cloudware

Cyberbezpieczeństwo w Polsce.

RAPORT CLOUDWARE POLSKA

cloudware

Cyberbezpieczeństwo – sprawa najwyższej wagi

FOT. SHUTTERSTOCK

Chmura na ratunek firmom, sztuczna inteligencja szansą, ale i zagrożeniem, ochrona w modelu subskrypcyjnym – Cloudware Polska przygląda się stanowi cyberbezpieczeństwa w naszym kraju. Czy polscy przedsiębiorcy wiedzą, jak dbać o własne dane?

Cyberbezpieczeństwo to obecnie kluczowa kwestia, nie tylko w biznesie. Do tego stopnia, że coraz częściej pojawia się nawet w rządowej agendzie. W drugiej połowie 2024 roku, podczas wystąpienia na „Kongresie Bezpieczeństwo Polski", wicepremier i minister cyfryzacji Krzysztof Gawkowski zapowiedział, że Polska w latach 2025-2026 wyda na cyberbezpieczeństwo ok. 10 mld zł. Polityk zaznaczył jednocześnie, że nasz kraj jest w czołowej piątce państw najlepiej przygotowanych do działań defensywnych w cyberprzestrzeni.

Są więc pewne przesłanki, że na przyszłość można patrzyć z nadzieją, biznesowi wciąż jednak daleko do optymizmu.

Z najnowszego badania KPMG aż 66 proc. polskich firm doświadczyło w ostatnim roku co najmniej jednego cyberatatku, a średni koszt naruszenia bezpieczeństwa danych dla organizacji w Polsce wynosi ponad 4 mln zł.

Eksperci cybersecurity przekonują, że przedsiębiorcy nie powinni próbować odpowiedzieć sobie na pytanie „Czy zostaniemy zaatakowani", lecz „Kiedy zostaniemy zaatakowani" (oczywiście przy optymistycznym założeniu, do incydentu nie doszło już w przeszłości".

– Od wybuchu pandemii COVID-19 aktywność cyberprzestępców znacząco wzrosła. Powszechna stała się praca zdalna, częściej korzystamy ze sprzętu firmowego - również do celów prywatnych - więc staliśmy się łatwiejszym celem dla hakerów. Jestem przekonany, że cyberbezpieczeństwo będzie kluczowym tematem w nadchodzących miesiącach, ponieważ musimy budować świadomość nie tylko wśród przedsiębiorców – przekonuje Łukasz Kuflewski, architekt, projektant i deweloper dostępu w Cloudware Polska.

Z cyberatakami mierzą się przede wszystkim małe i średnie przedsiębiorstwa, których nie stać nie tylko na inwestycję w nowoczesne narzędzia cyberbezpieczeństwa, jak również w wykwalifikowanych ekspertów IT. Ze statystych organizacji ISC2 – zajmującej się m.in. szkoleniami z zakresu cyberbezpieczeństwa – wynika, że na całym świecie może brakować ponad 4 mln specjalistów, którzy zajęliby się ochroną firmowych zasobów.

Więcej danych? Raport „Cyberskills" dowodzi, że aż 39 proc. polskich firm nie zatrudnia ani jednego pracownika odpowiedzialnego za cyberbezpieczeństwo. Jednego pracownika odpowiedzialnego za cyfrowe bezpieczeństwo zatrudnia 45 proc. firm, a dwóch do trzech pracowników zatrudnia 8 proc. przedsiębiorstw. Najmniej firm bez żadnego specjalisty jest w Luksemburgu (co piąta), a najwięcej w Bułgarii (65 proc.). Dodatkowym problemem są niskie kwalifikacje tych osób.

Sporo unijnych firm pozyskuje swoich specjalistów ds. cyberbezpieczeństwa w ramach wewnętrznej rekrutacji lub zmian organizacyjnych. Największą grupę pracowników odpowiedzialnych za cyfrowe bezpieczeństwo stanowią pracownicy, którzy zostali wchłonięci do tej roli z innego stanowiska w organizacji – dzieje się tak w 53 proc. polskich firm (wobec 57 proc. w UE). Zaledwie co dziesiąty specjalista ds. cyberbezpieczeństwa w polskiej firmie to osoba, która wcześniej specjalizowała się w tym obszarze (wobec średniej 18 proc. w całej UE).

Sytuacji nie sprzyja fakt, że - jak tłumaczą specjaliści Cloudware Polska - wielu przedsiębiorcom w Polsce wciąż wydaje się, iż w organizacji wystarczy wdrożyć jeden system bądź jedno rozwiązanie, które ochroni ich przed wszystkimi zagrożeniami. - Infrastruktura firm jest zwykle na tyle rozbudowana, że na cybersecurity należy patrzeć kompleksowo. Ochrona przed hakerami to długotrwały proces, a nie jednorazowe wdrożenie - dodaje Kuflewski.

cloudware

Nie ufaj nikomu – cyberbezpieczeństwo w strategii zero trust security

FOT. SHUTTERSTOCK

Choć pojęcie zero trust security wciąż budzi niemałe dyskusje w branży, wydaje się, że ta strategia ma znacznie więcej przeciwników niż zwolenników. Ci drudzy twierdzą, że wdrożenie do przedsiębiorstwa takiej polityki wiąże się z nakładami finansowymi, jakim mogą sprostać wyłącznie najwięksi gracze. Uważają, że to skomplikowany proces, na który stać nielicznych. Zdaniem zwolenników zero trust to jednak bardzo powierzchowne myślenie, szkodliwe dla organizacji, które patrzą na cyberbezpieczeństwo wyłącznie pod kątem kosztów. Poza tym na rynku działa mnóstwo firm technologicznych – takich jak Cloudware Polska – które pomagają efektywnie kosztowo wdrożyć rozwiązania z zakresu cyberbezpieczeństwa.

Zero trust security to model bezpieczeństwa oparty na braku zaufania. Zwolennicy tej koncepcji przekonują, iż nawet za korporacyjnymi zaporami nikt nie jest bezpieczny, a każdy użytkownik, sprzęt czy też adres IP uzyskujące dostęp do zasobu – np. danych – stanowi potencjalne zagrożenie. Co to oznacza w praktyce? W dużym skrócie tyle, że działy odpowiedzialne za cyberbezpieczeństwo powinny otrzymać niezbędne narzędzia pozwalające na kontrolę dostępu, a także weryfikację tego, co (lub kto) próbuje połączyć się z siecią przedsiębiorstwa.

W modelu zero trust każde żądanie dostępu – zanim zostanie przyznane – musi zostać odpowiednio uwierzytelnione,

zautoryzowane i zaszyfrowane. Nie jest istotne, skąd łączy się użytkownik, ponieważ firma przyjmuje, że w każdym momencie może dojść do próby cyberataku. Dlatego właśnie podstawą koncepcji zero trust są silne polityki bezpieczeństwa, oparte chociażby na wieloskładnikowym uwierzytelnianiu.

Niemałe znaczenie w kontekście popularazycji koncepcji zerowego zaufania miał rozwój rozwiązań chmurowych. Obecnie trudno wyobrazić sobie prowadzenie biznesu bez całodobowego dostępu do skrzynki mailowej, wglądu do istotnych systemów firmy podczas wizyty u klienta czy możliwości sprawnej organizacji zdalnego spotkania, np. z zespołem. Coraz trudniej wskazać branżę, w której w ostatnich miesiącach chmura nie odegrała ważnej roli.

Jak wskazują dane, zainteresowanie rozwiązaniami chmurowymi szybko rośnie. Wybierają je zarówno przedsiębiorcy będący w trakcie cyfrowej transformacji, jak i ci, którzy dopiero rozpoczanają digitalizację. Oczywiście jednych i drugich kuszą te same korzyści – chmura to przede wszystkim oszczędności, optymalizacja firmowych procesów oraz sygnał, że organizacja dba o ekologiczny wymiar swoich działań, ponieważ według ekspertów technologia chmurowa może niwelować pozostawiany przez przedsiębiorstwo ślad węglowy nawet o 90 proc. W czasach, kiedy konsumenci wybierają marki zgodnie z własnymi przekonaniami, takie aspekty są na tyle istotne, że na ich podstawie można budować przewagę konkurencyjną.

Choć chmura to liczne korzyści, wiąże się także z zagrożeniami. Z badania IBM pt. „Cost of a Data Breach Report 2022” wynika, iż 45 proc. cyberincydentów w organizacjach dotyczyło właśnie chmury. Wdrażanie tej technologii generuje kolejne dane, o które trzeba odpowiednio zadbać. Jednocześnie nie ma co ukrywać, że im więcej powstaje zabezpieczeń, tym bardziej chcą je złamać cyberprzestępcy.

Usługi świadczone w chmurze stały się nieodzownym elementem nowoczesnych organizacji. Rozwój i szersza dostępność oprogramowań SaaS ułatwiły menedżerom efektywniejsze planowanie budżetów przy równoczesnym zwiększaniu skali działalności. Coraz więcej przedsiębiorców korzysta już wyłącznie z tego typu usług, a w ich skład wchodzą nie tylko narzędzia ułatwiające sprzedaż, ale także np. systematyzujące komunikację wewnątrz organizacji. Przedsiębiorcy odważnie inwestujący w chmurę, odważnie inwestują także w rozwiązania SaaS - przede wszystkim zaufanych dostawców.

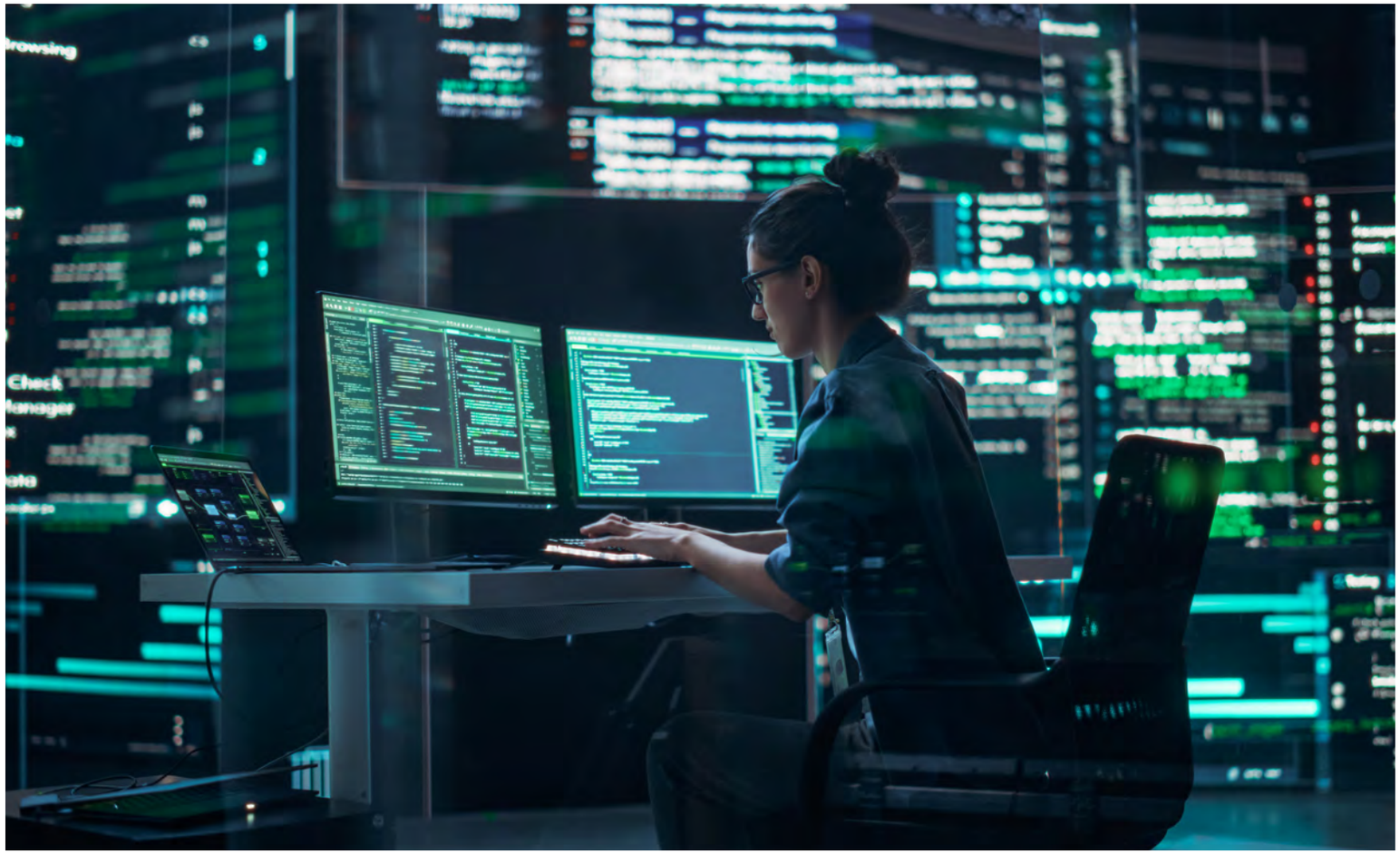
45%

cyberincydentów w organizacjach dotyczy chmury

BADANIA IBM „COST OF A DATA BREACH REPORT 2022

cloudware

Bezpieczeństwo jako usługa



FOT. SHUTTERSTOCK

Rosnące znaczenie usług Saas również w kontekście dbania o cyberbezpieczeństwo firmy to bardzo ciekawe zjawisko – branżowi eksperci już teraz przewidują, że przyszłość tego obszaru będzie coraz szybciej zmierzać w kierunku oferowania usług, a nie sprzedaży pojedynczych programów czy sporadycznych działań.

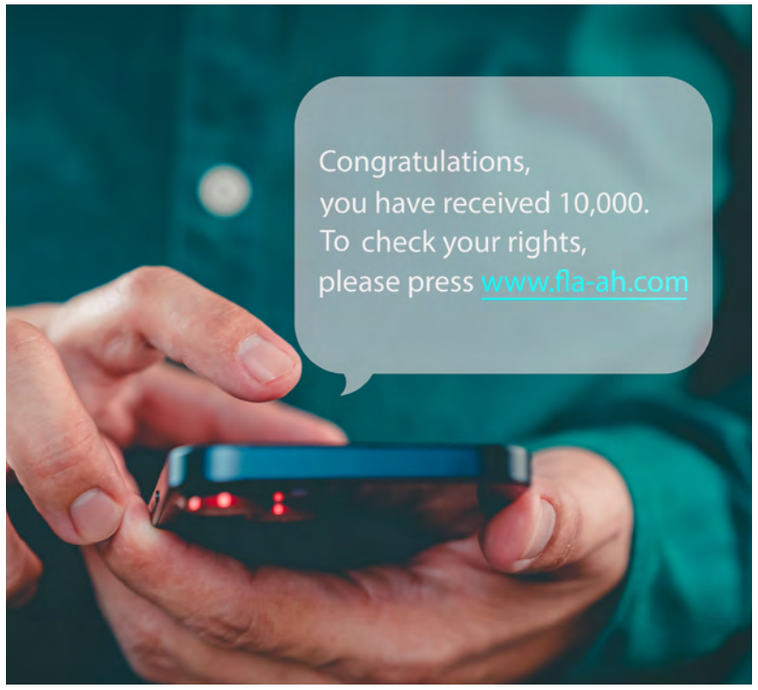
W modelu subskrypcyjnym to zewnętrzny podmiot dba o cyfrowe bezpieczeństwo naszej organizacji – wykrywa m.in. złośliwe aktywności w infrastrukturze, a także wszelkie cyberincydenty. Taka współpraca pozwala nie tylko zapobiegać atakom, ale także szybko reagować, jeśli już do takowych dojdzie.

I choć eksperci przewidują, że współpraca w takim modelu stanie się wkrótce dominująca w wielu przedsiębiorstwach, nie można rezygnować z innych działań. Jednym z podstawowych powinno być zdefiniowanie właściwej polityki bezpieczeństwa IT.

Procedury powinny być jak najbardziej precyzyjne i jednoznaczne. Każdy pracownik powinien wiedzieć, co musi, a czego nie wolno mu robić (np. nigdy nie używaj tego samego hasła do wielu aplikacji, nie korzystaj z nieszyfrowanych sieci Wi-Fi, nie udostępniaj nikomu firmowego sprzętu, sprawdzaj, czy strona, na którą wchodzisz, ma połączenie szyfrowane, nie

klikaj w podejrzane linki, korzystaj z zasady uwierzytelnienia dwustopniowego itd.), a urządzenie być odpowiednio zabezpieczone i monitorowane. Ważnym elementem polityki bezpieczeństwa jest też plan reagowania na incydenty i szybkiego naprawiania szkód wywołanych atakiem. Zespół powinien go znać i rozumieć, wiedzieć, do kogo się zgłosić w razie utraty firmowego sprzętu czy podejrzeń naruszenia bezpieczeństwa, bez względu na porę czy dzień tygodnia. Szybka reakcja pozwoli zapobiec atakowi lub go zatrzymać, zanim rozprzestrzeni się po całej sieci i wyrządzi poważne szkody.

Im większą wiedzę mają pracownicy, tym skuteczniej potrafią się ochronić. Nie chodzi tu oczywiście o to, by wszyscy dorównywali poziomem najlepszym specjalistom z branży cybersecurity, ale by wiedzieli, jak chronić narzędzia, którymi się posługują, bezpiecznie poruszać się w sieci i nie dać się nabrać na wszelkiego rodzaju próby wyciągnięcia cennych danych. Phishing, spoofing, malware, ransomware, korzystanie z niezaufanych sieci Wi-Fi, posługiwanie się łatwymi do złamania hasłami, korzystanie z niezaufanych urządzeń podpinanych pod USB, sposoby gromadzenia i przechowywania danych i konsekwencje ich utraty to tylko niektóre z długiej listy zagadnień, które trzeba poruszyć.



FOT. SHUTTERSTOCK

Obszarem, który z pewnością może być pomocny dla przedsiębiorców są testy penetracyjne, czyli skanowanie środowiska firmy pod kątem podatności na cyberataki. Tego typu rozwiązania imitują działania prawdziwych hakerów – próbują zaatakować struktury organizacji – dzięki czemu można ocenić, które obszary wymagają działań w pierwszej kolejności. To nic innego, jak kompleksowy audyt.

PODSTAWOWE ZASADY BEZPIECZENSTWA IT

- **Nigdy nie używaj tego samego hasła do wielu aplikacji,**
- **Nie korzystaj z nieszyfrowanych sieci Wi-Fi,**
- **Nie udostępniaj nikomu firmowego sprzętu,**
- **Sprawdzaj, czy strona, na którą wchodzisz, ma połączenie szyfrowane,**
- **Nie klikaj w podejrzane linki,**
- **Korzystaj z zasady uwierzytelnienia dwustopniowego**

cloudware

Sztuczna inteligencja pomoże ci się chronić

Sztuczna inteligencja staje się nieodzownym narzędziem w arsenale firm dążących do zapewnienia sobie najwyższego poziomu cyberbezpieczeństwa. AI stanowi już 59 proc. wszystkich patentów cybernetycznych i należy do najpopularniejszych przedmiotów badań związanych cyberbezpieczeństwem od 2017 roku. Jednak na kwestiach ochrony zasobów firm jej potencjał się nie kończy.

FOT. SHUTTERSTOCK

Postępy w dziedzinie głębokiego uczenia i sieci neuronowych umożliwiają sztucznej inteligencji analizowanie większych i bardziej zróżnicowanych zbiorów danych w czasie rzeczywistym. Zdolność do samokształcenia przyspiesza automatyzację, pomagając zespołom cybernetycznym w ciągłym monitorowaniu sieci i aplikacji, a także wykrywaniu oraz prognozowaniu zagrożeń w czasie zbliżonym do rzeczywistego. Oznacza to szybsze reagowanie na incydenty.

Innym aspektem, przed którym chroni wysoki poziom obrony cybernetycznej, są przestoje w działalności operacyjnej i straty finansowe w wyniku wirtualnych ataków. Sztuczna inteligencja, która analizuje systemy i zachowania użytkowników w czasie rzeczywistym, minimalizuje ryzyko ich wystąpienia. Mniejsza liczba incydentów oznacza także płynniejszą działalność i lepszą obsługę klientów.

Patrzmy w przyszłość

Podejście do cyberbezpieczeństwa musi ewoluować, ponieważ zmieniają się również zagrożenia. Sami eksperci ds. cyberbezpieczeństwa mówią o tym, jak sprawnymi grupami przestępczymi stali się hakerzy, nie mający już w zasadzie żadnych skrupułów – powszechne stały się chociażby przekręty związane z fałszywymi zbiórkami na chore dzieci. Bezwzględność i cynizm, niestety, nie mają granic.

Jednocześnie – jak przewidują obserwatorzy rynku pracy – jeszcze powszechniejsza stanie się praca hybrydowa. Już teraz służbowy sprzęt wykorzystujemy także do celów prywatnych, co rodzi kolejne wyzwania po stronie pracodawcy. Co z tego, że w biurze jesteśmy skutecznie chronieni przed cyberzagrożeniami, skoro po odłączeniu od firmowych systemów i po powrocie do domu, stajemy się narażeni np. na ataki phishingowe? Hybrydowy model pracy wymusza jeszcze większą kompleksowość w działaniu zespołów ds. cyberbezpieczeństwa każdego podmiotu.

Gigantyczne znaczenie w ochronie organizacji będzie miało skupienie się na firmowych danych, które stają się najcenniejszą, najstabilniejszą walutą. Samo agregowanie danych już dawno przestało być wartością dla przedsiębiorstwa, obecnie – by zdobyć bądź utrzymać przewagę konkurencyjną – trzeba je właściwie analizować. To nie będzie możliwe, jeśli nie zadbamy odpowiednio o ich bezpieczeństwo. Warto pamiętać, że każdy wyciek danych to nie tylko potencjalne duże straty finansowe dla firmy, ale także wizerunkowe. Współcześnie raz utracone zaufanie bardzo trudno odzyskać.

W przypadku cyberprzestępczości działa zjawisko skali – hakerom łatwiej złowić kilka mniejszych rybek w wielką sieć, niż gigantycznego wieloryba na wędkę. Nikt nie jest bezpieczny, a twierdzenie, że na cyberataki narażone są przede wszystkim największe instytucje finansowe, to w najmniejszym stopniu przejaw ignorancji. Skupienie się na skali nie oznacza jednak, że spadnie liczba ściśle targetowanych ataków – eksperci od cyberbezpieczeństwa zauważają, że np. poprzez współpracę z byłymi pracownikami danych firm, chcącymi oczernić byłego pracodawcę, nasilą się incydenty wymierzone w konkretne przedsiębiorstwa. Przed takimi atakami bardzo trudno się obronić, a bez wsparcia doświadczonych partnerów technologicznych – i oferowanych przez nich rozwiązań z zakresu cyberbezpieczeństwa – może to być wręcz niemożliwe.

Nigdy nie będziemy w pełni bezpieczni – nawet po wdrożeniu najnowocześniejszych zabezpieczeń – zwłaszcza, że najsłabszym ogniwem każdej organizacji zawsze jest człowiek. Jednak poświęcając należytą uwagę cyberbezpieczeństwu, znacząco obniżamy ryzyko związane z potencjalnymi atakami.

E-book powstał przy współpracy z Hewlett Packard Enterprise

Hewlett Packard Enterprise

cloudware

Specjaliści w łączeniu
technologii z biznesem.

Skontaktuj się z nami!

Grzegorz Gołda
Dyrektor Sprzedaży