CRÉDIT AGRICOLE
EFL LEASING

Z korzyścią dla Twojego biznesu

RAPORT SPECJALNY EFL

CYBERBEZPIECZEŃSTWO W FIRMIE. JAK O NIE ZADBAĆ?

WPROWADZENIE

Potencjalne zagrożenie dotyczy wszystkich przedsiębiorców, jednak aż 47 procent cyberataków jest wymierzonych w firmy średniej wielkości – wynika z raportu „Internet Complaint Center w FBI".

W małych i średnich przedsiębiorstwach nie poświęca się zbyt wiele czasu na edukowanie pracowników zarówno w zakresie ochrony urządzeń, jak i zabezpieczenia znajdujących się na nich danych. Mniejsze firmy często mają też problem z odpowiednim rozwojem systemów zabezpieczeń i dostosowaniem ich do nieustannie rosnącej liczby zagrożeń. Nie mają odpowiedniego budżetu na utrzymanie etatu wykwalifikowanych specjalistów ds. bezpieczeństwa.

Jak swoją cyberodporność oceniają polscy przedsiębiorcy? Jakie ataki grożą firmom? I jakie wyzwania stoją przed biznesem w przyszłości? Zapraszamy do lektury raportu!

RODZAJE INCYDENTÓW

Aż jedna trzecia firm działających w Polsce odnotowała wzrost intensywności cyberataków na swoje systemy. Jak podaje CERT, pierwszy polski zespół ds. monitorowania zagrożeń cyberbezpieczeństwa na poziomie krajowym, działający w strukturach NASK, w ubiegłym roku odnotowano 39 683 zgłoszonych incydentów. Rok wcześniej – 29 483.

Jako cyberzagrożenia stanowiące największe ryzyko dla organizacji wskazywane są[1]:

- wyłudzanie poufnych informacji, najczęściej danych uwierzytelniających (phishing),
- zaawansowane, długotrwałe i zazwyczaj ukierunkowane ataki, które najczęściej pozostają niewykryte przez długi czas (Advanced Persistent Threat, APT),
- wycieki danych za pośrednictwem złośliwego oprogramowania (malware),
- kradzież danych przez pracowników,
- kampanie ransomware (ransom – okup, ware – od software), które blokują dostęp do systemów komputerowych i najczęściej są powiązane z próbą uzyskania okupu za przywrócenie stanu pierwotnego zaszyfrowanych danych,
- ataki wykorzystujące błędy w aplikacjach,
- wyciek danych w wyniku kradzieży lub zgubienia nośników czy urządzeń mobilnych,
- ataki typu „odmowa usługi” (DoS/DDoS), które polegają na przeciążeniu aplikacji lub usługi w celu złośliwego jej zatrzymania,
- kradzież danych na skutek naruszenia bezpieczeństwa fizycznego,
- podsłuchiwanie ruchu i ataki Man-in-the-Middle (MitM), polegające na modyfikowaniu wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy,
- ataki na sieci bezprzewodowe,
- włamania do urządzeń mobilnych.

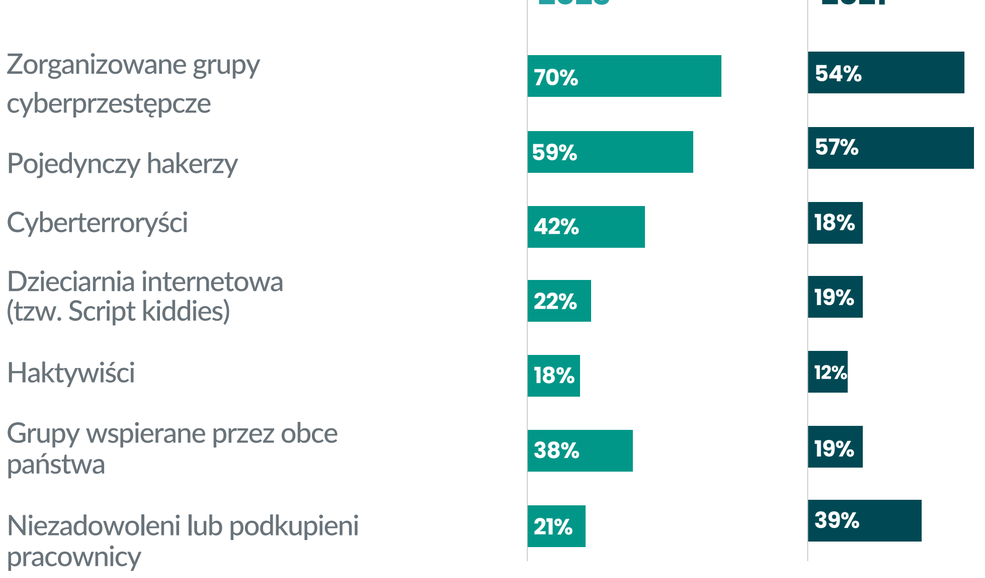
[1] Źródło: „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu", KPMG, 2023.

GŁÓWNE ŹRÓDŁA CYBERATAKÓW

Według większości przedsiębiorców największe zagrożenie stanowią zorganizowane grupy, które specjalizują się w cyberprzestępczości, a także hakerzy. Względem ubiegłych lat znacznie zmniejszyło się grono odczuwające zagrożenie ze strony pracowników, zwłaszcza tych niezadowolonych – z 39 procent w 2021 roku do 21 procent w 2023 roku.

Z kolei rosyjska inwazja na Ukrainę wpłynęła na większe obawy przed niebezpieczeństwem wynikającym z aktywności grup finansowanych przez obce państwa, w tym działania wspierane przez rosyjski i białoruski rząd. Tuż po rozpoczęciu ataku, w związku z realnym zagrożeniem w przestrzeni cyfrowej, na terenie Polski wprowadzono CHARLIE–CRP. To trzeci z czterech stopni alarmowych, które zostały określone w ustawie o działaniach antyterrorystycznych w cyberprzestrzeni.

Grupy stanowiące realne zagrożenie dla organizacji



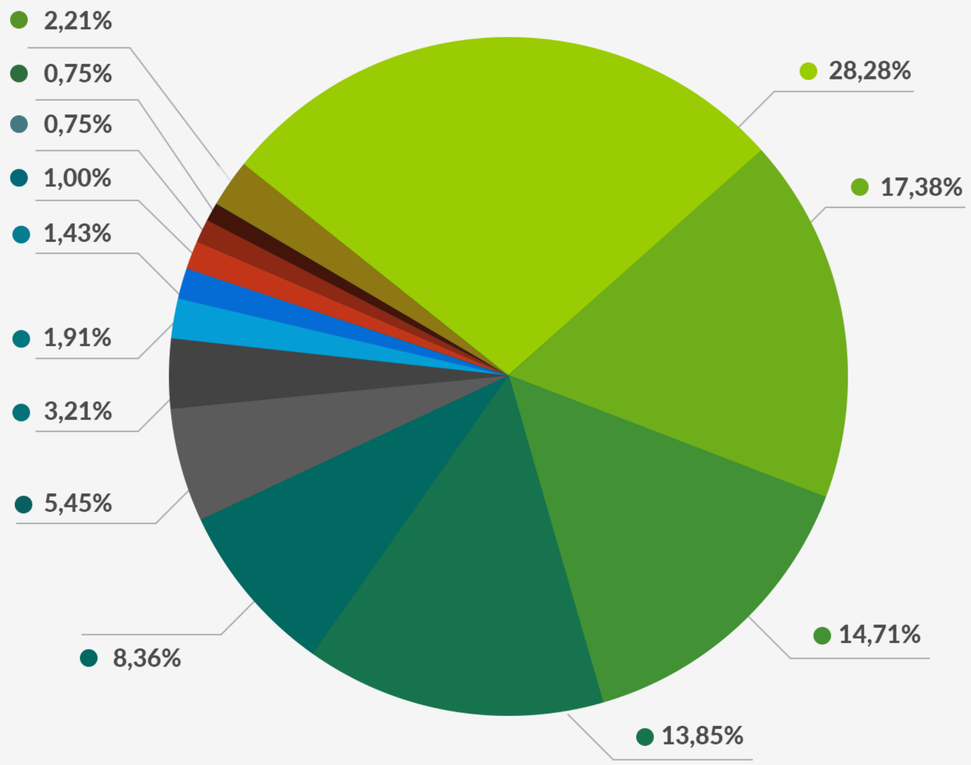
Źródło: „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu", KPMG, 2023

PODMIOTY NARAŻONE NA CYBERATAKI

Czy istnieją branże, które nie muszą obawiać się ataków w przestrzeni cyfrowej? Niestety nie. Jak pokazują dane zgromadzone przez CERT, większość kluczowych sektorów narażonych jest na cyberataki. Celem może być bowiem wszystko: dane pracowników lub klientów, know-how, zasoby informatyczne, mienie, dobry wizerunek organizacji, jak i dowolna przewaga rynkowa przedsiębiorstwa.

Najwięcej incydentów odnotowano w czterech sektorach. Są to: media, handel hurtowy i detaliczny, poczta i usługi kurierskie, energetyka.

Sektory gospodarki narażone na cyberataki



Źródło: „Cyberbezpieczeństwo – wyzwania dla biznesu", Pracodawcy Rzeczypospolitej Polskiej, 2023

ZAGROŻENIA DLA ORGANIZACJI

Ataki wymierzone w infrastrukturę firmową mogą nieść za sobą wiele negatywnych skutków. Wśród nich najczęściej wskazuje się[1]:

- problem z zapewnieniem ciągłości działania firmy,
- utratę przewagi rynkowej,
- straty finansowe,
- naruszenie zasad zawartych w umowach z kontrahentami,
- ujawnienie informacji poufnych,
- utratę danych,
- szkody materialne (np. uszkodzenie serwerów),
- konieczność zakupu dodatkowych zabezpieczeń i nowych urządzeń,
- niekorzystny wpływ na wizerunek przedsiębiorstwa.

[1] Źródło: „Cyberbezpieczeństwo – wyzwania dla biznesu", Pracodawcy Rzeczypospolitej Polskiej, 2023.
[2] „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu" KPMG, 2022.

Nawet 10% przedsiębiorstw, które w przeszłości doświadczyły cyberataku, od tego czasu nie zmieniło niczego w podejściu ich organizacji do zapewnienia bezpieczeństwa[2].

CRÉDIT AGRICOLE
EFL LEASING

LEASING Z KORZYŚCIĄ DLA CIEBIE I ŚRODOWISKA

Poczuj moc oszczędności, którą wytworzysz dzięki fotowoltaice, pompie ciepła i magazynowi energii w leasingu EFL.

TURBINY POLSKIEJ GOSPODARKI 2023

Materiał informacyjny kierowany wyłącznie do osób i podmiotów prowadzących działalność gospodarczą.
Ma charakter informacyjny i nie stanowi oferty w rozumieniu art. 66 k.c.

BEZPIECZEŃSTWO URZĄDZEŃ CYFROWYCH

Urządzenia cyfrowe towarzyszą nam na co dzień. Korzystamy z nich również w sytuacjach zawodowych, jednak nie zawsze są odpowiednio zabezpieczone – chociażby w zapory i programy antywirusowe. Odgrywają w naszym życiu bardzo ważną rolę, dlatego musimy pamiętać, by korzystać z nich odpowiedzialnie.

Jak ochronić swoje urządzenie przed cyberprzestępcami?

- korzystaj z systemów antywirusowych,
- używaj managera haseł, który umożliwia przechowywanie ich w bezpieczny sposób,
- w aplikacjach i różnych serwisach stosuj różne i silne hasła; nie wykorzystuj tych samych haseł w systemach firmowych i życiu prywatnym,
- korzystaj z uwierzytelnienia dwuskładnikowego lub wieloskładnikowego,
- pobieraj aplikacje tylko z autoryzowanych sklepów,
- sprawdzaj certyfikaty oprogramowania – potwierdzają bezpieczeństwo i funkcjonalność danych programów,
- pamiętaj o tworzeniu kopii zapasowych,
- rozważ szyfrowanie dysków firmowych,
- wykorzystuj VPN, czyli wirtualną sieć prywatną,
- urządzenia ładuj tylko własnymi ładowarkami i powerbankami,
- regularnie aktualizuj system operacyjny i zainstalowane aplikacje,
- zwiększaj świadomość cyberbezpieczeństwa w swojej organizacji.

[1] Urząd Komunikacji Elektronicznej – https://www.uke.gov.pl/akt/badanie-klientow-instytucjonalnych-przeprowadzone-w-2022-roku,471.html

W 2022 roku ponad 70 procent przedsiębiorców korzystało z dostępu mobilnego w telefonie komórkowym, a 44 procent na laptopie lub innym urządzeniu przenośnym[1].

ILE WIE O TOBIE SAMOCHÓD

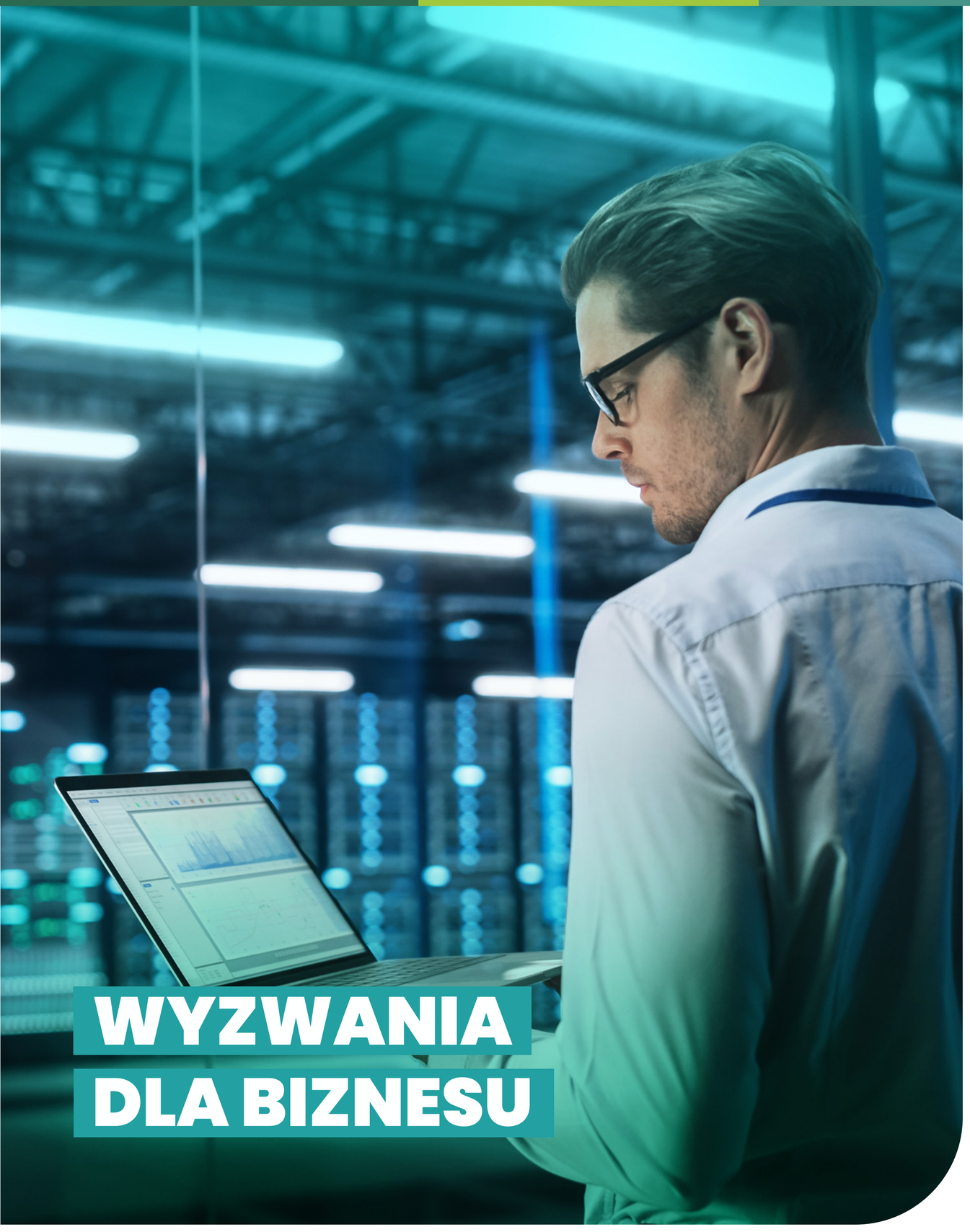
Od lat branża automotive czerpie z nowych technologii, a pojazdy, którymi się poruszamy, wyposażone są w szereg urządzeń elektronicznych, w większości połączonych z siecią. Dają więc hakerom szansę na uzyskanie poufnych danych oraz uzyskanie dostępu do funkcjonalności samochodu. A czy zdajemy sobie sprawę z tego, ile informacji gromadzi o nas chociażby komputer pokładowy?

Cyberprzestępcy najczęściej atakują systemy alarmowe, ułatwiając tym samym fizyczny dostęp do samochodu, a także nawigację – mogą w ten sposób wykraść nasze dane adresowe, informacje o stylu jazdy i regularnie pokonywanych trasach. Ingerują również w systemy komunikacji, chociażby poprzez zmianę ustawienia lusterek, wyłączenie wspomagania kierownicy lub kamery cofania.

Samochody należące do firmowej floty muszą być też przygotowane na potencjalne ataki z wykorzystaniem złośliwego oprogramowania ransomware. Umożliwia ono szyfrowanie dostępnych danych, wpływając tym samym na bezpieczeństwo kierowców.

Warto wspomnieć, że najczęstszym sposobem kradzieży nowych samochodów stała się tak zwana metoda „na walizkę”. Polega na przechwyceniu sygnału radiowego, wysyłanego w kierunku auta przez kluczyk. Wymaga jednak koordynacji dwóch osób – wyposażonego we wzmacniacz sygnału przestępcy, który znajduje się w okolicy kierowcy samochodu, który posiada oryginalny kluczyk, a także osoby, która skanuje sygnał i znajduje się jak najbliżej tego pojazdu.

Wyzwanie stanowią również pojazdy autonomiczne. Na świecie znane są już przypadki przejęcia kontroli nad nimi przez nieupoważnione osoby. Pojazdy te wyposażane są jednak coraz to lepsze technologie, które zwiększają ich bezpieczeństwo – chociażby w oparte na chmurze i sztucznej inteligencji silniki detekcyjne do zdalnego wykrywania cyberataków. W celu wykrywania zagrożeń związanych z interfejsem radiowym i radarami, stosuje się w nich również techniki uczenia maszynowego.

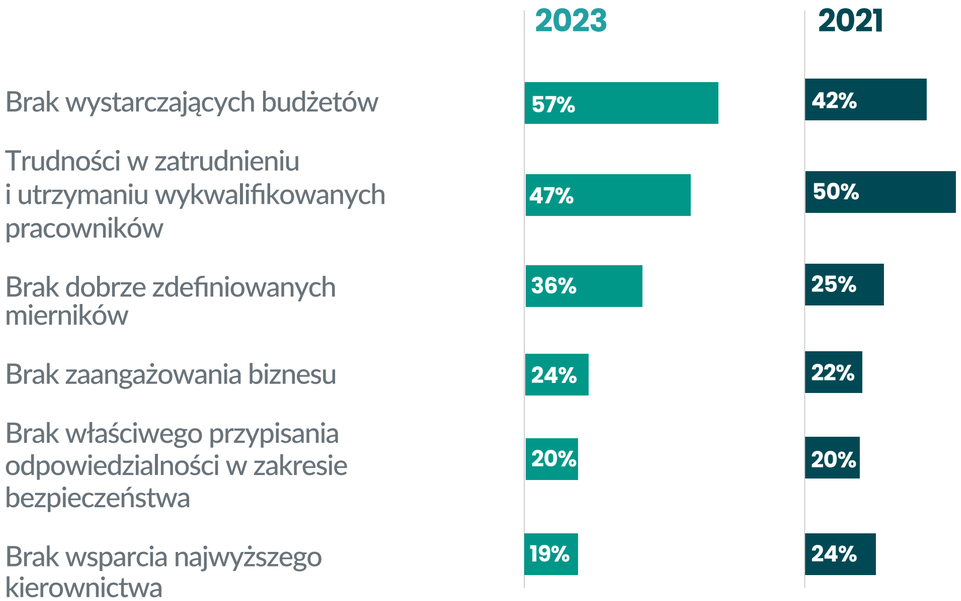


WYZWANIA DLA BIZNESU

To niewystarczający budżet oraz trudności w zatrudnieniu oraz utrzymaniu wykwalifikowanych pracowników wskazywane są przez przedsiębiorców jako największe przeszkody, które utrudniają poprawę poziomu cyber-zabezpieczeń.

Problem związany z brakiem specjalistów można jednak szybko rozwiązać. Aż 81 procent firm korzysta z outsourcingu przynajmniej jednej z funkcji cyberbezpieczeństwa – powszechność tej usługi nie była nigdy wcześniej na tak wysokim poziomie. Zewnętrzne firmy zajmują się przede wszystkim wsparciem w reakcji na cyberataki, analizą złośliwego oprogramowania oraz przeprowadzaniem testów podatności infrastruktury na zagrożenia.

Główne ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń w organizacji



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

PROGNOZY

Kiedy weźmiemy pod uwagę dane z ostatnich lat oraz informacje o rosnącej liczbie incydentów w przestrzeni cyfrowej, wniosek nasuwa się sam – w najbliższych latach przedsiębiorcy powinni przygotować się na coraz bardziej zróżnicowane i trudne do przewidzenia, zaawansowane ataki.

Według ENISA – agencji Unii Europejskiej ds. Cyberbezpieńczeństwa, do 2030 roku będziemy mieli do czynienia przede wszystkim z[1]:

- kampaniami dezinformacyjnymi,
- atakami na łańcuchy dostaw z użyciem złośliwego oprogramowania, utratą prywatności w cyberprzestrzeni,
- ukierunkowanymi atakami, które zostaną wzmocnione danymi z inteligentnych urządzeń,
- manipulowaniem algorytmami AI (sztuczna inteligencja),
- powstaniem zaawansowanych zagrożeń hybrydowych, które będą łączyć świat online i offline,
- cyberatakami na transgranicznych dostawców usług teleinformatycznych, które czasowo będą ograniczać dostępność infrastruktury krytycznej,
- atakami na infrastrukturę kosmiczną.

Najbliższe lata to również czas na wprowadzenie zmian wynikających z nowych regulacji prawnych (np. DORA, NIS2). Zgodnie z DORA, do 17 stycznia 2025 roku wskazani przedsiębiorcy powinni: wprowadzić ramowe zasady zarządzania ryzkiem związanym z technologiami informacyjno-telekomunikacyjnymi, wdrożyć procedury, które pozwolą zarządzać incydentami, a także używać zaktualizowanych systemów.

Natomiast procedury wynikające z dyrektywy NIS2 powinny być wprowadzone do 16 października 2024 roku. To między innymi: analiza ryzyka i polityka bezpieczeństwa systemów informacyjnych, zapewnienie bezpieczeństwa łańcucha dostaw, gwarancja ciągłości działania i efektywne zarządzanie kryzysowe.

Statystycznie nawet co trzeci pracownik klika w nieznany link lub wiadomość e-mail albo niewłaściwie reaguje na podejrzane powiadomienie, czym stwarza realne ryzyko dla organizacji[2].

[1] Prognozy ENISA – https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
[2] Źródło: "Phishing by Industry", KnowBe2022, 2022.

CREDIT AGRICOLE
EFL LEASING