszewski, dyrektor ds. ryzyka i bezpieczeństwa IT w Grupie PZU

Trendy i wyzwania w obszarze bezpieczeństwa sieci

W najbliższych latach wyzwaniem będzie różnorodność urządzeń, które mogą być źródłem zagrożenia oraz brak — w mojej ocenie — jednolitego standardu i regulacji w tym zakresie.

Najczęściej są to zamknięte konstrukcje, w które nie można prosto ingerować, dlatego ważne jest obserwowanie ich zachowania w sieci z pomocą systemów mogących wykryć niebezpieczne zachowania, takich jak NDR.

Obecnie ilość urządzeń generujących ruch sieciowy zwiększa się wykładniczo, przez co potrzebujemy coraz lepszych i wydajniejszych sieci. Zwłaszcza że każde urządzenie zwiększa powierzchnię ataku i musi być monitorowane.

AI i machine learning wspomagają i będą w coraz większym stopniu wspierać przetwarzanie i analizę danych dotyczącą takich urządzeń oraz identyfikację wszelkich zagrożeń. Obserwujemy coraz częstsze wykorzystywanie tych technologii w cyberbezpieczeństwie, ponieważ złożoność i ilość danych przekracza już możliwości ludzkiej analizy, a także brakuje specjalistów w tym zakresie.

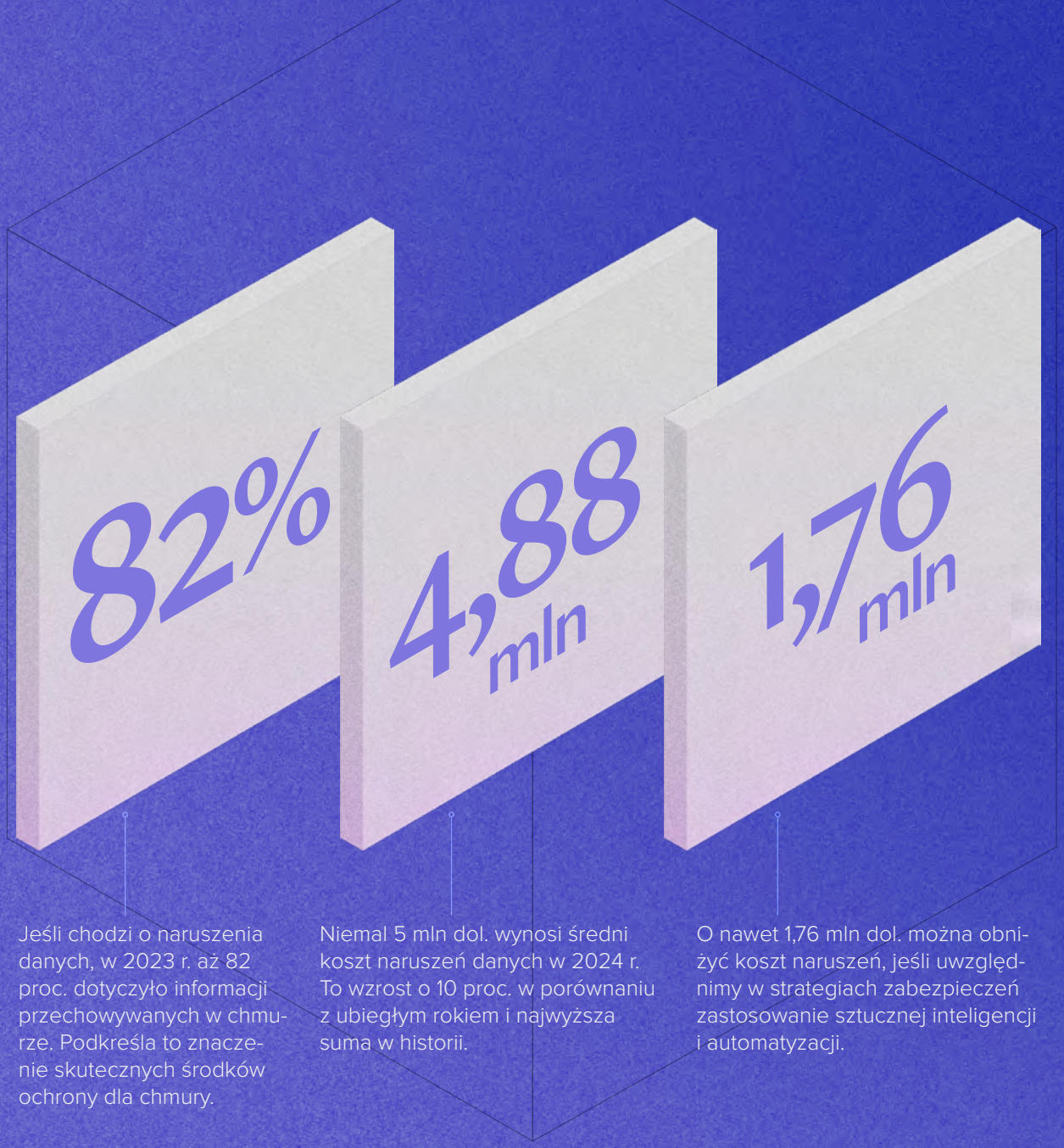
Człowiek oczywiście nadal jest i pozostanie niezbędny, ale musi mieć narzędzia analityczne, które go wspomagają. Dane z kolei coraz częściej muszą być przetwarzane w chmurze, ponieważ tylko tam uzyskujemy niezbędną wydajność i pojemność dla takiej ilości informacji. ■

6

Cyberbezpieczeństwo w chmurze i AI

PZU

BUSINESS INSIDER



Jeśli chodzi o naruszenia danych, w 2023 r. aż 82 proc. dotyczyło informacji przechowywanych w chmurze. Podkreśla to znaczenie skutecznych środków ochrony dla chmury.

Niemal 5 mln dol. wynosi średni koszt naruszeń danych w 2024 r. To wzrost o 10 proc. w porównaniu z ubiegłym rokiem i najwyższa suma w historii.

O nawet 1,76 mln dol. można obniżyć koszt naruszeń, jeśli uwzględnimy w strategiach zabezpieczeń zastosowanie sztucznej inteligencji i automatyzacji.

Źródło: Raporty „Cost of a Data Breach 2024” oraz „New X-Force Cloud Threat Landscape 2023” firmy IBM

Według raportu IBM dane przechowywane w publicznych chmurach mają najwyższe średnie koszty naruszeń, osiągające niemal 5 mln dol. Kolejnym istotnym elementem jest zarządzanie dostępem. Wiele naruszeń wynika z niewłaściwego użycia poświadczeń oraz nadmiaru uprawnień. Raport wskazuje, że niewłaściwe zarządzanie dostępem do danych było główną przyczyną kompromitacji chmur w ciągu ostatnich 12 miesięcy. Firmy powinny wdrożyć zasady minimalnych uprawnień (Zero Trust) oraz regularnie przeglądać i aktualizować polityki dostępu.

Rola umów SLA (Service Level Agreement) oraz certyfikatów bezpieczeństwa dostawców chmury też nie może być pomijana. Umowy te określają poziom usług i odpowiedzialności dostawcy, co jest krytyczne dla zapewnienia bezpieczeństwa danych. Certyfikaty takie jak ISO/IEC 27001 potwierdzają zgodność dostawcy z uznawanymi standardami zarządzania bezpieczeństwem informacji.

W kontekście wykorzystania sztucznej inteligencji, zastosowanie AI i automatyzacji w strategiach zabezpieczeń może znacząco obniżyć koszty naruszeń. Organizacje, które wdrożyły te technologie, oszczędzają nawet ok. 2 mln dol. na kosztach związanych z naruszeniami. Bezpieczeństwo danych w chmurze wymaga natomiast kompleksowego podejścia, obejmującego szyfrowanie danych, zarządzanie dostępem oraz regularne przeglądy polityk bezpieczeństwa.

Cyberbezpieczeństwo w chmurze i AI

Coraz więcej firm przenosi swoje operacje do chmury. Z tego powodu bezpieczeństwo danych staje się bardzo ważnym zagadnieniem.

W 2023 r. według raportu IBM aż 82 proc. naruszeń danych dotyczyło informacji przechowywanych w chmurze. Podkreśla to znaczenie wdrażania najlepszych praktyk w zakresie bezpieczeństwa. Firmy powinny skupić się na kilku obszarach, aby skutecznie zabezpieczyć swoje zasoby w chmurze.

Jednym z najważniejszych kroków jest zabezpieczanie danych poprzez szyfrowanie. Szyfrowanie danych w spoczynku i w trakcie przesyłania jest niezbędne, aby chronić informacje przed nieautoryzowanym dostępem. Dostawcy usług chmurowych oferują zaawansowane funkcje szyfrowania, które powinny być wykorzystywane przez organizacje. Ważne jest również stosowanie silnego uwierzytelniania, takiego jak uwierzytelnianie wieloskładnikowe (MFA), które dodaje dodatkową warstwę ochrony.

Kolejnym istotnym aspektem jest **regularny przegląd polityk bezpieczeństwa**. Firmy powinny cyklicznie oceniać swoje procedury i polityki dotyczące bezpieczeństwa, aby dostosować je do zmieniających się zagrożeń oraz wymagań regulacyjnych. Warto również prowadzić audyty bezpieczeństwa i testy penetracyjne, które pomogą

zidentyfikować potencjalne luki w zabezpieczeniach.

Rola umów SLA (Service Level Agreement) jest również istotna w kontekście korzystania z usług chmurowych. Umowy te definiują poziom usług, jakie dostawca zobowiązuje się zapewnić, w tym kwestie związane z dostępnością, wsparciem technicznym oraz bezpieczeństwem danych. Firmy powinny dokładnie analizować te umowy, aby upewnić się, że dostawca spełnia ich oczekiwania dotyczące ochrony danych.

Pomogą certyfikaty

Certyfikaty bezpieczeństwa, takie jak ISO/IEC 27001, są kolejnym ważnym elementem oceny dostawców chmurowych. **Potwierdzają one, że dostawca stosuje uznane standardy zarządzania bezpieczeństwem informacji.** Wybierając dostawcę chmury, warto zwrócić uwagę na jego certyfikaty oraz zgodność z regulacjami branżowymi.

Zgodnie z danymi przedstawionymi przez Deloitte, istotnym elementem odpowiedzialności za bezpieczeństwo w chmurze jest także zrozumienie modelu wspólnej odpowiedzialności. Oznacza to, że choć dostawca chmury odpowiada za bezpieczeństwo infrastruktury, to organizacja korzystająca z tych usług musi dbać o zabezpieczenie swoich danych i aplikacji.

— Chmura staje się coraz bardziej powszechnym miejscem przetwarzania danych, ale niesie ze sobą liczne wyzwania i zagrożenia. W chmurach publicznych kluczowym problemem jest współdzielenie infrastruktury między wieloma użytkownikami, co zwiększa ryzyko nieautoryzowanego dostępu i ataków na dane. W chmurze prywatnej kontrola jest większa, ale wymaga ona znacznych nakładów na zabezpieczenia i utrzymanie infrastruktury — zauważa Artur Butryn, kierownik zespołu bezpieczeństwa rozwiązań chmurowych i testów bezpieczeństwa w Grupie PZU. — Model hybrydowy z kolei łączy te dwa światy, co **prowadzi do trudności w zapewnieniu spójnych zabezpieczeń i zarządzania danymi na różnych platformach**. Wyzwania związane z bezpieczeństwem w tym obszarze wymagają ciągłego monitorowania i aktualizacji konfiguracji oraz definiowania strategii bezpieczeństwa uwzględniając zgodność z obowiązującymi przepisami — dodaje.

Niezależnie od rodzaju chmury, najlepsze praktyki bezpieczeństwa obejmują szyfrowanie danych, regularne przeglądy polityk bezpieczeństwa oraz dokładną analizę umów SLA i certyfikatów dostawców. W miarę jak firmy kontynuują swoją cyfrową transformację, wdrażanie tych zasad stanie się niezbędne dla ochrony ich zasobów i zapewnienia zgodności z regulacjami. ■

Składowe elementy bezpieczeństwa w chmurze

Kontrola dostępu — w środowisku chmurowym, które jest dostępne przez internet, niezbędne jest, aby dostęp do zasobów miały wyłącznie uprawnione osoby, i to tylko na określony czas, niezbędny do realizacji ich zadań.

Zabezpieczenie danych — firmy muszą dokładnie monitorować lokalizację swoich danych i wdrażać odpowiednie mechanizmy ochronne, aby zabezpieczyć zarówno te dane, jak i infrastrukturę, która je przechowuje.

Przywracanie danych — niezbędnym elementem ochrony jest posiadanie solidnego rozwiązania do tworzenia kopii zapasowych oraz planu odzyskiwania danych na wypadek ich naruszenia.

Reagowanie na incydenty — w sytuacji ataku organizacja powinna mieć gotowy plan działania, który pozwoli ograniczyć skutki ataku oraz zabezpieczyć inne systemy przed potencjalnym naruszeniem.

Wdrażanie zabezpieczeń na wczesnym etapie — współpraca zespołów bezpieczeństwa i programistów w celu wbudowania zabezpieczeń w kod już na etapie tworzenia, tak by aplikacje chmurowe były od samego początku bezpieczne.

Skupienie zespołów ds. bezpieczeństwa na nowych zagrożeniach — wzmacniajmy też konfiguracje zasobów chmurowych w kodzie, aby zminimalizować ryzyko problemów związanych z bezpieczeństwem w środowiskach produkcyjnych.

Bezpieczeństwo chmurowe korzysta z AI

Sztuczna inteligencja w kontekście cyberbezpieczeństwa chmury może działać na dwóch płaszczyznach. Z jednej strony wspiera analizę dużej ilości danych, pozwalając na automatyczne wykrywanie anomalii. Natomiast z drugiej strony — może zostać wykorzystana przez cyberprzestępców np. do tworzenia zaawansowanych ataków phishingowych, które naśladują autentyczne, spersonalizowane wiadomości na podstawie m.in. danych pozyskanych z internetu.

Przykładem praktycznego zastosowania AI jest automatyzacja i optymalizowania procesów wewnętrznych, jak również usprawnianie doświadczeń oraz relacji z obecnymi i potencjalnymi klientami. W Grupie PZU funkcjonuje kilkaset modeli machine learningowych i AI, które wymagają bieżącego, aktywnego zarządzania i monitorowania.

Jednocześnie firmy korzystające z chmury powinny uwzględniać przede wszystkim odpowiednie mechanizmy zarządzania tożsamością i dostępem, wykorzystywanie wieloskładnikowego uwierzytelniania, dostępu z urządzeń zarządzanych oraz cyklicznej weryfikacji bezpiecznej konfiguracji. Ważnym elementem jest także szyfrowanie danych zarówno w spoczynku, jak i w trakcie ich transferu.

Nie możemy też zapominać o stosowaniu zabezpieczeń do ochrony danych wrażliwych przed ich utratą, nadużyciem, lub dostępem do nich nieuprawnionych osób, przy wykorzystaniu narzędzi DLP (Data Loss Prevention).

Co więcej, firmy powinny dokładnie weryfikować dostawców chmurowych w zakresie zgodności z wymaganiami bezpieczeństwa oraz pod kątem posiadanych certyfikatów, audytów bezpieczeństwa i przeprowadzonych testów penetracyjnych. ■

Artur Butryn, kierownik zespołu bezpieczeństwa rozwiązań chmurowych i testów bezpieczeństwa w Grupie PZU

7

Reagowanie na incydenty i planowanie awaryjne

PZU

BUSINESS INSIDER

Reagowanie na incydenty i planowanie awaryjne

W historii jest kilka przykładów incydentów bezpieczeństwa, które potwierdziły skuteczność zarządzania incydentami i planowania awaryjnego. — Jedna z największych firm transportowych na świecie padła ofiarą ataku ransomware. Atak sparaliżował systemy, co wpłynęło na globalne operacje — mówi Dariusz Gołębiewski, prezes zarządu PZU LAB SA. I dodaje: — Spółka miała wcześniej opracowane plany awaryjne, które obejmowały regularne kopie zapasowe danych oraz procedury przywracania systemów. **Po ataku zespół IT szybko zareagował, izolując zainfekowane systemy i przywracając operacje z kopii zapasowych.** Dzięki skutecznemu zarządzaniu incydentami i planowaniu awaryjnemu, spółka była w stanie zminimalizować czas przestoju i straty finansowe, a także szybko wznowić działalność.

Innym przykładem jest atak DDoS na dostawcę usług DNS, który spowodował zakłócenia w działaniu wielu popularnych stron internetowych, w tym Twittera (obecnie: X) i Netfliksa. Spółka miała wdrożone procedury monitorowania i reagowania na incydenty. — Po wykryciu ataku zespół natychmiast zidentyfikował źródło ataku i wprowadził środki zaradcze. **Dzięki wcześniejszym planom i szybkiemu działaniu, zdołano ograniczyć wpływ ataku na użytkowników i przywrócić usługi w stosunkowo krótkim czasie** — zauważa Dariusz Gołębiewski. Ekspert podkreśla, że skuteczne zarządzanie incydentami oraz planowanie awaryjne są kluczowe w minimalizacji skutków incydentów bezpieczeństwa. — Regularne testowanie planów, szkolenia zespołów oraz inwestycje w technologie zabezpieczeń przyczyniają się do szybkiej reakcji i ograniczenia strat — mówi.

Skuteczne zarządzanie incydentami oraz planowanie awaryjne stają się nie tylko obowiązkiem, ale i koniecznym elementem strategii biznesowej. W dobie cyfryzacji, gdzie każda minuta przestoju może oznaczać ogromne straty finansowe, umiejętność szybkiej reakcji i minimalizacji skutków kryzysowych staje się fundamentem nie tylko przetrwania, ale i rozwoju przedsiębiorstw.

Skuteczne reagowanie

Integracja planowania awaryjnego i ciągłości działania z ogólną strategią biznesową jest ważnym elementem zapewniającym stabilność i odporność organizacji na nieprzewidziane zdarzenia. Współczesne przedsiębiorstwa muszą dostosować swoje plany do stale zmieniającego się otoczenia, a to wymaga nie tylko opracowania skutecznych strategii, ale także ich regularnej aktualizacji i testowania. — Przede wszystkim należy upewnić się, że plany awaryjne są zgodne z celami strategicznymi firmy. **Należy zidentyfikować kluczowe procesy biznesowe i zasoby, które muszą być chronione.** Kierownictwo firmy musi być zaangażowane w proces planowania, aby zapewnić wsparcie i zasoby niezbędne do wdrożenia przyszłych planów — podkreśla Dariusz Gołębiewski z PZU LAB SA.

Ważnym aspektem jest zaangażowanie wszystkich działów w proces tworzenia planów awaryjnych. **Współpraca między działami pozwala na lepsze zrozumienie specyfiki działalności oraz identyfikację obszarów**, które wymagają szczególnej uwagi w sytuacjach kryzysowych.

Co więcej, organizacje powinny zapewnić, że plany awaryjne są zgodne z innymi politykami i procedurami wewnętrznymi. To oznacza, że powinny być one regularnie przeglądane i aktualizowane, aby odpowiadały zmieniającym się warunkom rynkowym oraz technologicznym.

— Regularnie przeprowadzana analiza ryzyk, aby zidentyfikować potencjalne zagrożenia dla działalności i dostosować plany do zmieniającego się otoczenia, jest niezbędna. Muszą być określone jasne kanały komunikacji dotyczące planów awaryjnych, aby wszyscy interesariusze mieli dostęp do informacji i wiedzieli, jak reagować w sytuacjach kryzysowych. **Przede wszystkim zalecam regularne testy planów awaryjnych (np. symulacje, ćwiczenia) co najmniej raz w roku.** To pomoże zidentyfikować luki i obszary do poprawy — przekonuje Dariusz Gołębiewski.

Niezbędne szkolenia

Kolejną praktyką jest szkolenie pracowników. Regularne ćwiczenia i symulacje pomagają pracownikom zrozumieć swoje role w sytuacjach kryzysowych oraz pozwalają na identyfikację luk w planach, które mogą wymagać poprawy. **Po każdym teście należy sporządzić raport podsumowujący wyniki** oraz rekomendacje dotyczące dalszych działań. Taki raport stanowi później cenne źródło informacji do ciągłego doskonalenia planów awaryjnych.

Wreszcie, organizacje powinny stosować podejście oparte na cyklu życia planu awaryjnego. Oznacza to, że plany powinny być nie tylko testowane, ale również regularnie aktualizowane w odpowiedzi na zmiany w otoczeniu biznesowym oraz technologii. Utrzymywanie planów w aktualnym stanie zapewnia ich skuteczność i gotowość na przyszłe wyzwania. ■

Ważnym aspektem jest zaangażowanie wszystkich działów w proces tworzenia planów awaryjnych. Współpraca między działami pozwala na lepsze zrozumienie specyfiki działalności oraz identyfikację obszarów, które wymagają szczególnej uwagi w sytuacjach kryzysowych.

Najważniejsze elementy skutecznego planu reagowania na incydenty

Jednym z najważniejszych kroków jest wyznaczenie zespołu reagowania na incydenty, ustalenie metod wykrywania incydentów (np. monitoring, systemy IDS) oraz zasad zgłaszania incydentów.

Niezbędne są procedury reagowania, opisujące szczegółowe kroki do podjęcia w przypadku różnych typów incydentów (np. ataki DDoS, wycieki danych), które powinny być regularnie testowane. Pracownicy muszą być też szkoleni oraz zaleca się przeprowadzanie symulacji incydentów, aby przetestować skuteczność planu.

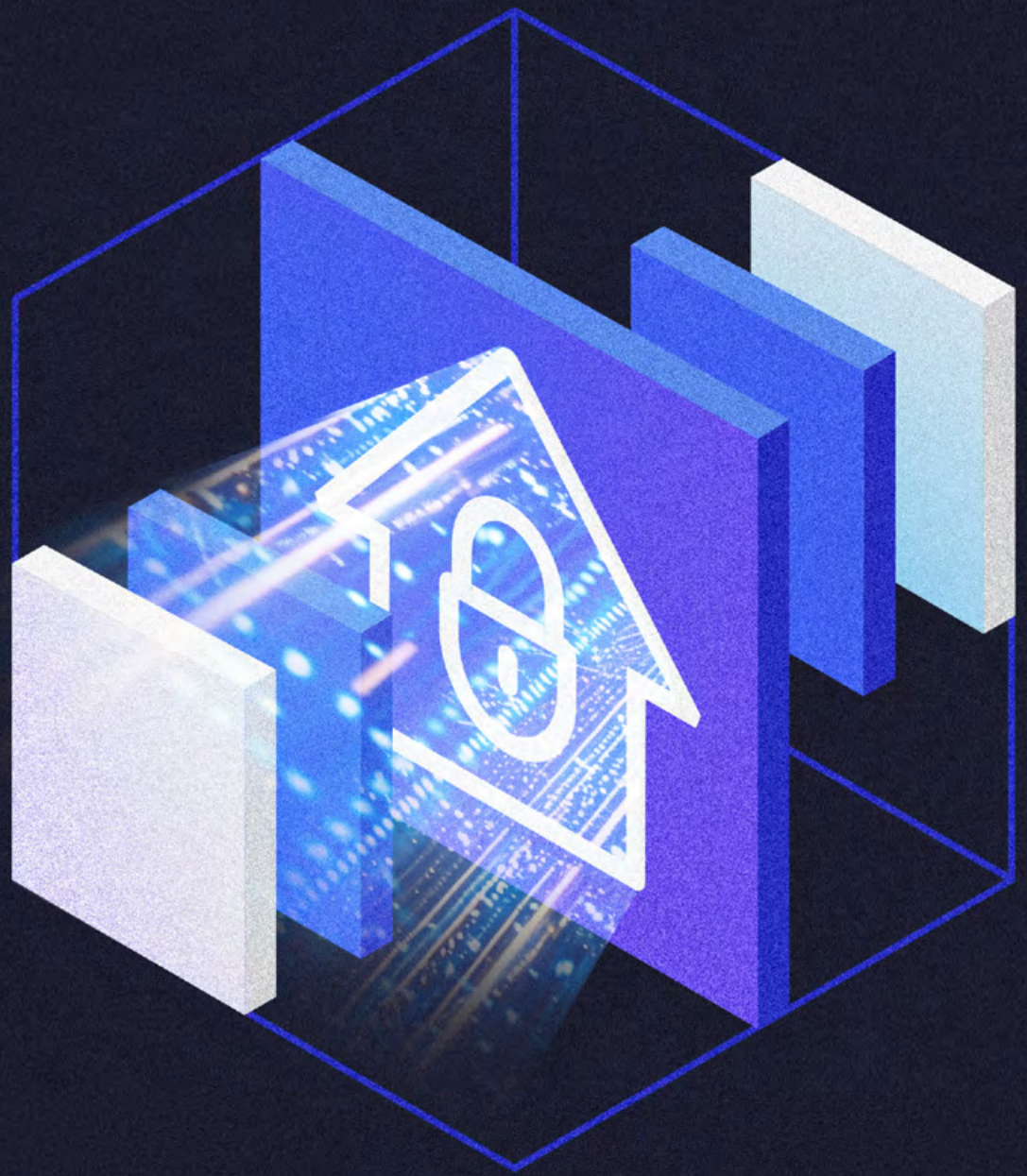
Jeżeli chodzi o praktyczne, kroki to istotne jest przeprowadzenie analizy ryzyka, pozwalającej na identyfikację potencjalnych zagrożeń. Ważne jest wprowadzenie odpowiednich zabezpieczeń technicznych (firewalle, szyfrowanie, aktualizacje) oraz stworzenie i wdrożenie polityk bezpieczeństwa dotyczących dostępu, używania danych i urządzeń. Następnie monitorowanie systemów i przeprowadzanie audytów bezpieczeństwa.

Biorąc pod uwagę ciągłość działania firmy, konieczne jest tworzenie kopii zapasowych danych, aby zminimalizować straty w przypadku ataku. Zaleca się nawiązanie współpracy z zewnętrznymi ekspertami ds. bezpieczeństwa w celu uzyskania wsparcia i wiedzy. Przygotowanie się na potencjalne ataki wymaga systematycznego podejścia i ciągłego doskonalenia planu reagowania na incydenty. Regularne aktualizacje i testowanie planu są zaś kluczowe, aby zapewnić skuteczność w obliczu zmieniających się zagrożeń. ■

Dariusz Gołębiewski,
prezes zarządu PZU LAB SA

8

Dyrektywa NIS 2 i jej wpływ na biznes



PZU

BUSINESS INSIDER

Dyrektywa NIS 2 i jej wpływ na biznes

Dyrektywa NIS2, czyli Network and Information Systems Directive 2, jest nową regulacją Unii Europejskiej. Ma na celu wzmocnienie poziomu cyberbezpieczeństwa w państwach członkowskich. Zastępuje ona wcześniejszą Dyrektywę NIS, która była pierwszym krokiem UE w kierunku ujednolicenia standardów bezpieczeństwa sieci i informacji.

Oto najważniejsze informacje na temat dyrektywy:

Cel dyrektywy NIS2
Dyrektywa NIS2 ma na celu ustanowienie podstawowych środków bezpieczeństwa dla podmiotów kluczowych i ważnych, ograniczenie ryzyka ataków cybernetycznych oraz poprawę ogólnego poziomu cyberbezpieczeństwa w Unii Europejskiej.

Nowe obowiązki dla firm
Firmy objęte dyrektywą NIS2 będą musiały identyfikować i kwantyfikować koszty, zasoby i usługi, a także prezentować możliwe ryzyka zarządowi. Będą również zobowiązane do raportowania incydentów bezpieczeństwa, co wymaga korzystania z efektywnych systemów wykrywania zagrożeń.

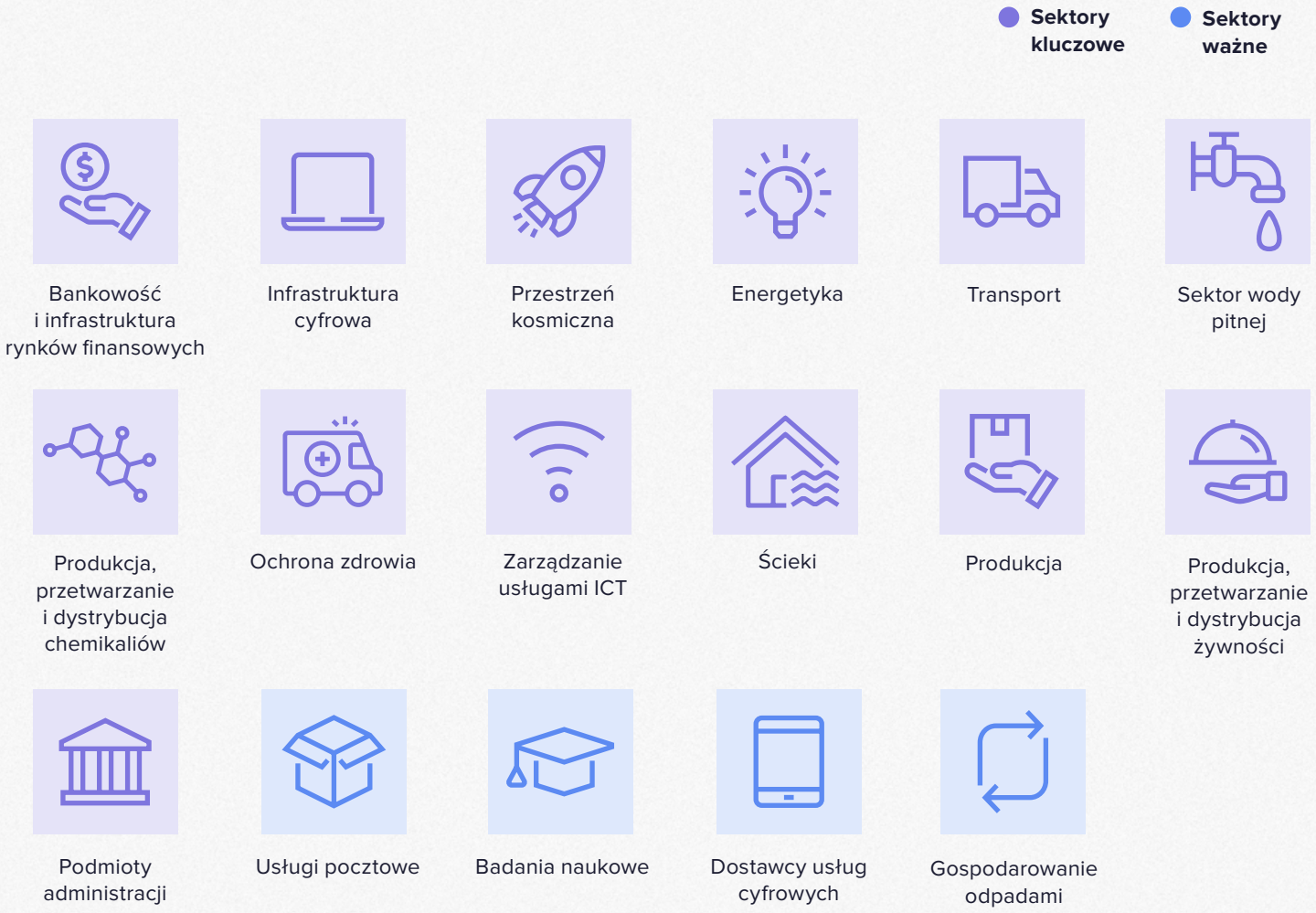
Wymóg świadomego zarządzania ryzykiem
Dyrektywa NIS2 wymaga od firm świadomego zarządzania ryzykiem, obejmującego identyfikację zagrożeń, wykrywanie i zgłaszanie incydentów oraz ich obsługę. W tym pomagają np. systemy SOC/SIEM.

Rozszerzenie zakresu podmiotów objętych dyrektywą
NIS2 rozszerza obowiązki dotyczące cyberbezpieczeństwa z 400 do 39 tys. firm i instytucji w Polsce, w tym w 18 kluczowych sektorach, takich jak zdrowie, żywność, energia czy transport. Dla wielu firm jest to nowa sytuacja, wymagająca dostosowania się do nowych regulacji.

Od kiedy ustawa zacznie obowiązywać?

Dyrektywa NIS2 weszła w życie 16 stycznia 2023 r., dając państwom członkowskim Unii Europejskiej czas na implementację jej postanowień do dnia 17 października 2024 r. Ze względu na dosyć dużą liczbę uwag, jaką otrzymało Ministerstwo Cyfryzacji, oraz sam proces legislacyjny, praktyczne uchwalenie nie nastąpi jednak wcześniej niż w drugim kwartale 2025 r. Spodziewany moment realnego wejścia w życie przepisów to jesień 2025.

Sektory kluczowe i ważne według NIS2



Co grozi za nieprzestrzeganie ustawy?

Podmiot kluczowy: maks. 10 mln euro lub 2 proc. przychodów osiąganych w roku obrotowym poprzedzającym kary. Kara nie może być niższa niż 20 tys. zł.

Podmiot ważny: maks. 7 mln euro lub 1,4 proc. przychodów osiąganych w roku obrotowym poprzedzającym kary. Kara nie może być niższa niż 15 tys. zł.

Konieczność szkoleń i audytów

Aby spełnić wymagania dyrektywy, firmy muszą przeprowadzać regularne audyty bezpieczeństwa, testy penetracyjne oraz szkolić kadrę kierowniczą i pracowników w zakresie cyberbezpieczeństwa. Pomocne mogą być tu centra doświadczeń cyberbezpieczeństwa i specjalistyczne szkolenia.

Wyższe wymagania dla dodatkowych sektorów

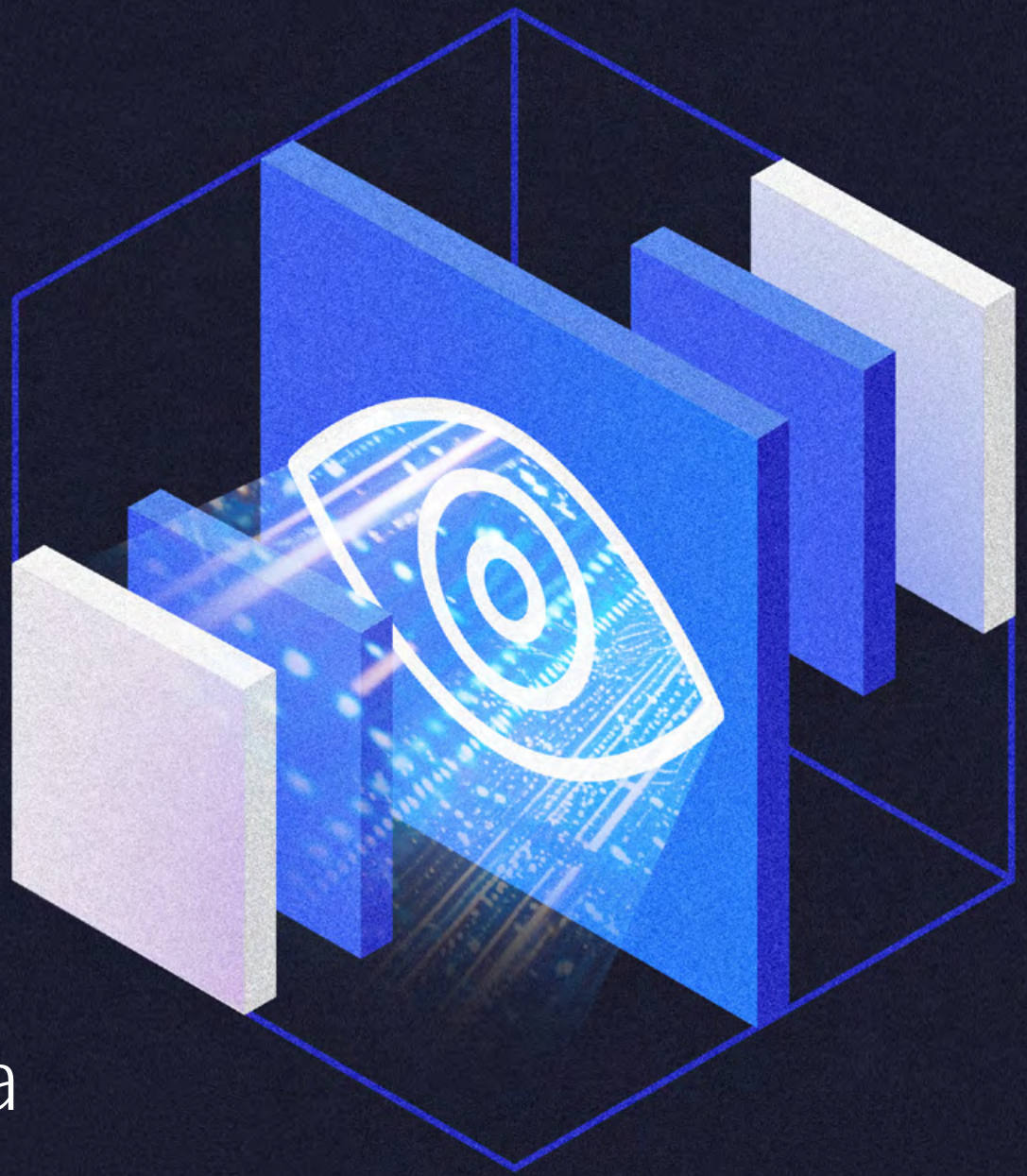
Polska planuje uznać dodatkowe sektory (np. chemiczny, żywnościowy, produkcyjny) za kluczowe, nakładając na nie surowsze wymagania niż przewiduje dyrektywa.

Bardzo wysokie kary

Projekt przewiduje bardzo wysokie kary finansowe za naruszenia, co może być nieproporcjonalne i prowadzić nawet do upadłości niektórych firm. Tym bardziej więc warto wdrożyć odpowiednie zabezpieczenia. ■

9

Przyszłość cyberbezpieczeństwa



PZU

BUSINESS INSIDER

10 trendów w cyberbezpieczeństwie na 2025 i kolejne lata

W nadchodzących latach Europa stanie przed wieloma wyzwaniami i trendami w obszarze cyberbezpieczeństwa. Na co powinniśmy się nastawić?

1 Wzrost liczby ataków i ich złożoności

Oczekuje się, że liczba cyberataków oraz przestępczości internetowej będzie nadal rosnąć, a ataki staną się coraz bardziej wyrafinowane. W 2025 r. na świecie ma być połączonych ok. 41 mld urządzeń w ramach Internetu rzeczy (IoT), co stwarza nowe możliwości dla cyberprzestępców.

2 Koszty cyberprzestępczości

Szacuje się, że koszty związane z cyberprzestępczością mogą osiągnąć 12 bln dolarów do 2025 r., co skłoni organizacje do zwiększenia inwestycji w zabezpieczenia.

3 Nowe strategie i regulacje

Unia Europejska wdraża nową strategię, która ma na celu zwiększenie odporności na zagrożenia cybernetyczne oraz zapewnienie, że obywatele i przedsiębiorstwa korzystają z zaufanych technologii cyfrowych. Kluczowe obszary obejmują regulacje, inwestycje oraz współpracę międzynarodową.

4 Budżety na cyberbezpieczeństwo

Wiele organizacji planuje zwiększenie budżetów na cyberbezpieczeństwo o 6-10 proc. w nadchodzących latach. Wzrost ten jest odpowiedzią na rosnące zagrożenia oraz potrzeby związane z ochroną danych.

5 Wzmocnienie cyberhigieny

Ludzki błąd pozostanie główną podatnością cyberbezpieczeństwa w 2025 r. i kolejnych latach. Przewiduje się, że phishing i inne ataki socjotechniczne pozostaną główną przyczyną naruszeń danych, a przeciętna firma będzie mierzyć się z ponad 700 takimi atakami rocznie. Aby temu przeciwdziałać, trzeba podwoić wysiłki w zakresie szkoleń i programów uświadamiających pracowników, promując kulturę silnej cyberhigieny.

6 Zmiana ze strategii reaktywnych na proaktywne

Organizacje będą coraz częściej polegać na systemach ciągłego monitorowania, aby identyfikować i usuwać luki w czasie rzeczywistym. Ponadto wykrywanie zagrożeń oparte na AI odegra istotną rolę w przewidywaniu i zapobieganiu atakom, zanim zdążą one wyrządzić krzywdę.

7 Architektura Zero Trust

Model bezpieczeństwa oparty na zasadzie „nigdy nie ufaj, zawsze weryfikuj" zyska na znaczeniu. Zero Trust będzie niezwykle ważnym elementem strategii ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi.

8 AI w cyberbezpieczeństwie

Sztuczna inteligencja będzie odgrywać ważną rolę w automatyzacji wykrywania zagrożeń oraz analizie dużych zbiorów danych. Jednak cyberprzestępcy również będą korzystać z AI — do tworzenia bardziej skomplikowanych ataków.

9 Bezpieczeństwo chmury

Oczekuje się, że 85 proc. firm przyjmie podejście „cloud-first" do 2025 r. To zwiększy zapotrzebowanie na zaawansowane rozwiązania zabezpieczające w środowiskach chmurowych.

10 Więcej oszustw deepfake

Ataki oparte na deepfake będą się rozprzestrzeniać, ponieważ są wykorzystywane do podszywania się pod dyrektorów, pracowników i osoby publiczne — nierzadko z dużą skutecznością. Technologia ta umożliwi oszukańcze działania, takie jak BEC (business email breach) i rozprzestrzenianie dezinformacji, potencjalnie manipulując rynkami i poważnie szkodząc niektórym organizacjom.

Źródła: Council of the European Union, Forrester, PwC

Przyszłość cyberbezpieczeństwa: na styku AI, kwantów i talentów

Przyszłość cyberbezpieczeństwa to niewątpliwie część szerszej perspektywy. Funkcjonujemy w supercyklu technologicznym, stąd też ewoluuje dynamika zagrożeń cybernetycznych. Dodatkowo obecna sytuacja geopolityczna intensyfikuje presję na systemy zabezpieczeń, generując znaczący wzrost wyrafinowanych ataków na infrastrukturę krytyczną. Ta nowa rzeczywistość wymaga holistycznego podejścia do cyberbezpieczeństwa, wykraczającego często poza tradycyjne rozwiązania i to właśnie tutaj należy szukać źródeł nowych trendów.

Widzimy już, że chociażby sztuczna inteligencja staje się coraz istotniejszym elementem nowoczesnych systemów ochrony. Zaawansowane modele AI mogą nie tylko wykrywać anomalie w czasie rzeczywistym, ale również przewidywać potencjalne wektory ataków. Z innych ciekawych zmian — rośnie wykorzystanie danych biometrycznych w cyberbezpieczeństwie. Bio-dane oferują nowy poziom ochrony tożsamości, ale rodzą pytania o prywatność i bezpieczeństwo tych informacji. Z drugiej strony rosnąca świadomość tego, że cyberbezpieczeństwo jest sprawą każdego użytkownika rozwija np. rynek cyber-ubezpieczeń, które ewoluują w kierunku kompleksowych produktów, dostępnych także dla klientów indywidualnych.

A co na dalszym horyzoncie? Na pewno poważne wyzwanie związane z erą kwantową. Perspektywa nadejścia „Q-Day", czyli momentu, w którym komputery kwantowe będą w stanie złamać obecne systemy kryptograficzne, wymusza już teraz długoterminowe strategie, np. takie jak inwestycje w kryptografię postkwantową (PQC). W tym złożonym krajobrazie kluczowa staje się rola wyspecjalizowanych talentów. Potrzebujemy ekspertów łączących głęboką wiedzę techniczną z umiejętnością strategicznego, a nawet kreatywnego myślenia. Z tej perspektywy przyszłość cyberbezpieczeństwa będzie opierać się głównie na budowaniu cyberodporności poprzez rozwój adaptacyjnych strategii wobec dynamicznie zmieniających się zagrożeń. ■

Monika Borycka
Obserwatorka trendów, analityczka innowacji technologicznych i specjalistka futures studies. Założycielka i CEO marki TrendRadar, pod szyldem której przybliża wiedzę o trendwatchingu i analizowaniu przyszłości, współautorka podcastu „Wycinki z przyszłości". Wykładowczyni, opiekunka merytoryczna studiów podyplomowych Trendwatching & Futures Studies na AGH. Współpracuje z firmami i organizacjami w zakresie analizy trendów i innowacji, pomagając im zrozumieć przyszłość i dobrze przygotować się na zmiany.

Monika Borycka, analityczka trendów, CEO TrendRadar

Czytaj więcej o cyberbezpieczeństwie

Twoje zdjęcia i dokumenty mogą trafić w niepowołane ręce. Udogodnienia AI vs prywatność

Czytaj →

Cyberbezpieczeństwo jako pilna sprawa dla firm. „Kiedyś cyberprzestępca musiał być specjalistą. Dziś wystarczy myszka i karta kredytowa”

Czytaj →

Nasilenie cyberataków w Polsce i na świecie. Oto jak zwiększyć bezpieczeństwo na smartfonie

Czytaj →

Redaktor prowadzący: Grzegorz Kubera
Skład graficzny: Serigala Tech

PZU

BUSINESS INSIDER