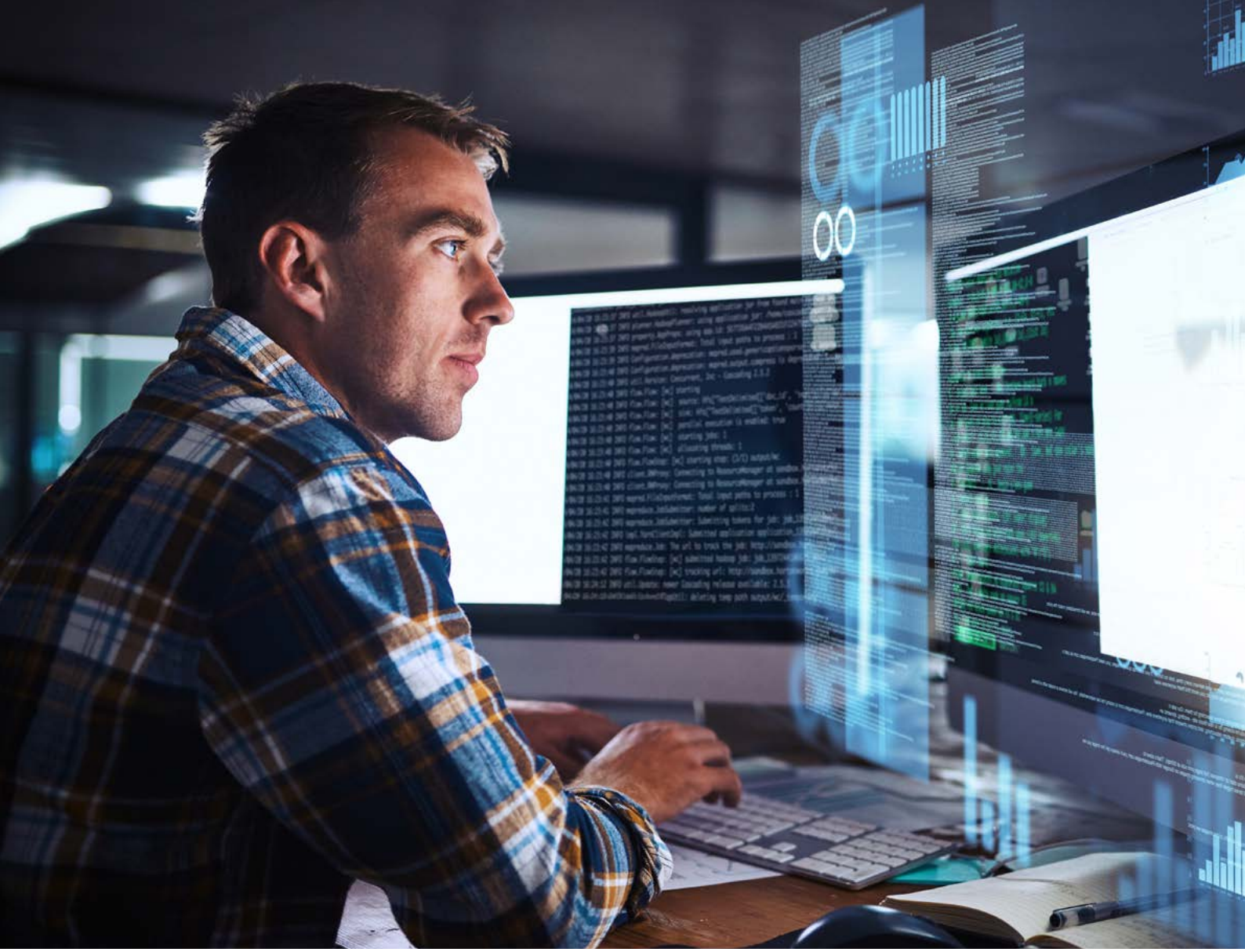


COMARCH

Cyberbezpieczeństwo od A do Z

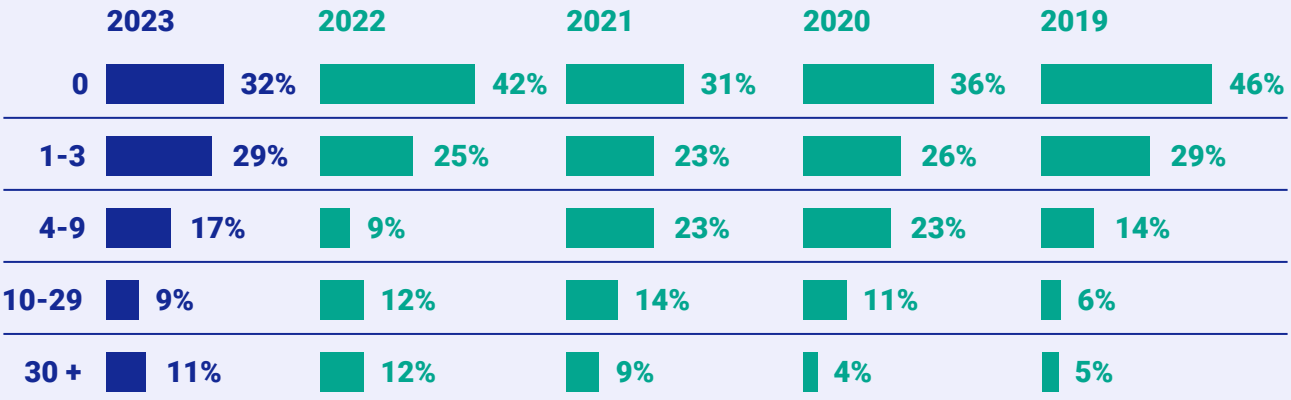
Ochrona zasobów cyfrowych dla małych i średnich firm

Cyberbezpieczeństwo – proste kroki do ochrony zasobów w Twojej firmie

Słowem wstępu

Wyniki badań dotyczących cyberbezpieczeństwa nie napawają optymizmem. Choć z roku na rok rośnie liczba firm deklarujących dobre przygotowanie w tym zakresie, jednocześnie **rośnie też liczba zarejestrowanych ataków.** Łakomym kąskiem dla cyberprzestępców są szczególnie małe i średnie przedsiębiorstwa, które dysponują dużo mniejszymi zasobami niż wielkie korporacje. Dlatego szacuje się, że są one dziś celem 47%, czyli prawie połowy wszystkich cyberataków.

Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa

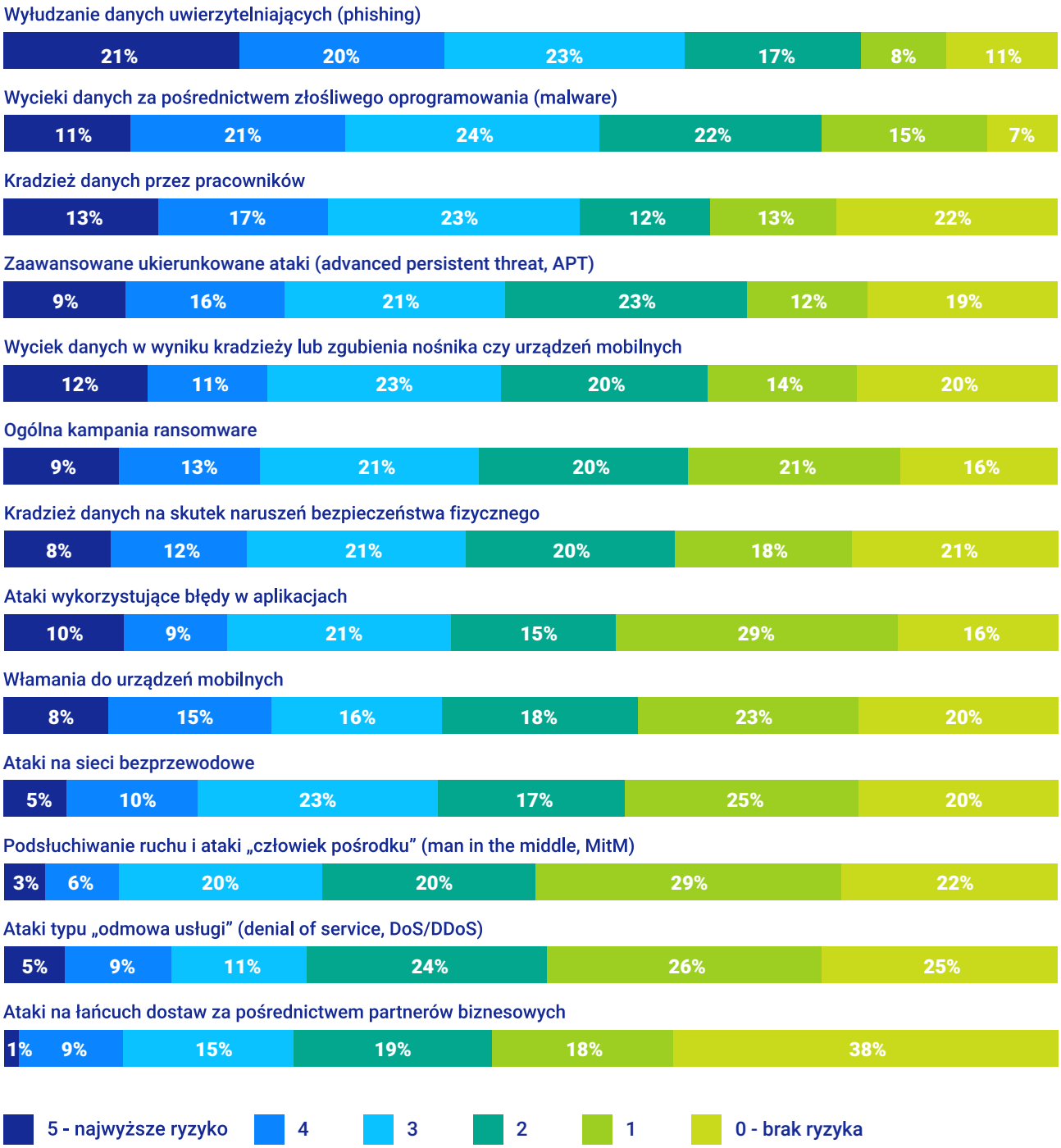


* Wartość na wykresie nie sumuje się do 100% (2% stanowi odmowa odpowiedzi)

Źródło: Raport „Barometr cyberbezpieczeństwa" na zlecenie KPMG, luty 2024 roku.

Największym zagrożeniem pozostaje **phishing**, czyli metoda podszywania się pod inną osobę lub instytucję w celu wyłudzenia danych. 20% firm wskazuje je jako najbardziej prominentne. Na drugim miejscu plasuje się **malware** – trojany, wirusy i innego rodzaju złośliwe oprogramowanie, które pracownicy instalują na swoim sprzęcie służbowym np. w wyniku kliknięcia w podejrzany link. Obecne podium zagrożeń zamyka **kradzież danych** związana z naruszeniem bezpieczeństwa fizycznego lub utratą nośników – znaczenie tego zagrożenia wzrosło ostatnio szczególnie.

Cyberzagrożenia stanowiące największe ryzyko dla organizacji



Źródło: Raport „Barometr cyberbezpieczeństwa" na zlecenie KPMG, luty 2024 roku.

Jak w obliczu tych zagrożeń starają się radzić sobie firmy? Niestety tylko jedna trzecia ankietowanych deklaruje, że ich załoga przechodzi regularne szkolenia w tym zakresie. Tymczasem **rośnie rola błędu ludzkiego jako przyczyny wycieków danych w firmach** – najnowsze badania wskazują, że jest on już odpowiedzialny za aż 68% incydentów bezpieczeństwa. W obliczu tych danych jasne staje się, że kluczowym elementem budowania odpornego systemu zabezpieczeń w firmach powinni być świadomi i wyposażeni w odpowiednie narzędzia pracownicy.

Jak z ich pomocą zbudować kulturę cyberbezpieczeństwa w organizacji? Gdzie szukać punktów styku między silną ochroną i wysoką produktywnością? Czy model Zero Trust stanowi odpowiedź na wszystkie wyzwania? Wreszcie – gdzie szukać wiedzy i kompetencji w zakresie cyberbezpieczeństwa? Na te pytania staramy się odpowiedzieć w naszym e-booku. Zaczniemy jednak od pojęcia, które stanowi podstawę dalszych rozważań i rekomendacji.

Co kryje się za hasłem higieny cyfrowej?

Na higienę cyfrową składają się dwa główne aspekty. Aby je omówić, odwołamy się do definicji stworzonych przez Polskiego Ministerstwo Cyfryzacji.

Po pierwsze, **higiena cyfrowa to zespół czynności i postaw, które zapewniają bezpieczne** – czyli niestanowiące zagrożenia dla zdrowia i życia – **użytkowanie urządzeń elektronicznych oraz nowoczesnych technologii.** W tej optyce chodzi o minimalizowanie negatywnego wpływu na formę psychiczną i fizyczną, który może objawiać się np. problemami ze snem, zaniedbywaniem obowiązków czy kłopotami z koncentracją.

Po drugie, a dla nas w tym przypadku kluczowe, **cyfrowa higiena to użytkowanie zasobów elektronicznych w taki sposób, aby zapobiegać zagrożeniom związanym z wyciekiem danych i atakami** wykorzystującymi złośliwe oprogramowanie czy socjotechnikę.

To podejście koncentruje się na takich elementach jak poufność informacji, ograniczenie dostępu do danych osobom nieupoważnionym oraz gwarancja dostępności systemów.

Higiena cybernetyczna ma w miejscu pracy ogromne znaczenie, ponieważ **nieprzestrzeganie jej grozi:**

- dezorganizacją procesów (wymiany danych, produkcyjnych, logistycznych, księgowych itd.),
- przerwami w świadczeniu usług,
- ujawnieniem danych poufnych (w tym osobowych, np. klientów),
- utratą zaufania do marki i jej produktów lub usług.

Wymagania stawiane firmom, czyli jak zbudować kulturę cyberbezpieczeństwa w organizacji?

Wymagania związane z cyberbezpieczeństwem w małych i średnich przedsiębiorstwach, zależą w dużej mierze od konkretnej branży oraz rodzaju działalności. Mimo tego **istnieją uniwersalne zasady**, które powinny stanowić fundamenty budowy kultury bezpieczeństwa cyfrowego w każdej firmie. O jakich wytycznych mowa?

1. Opracowanie polityki bezpieczeństwa

Każda firma, niezależnie od swojej wielkości, powinna opracować i wdrożyć kompleksową politykę cyberbezpieczeństwa, aby skutecznie chronić swoje dane oraz systemy IT. Główny element takiej strategii to precyzyjne określenie zasad dostępu do danych oraz ich przetwarzania, czyli minimalizacja ryzyka nieautoryzowanego dostępu i naruszeń.

Wprowadzenie jasnych procedur to sposób na zwiększenie świadomości pracowników w tym temacie. Równie istotnym aspektem jest regularne szkolenie personelu, które podnosi świadomość zagrożeń oraz uczy, jak skutecznie reagować na incydenty związane z bezpieczeństwem.

2. Zarządzanie dostępem na różnych poziomach uprawnień

Główną zasadą rządzącą tym aspektem cyberbezpieczeństwa jest udzielanie minimalnych uprawnień (ang. least privilege), która polega na przyznawaniu użytkownikom jedynie tych dostępów, które są niezbędne do wykonywania ich obowiązków. Niezbędnym krokiem w zwiększeniu poziomu bezpieczeństwa jest również wdrożenie uwierzytelniania wieloskładnikowego (MFA) dla systemów krytycznych, co pozwala na skuteczniejsze zabezpieczenie wrażliwych danych poprzez wymaganie dodatkowej warstwy weryfikacji tożsamości.

Ważne, aby pamiętać, że budowanie cyberbezpieczeństwa to proces, który nigdy się nie kończy. Aby zapewnić aktualność i adekwatność dostępów oraz uprawnień, konieczne jest przeprowadzanie regularnych przeglądów oraz dostosowywanie poziomów do zmieniających się potrzeb organizacji.

3. Tworzenie kopii zapasowych, ochrona danych i sieci

Skuteczna ochrona danych w firmie wymaga wdrożenia odpowiednich środków bezpieczeństwa, które zabezpieczą informacje zarówno podczas ich przechowywania oraz przetwarzania, a także wymiany. Pierwszym elementem jest szyfrowanie danych zarówno w spoczynku, jak i w trakcie przesyłania.

Nie mniej istotne pozostaje regularne tworzenie kopii zapasowych (backupów), które powinny być przechowywane w bezpiecznych lokalizacjach, minimalizując ryzyko utraty informacji w wyniku awarii systemów, błędów ludzkich czy ataków cybernetycznych. Tworzenie kopii zapasowych to jednak nie wszystko – nie można zapominać o regularnym testowaniu procedur przywracania danych, aby mieć pewność, że w przypadku incydentu firma będzie w stanie szybko i skutecznie odzyskać zasoby.

Dodatkowym aspektem jest zabezpieczenie sieci poprzez wdrożenie zapory (firewall) oraz systemu wykrywania i zapobiegania włamaniom (IDS/IPS), które monitorują ruch sieciowy, identyfikują podejrzane aktywności i blokują potencjalnie niebezpieczne połączenia. Separacja sieci firmowej od gościnnej, pozwalająca na ograniczenie dostępu osób zewnętrznych do krytycznych zasobów przedsiębiorstwa, to jeszcze jeden ze sposobów ochrony.

4. Reagowanie na incydenty

Gdy nie zadziała prewencja i dojdzie do incydentu bezpieczeństwa, szybka i efektywna reakcja to ostatnia linia obrony. Aby jednak reagować skutecznie, należy wcześniej opracować szczegółowy plan postępowania, który określa procedury postępowania, role i odpowiedzialności poszczególnych członków zespołu oraz kroki, jakie należy podjąć w takiej sytuacji.

Równie ważne jest prowadzenie rejestru incydentów, który pozwala na ich dokładne przeanalizowanie i wyciągnięcie wniosków w celu udoskonalenia strategii ochrony. Efektywne reagowanie nie jest ponadto możliwe bez regularnych szkoleń z cyberbezpieczeństwa, które zapewniają pracownikom wiedzę i umiejętności.

5. Edukowanie i uświadamianie zespołów

Skoro już jesteśmy przy szkoleniach, warto przypomnieć, że kluczową rolę w ochronie danych firmy pełnią pracownicy. Dlatego systematyczne działania mające na celu aktualizację ich wiedzy w zakresie zagrożeń (np. phishingu czy ransomware), bezpiecznego korzystania z internetu oraz właściwego zabezpieczania danych, pozwala pracownikom lepiej rozumieć potencjalne ryzyka i unikać błędów. Warto również przeprowadzać okresowe testy socjotechniczne w rodzaju kontrolowanych kampanii phishingowych, które pozwalają sprawdzić, jak pracownicy reagują na konkretne próby wyłudzenia informacji.

6. Osiągnięcie zgodności z regulacjami i normami

W bezpieczeństwie cyfrowym nie chodzi „tylko” o ochronę danych firmy, ale również uniknięcie potencjalnych konsekwencji prawnych. Weryfikacja zgodności z przepisami, takimi jak RODO, w zakresie ochrony danych osobowych czy międzynarodowa norma ISO 27001 dotycząca systemów zarządzania bezpieczeństwem informacji, pozwala firmie działać zgodnie z najlepszymi praktykami i wymaganiami prawnymi.

Ostatnim aspektem tej części dbania o cyberbezpieczeństwo jest również prowadzenie regularnych audytów, które umożliwiają identyfikację ewentualnych dziur w zabezpieczeniach i ich załatanie. Dzięki konsekwentnemu monitorowaniu zgodności organizacja nie tylko wzmacnia swoje bezpieczeństwo, ale także buduje zaufanie klientów i partnerów biznesowych. Jak widać, inwestowanie w cyberbezpieczeństwo to jednoczesny wkład w budowanie pozytywnego wizerunku firmy.

Koncepcja Zero Trust – czym jest i jak wdrożyć ją krok po kroku?

Model Zero Trust opiera się na przekonaniu, że **każdy użytkownik (a także urządzenie czy adres IP), który uzyskuje dostęp do jakiegoś zasobu, stanowi potencjalne źródło niebezpieczeństwa** – przynajmniej do momentu, aż nie udowodni, że jest inaczej. Termin „Zero Trust" został stworzony w 2009 roku przez firmę Forrester, jeden z najbardziej wpływowych podmiotów badawczych i doradczych na świecie, jako alternatywa wobec tradycyjnego podejścia zabezpieczeń obwodowych (skoncentrowanych na ochronie wytyczonych „granic", np. sieci w firmowym budynku).

W ramach koncepcji Zerowego Zaufania **nie można ufać, należy za to sprawdzać** – a zatem dokładnie wiedzieć, jacy użytkownicy i z pomocą jakich urządzeń uzyskują dostęp do zasobów firmowych. Ścisła kontrola oraz weryfikacja, kto i co próbuje połączyć się z siecią, to jedno z oczywistych następstw wdrożenia modelu.

Jakie etapy zakłada wdrożenie Zero Trust?

1. Identyfikacja danych wrażliwych

To etap, w którym zadajemy sobie podstawowe pytania:

- Gdzie znajdują się dane naszej organizacji?
- Kto ma do nich dostęp i na jakich zasadach?
- Czy każda próba uzyskania danych (próba dostępowa) jest rejestrowana przez nasze systemy?

2. Wprowadzenie środków kontroli dostępów

To czas na wdrożenie konkretnych elementów pomagających chronić dane firmy, takich jak

- **Least-Privilege Access** (LPA, dostęp o najniższym poziomie uprawnień), czyli udzielanie tylko takiego dostępu i uprawnień do informacji oraz systemów, jakich użytkownicy potrzebują do wykonywania swoich obowiązków, ale nigdy większego.
- **Multi-Factor Authentication** (MFA, uwierzytelnianie wieloskładnikowe), czyli dodatkowy element uwiarygodnienia użytkownika po zalogowaniu, na przykład weryfikacji tożsamości poprzez skanowanie odcisku palca albo poproszenia o podanie kodu wysłanego na adres e-mail, numer telefonu czy w aplikacji.
- **Zero Trust Network Access** (ZTNA, dostęp do sieci zdefiniowany programowo lub izolowanie sieci), czyli segmentacja i mikrosegmentacja sieci na mniejsze elementy architektury, by w razie zagrożenia „odciąć" dostęp do poszczególnych części i powstrzymać eskalację problemu (np. wycieku).

3. Monitoring real-time i atomatyzacja

Ostatni krok to inwestycja w rozbudowanie szerokiego systemu zabezpieczeń, który daje zespołowi bezpieczeństwa w firmie pełną wiedzę na temat tego, co dzieje się z jej zasobami.

- **Analiza w czasie rzeczywistym** – monitoring i wykrywanie incydentów bezpieczeństwa muszą działać w czasie rzeczywistym, ponieważ nawet minimalne opóźnienia w raportowaniu podejrzanej aktywności, nieautoryzowanego dostępu i innych zagrożeń mogą spowodować olbrzymie konsekwencje.
- **Zautomatyzowane procesy reagowania** – zapewnianie cyberbezpieczeństwa nie może polegać wyłącznie na działaniach manualnych, szczególnie w sytuacji wielu alertów bezpieczeństwa jednocześnie. Dlatego konieczne jest wprowadzenie automatyzacji – zarówno odcinania dostępów przy wykryciu zagrożenia, jak i samego udzielania ich przy np. tworzeniu nowych kont użytkowników.

Czy można przesadzić z zabezpieczeniami? Znajdź złoty środek!

Choć dzisiejsze priorytetyzowanie ochrony zasobów jest dla biznesu oczywiste, pozostaje jedno „ale". Nakładanie na urządzenia (laptopy, komputery, telefony itd.) wielu warstw zabezpieczeń, a na pracowników dużej liczby obowiązków i obostrzeń mających na celu ochronę danych **może znacząco wpływać na efektywność oraz komfort pracy.** Tymczasem te elementy często przesądzają o przewadze konkurencyjnej przedsiębiorstwa.

Nie bez powodu zatem znalezienie równowagi między bezpieczeństwem i produktywnością stanowi dla wielu firm spore wyzwanie. Wymaga ono bowiem wdrożenia starannie zaplanowanej strategii, nierzadko inwestycji w odpowiednie (działające „w tle" wykonywanej racy) narzędzia oraz zaangażowania wszystkich pracowników w budowę bezpiecznych nawyków, które z czasem wykonywane będą automatycznie, bez wysiłku i odciągania uwagi od pracy projektowej.

Wyważone podejście do cyberbezpieczeństwa nie pociąga za sobą drastycznych zmian w żadnym z tych obszarów. Wspiera raczej **synergię ochrony i produktywności, w której oba elementy wzajemnie się wzmacniają.** Przyjmując taką strategię, firmy mają szansę tworzyć wyjątkowy ekosystem biznesowy, który będzie prosperował nawet w obliczu nieustannej ewolucji cyberzagrożeń.

Opracowanie jasnej i łatwo dostępnej polityki bezpieczeństwa, wdrożenie zautomatyzowanego monitoringu oraz reagowania na incydenty, zautomatyzowanie tworzenia kopii zapasowych danych i systemów, segmentacja architektury oraz regularne szkolenie zespołów **to najskuteczniejsze narzędzia służące do budowania synergii cyberbezpieczeństwa z produktywnością.**

Szkolenia, kursy, praktyka – jak budować cyberświadomość w firmie?

Istnieje dziś wiele sposobów na rozwój w zakresie cyberbezpieczeństwa, od możliwości działań podejmowanych osobiście na użytek prywatny, jak i w bardziej zorganizowanym zakresie – jeśli chcemy wesprzeć swoją firmę na poziomie systemowym, np. budując świadomość pracowników.

Skąd czerpać informacje o cyberbezpieczeństwie?

- Strony rządowe, w tym ta dotycząca Cyberbezpieczeństwa oraz Ministerstwa Cyfryzacji, a także organizacji rządowych.
- Portale tematyczne zrzeszające specjalistów i znawców tematu, skupiające cenne artykuły i e-booki dotyczące bieżących nowości z zakresu cyberbezpieczeństwa.
- Blogi, vlogi specjalistyczne, materiały video czy podcasty.
- Darmowe webinary, na przykład o roli AI w cyberbezpieczeństwie lub… jak Scarlett Johansson kopała kryptowaluty.
- Konferencje, seminaria, spotkania tematyczne organizowane zarówno przez środowiska naukowe jak i biznesowe.
- Studia (w tym kilkuletnie kierunkowe oraz podyplomowe).
- Specjalistyczne kursy i szkolenia z cyberbezpieczeństwa.

Kilka słów od eksperta

1. Czy cyberbezpieczeństwo powinno dziś stanowić integralną część strategii rozwoju biznesowego?

Kamil Migacz

Dyrektor zespołu ds. cyberbezpieczeństwa.

W dobie cyfryzacji i rosnącej liczby zagrożeń w sieci, cyberbezpieczeństwo nie może być traktowane jako dodatkowy element infrastruktury IT – powinno stanowić integralną część strategii rozwoju każdej organizacji. Firmy, które świadomie uwzględniają bezpieczeństwo w swoich planach rozwoju, zyskują przewagę konkurencyjną, minimalizują ryzyko strat finansowych i budują zaufanie klientów.

Jednym z kluczowych argumentów przemawiających za włączeniem cyberbezpieczeństwa do strategii biznesowej jest ochrona danych. Współczesne przedsiębiorstwa operują ogromnymi ilościami informacji, zarówno własnych, jak i powierzonych przez klientów. Każde naruszenie może prowadzić do poważnych konsekwencji – od kar finansowych po utratę reputacji. Z tego względu inwestycje w zabezpieczenia, regularne audyty oraz szkolenia pracowników stają się niezbędnym elementem odpowiedzialnego zarządzania.

Ponadto, cyberbezpieczeństwo wpływa na innowacyjność i skalowalność biznesu. Firmy, które już na etapie planowania nowych produktów czy usług uwzględniają kwestie bezpieczeństwa, mogą szybciej dostosowywać się do zmieniających się wymogów regulacyjnych i oczekiwań klientów.

Wreszcie, warto zauważyć, że cyberbezpieczeństwo to nie tylko zabezpieczenia techniczne, ale także element kultury organizacyjnej. Świadomość zagrożeń i odpowiedzialność za bezpieczeństwo powinna być obecna na każdym szczeblu firmy – od zarządu po szeregowych pracowników. Dopiero takie holistyczne podejście pozwala skutecznie chronić firmę przed cyberatakami i wspierać jej długoterminowy rozwój.

Cyberbezpieczeństwo nie jest już opcją, lecz koniecznością dla każdej rozwijającej się organizacji. Jego integracja ze strategią biznesową pozwala nie tylko unikać zagrożeń, ale także budować stabilną, innowacyjną i godną zaufania markę na rynku.

2. Od czego polecasz małym i średnim firmom zacząć budowę kultury cyberbezpieczeństwa w swoich strukturach?

Kamil Żaczek

Inżynier DevOps.

Pierwszym punktem od którego warto by było zacząć są szkolenia z zakresu cyberbezpieczeństwa które powinny być obowiązkowe dla wszystkich pracowników, niezależnie od ich stanowiska.

Warto by było żeby poruszałe one te tematy:

- *Phishing*
- *Reakcja na incydenty*
- *Dobre praktyki haseł i 2FA*
- *Jak bezpieczenie korzystać z internetu*

Ponadto warto udostępniać dodatkowe środki pracownikom, jak na przykład materiały szkoleniowe czy prowadzic kampanie uświadamiające.

Ważnymi aspektami są też audyty bezpieczeństwa, które pomogą w identyfikacji luk bezpieczeństwa i procedurach postępowania w przypadku zagrożenia, ponadto warto warto też uświadomić, że regularne aktualizacje mogą drastycznie zmniejszyć wektory ataków.

Podsumowując wszystkie opisane kwestie nie do końca będą w stanie zapobiedz incydentom jeżeli, te procesy nie będą ciągłe oraz nie będzie w nie zaangażowane kierownictwo dając doby przykład.

3. Jakie są najskuteczniejsze metody rozwijania wiedzy, dobrych nawyków i kompetencji w zakresie bezpieczeństwa cyfrowego?

Daniel Adamiec

Specjalista ds. cyberbezepieczeństwa, penetration tester.

Podobnie jak w innych kategoriach wiedzy, nie ma tu dobrej drogi na skróty. W temacie trzeba zwyczajnie „siedzieć" i budować powoli naszą znajomość z dziedziną cyberbezpieczeństwa. Jeżeli nie chcemy być ograniczeni przez strukturę oraz czasochłonność typowych źródeł wiedzy specjalistycznej, takich jak studia czy szkolenia, warto poszukać odpowiednich kanałów/społeczności/ stron na mediach społecznościowych czy blogach. W Polsce mamy całkiem sporo dużych i znanych tego typu źródeł, chociażby Niebezpiecznik, Sekurak, Kapitan Hack, Zaufana Trzecia Strona i wiele innych. Na YouTubie też bez problemu będziemy w stanie znaleźć kanały przeznaczone tego typu tematyce. Poza kanałami chociażby niektórych z wcześniej wymienionych stron, możemy znaleźć także takie osoby jak Mateusz Chrobok Czy Kacper Szurek. Jeżeli nie przeszkadza nam język angielski, liczba zarówno stron jak i kanałów znacząco rośnie (KONIECZNIE zapoznajecie się z OWASPem). Godnym uwagi jest także grupa ludzi skupiona na osiągnięciu prywatności w internecie – prywatność to w końcu właściwie bezpieczeństwo naszych własnych danych. Tutaj już niestety musimy raczej szukać źródeł anglojęzycznych.

Jeżeli chodzi o firmy i zagrożenia dla nich, warto śledzić change logi zależności i aplikacji z których korzystamy, listy CVE (wg. Wikipedii - słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa) oraz historie wycieków które pokażą nam odpowiednie antywzorce – te możemy znaleźć w tych samych miejscach wymienionych w poprzednim akapicie.

Jeżeli chodzi o rozwój własnych kompetencji, nie ma nic lepszego niż praktyka, dlatego osobiście polecam platformę TryHackMe oraz, dla tych bardziej zaawansowanych, HackTheBox. To nie są jedyne miejsca gdzie możemy uzyskać wiedzę teoretyczną wraz z praktyczną, ale na start są zdecydowanie najlepsze – jeżeli umiecie więcej to raczej będziecie już w stanie sami znaleźć podobne platformy. My również przeprowadzamy szkolenia łączące teorię z praktyką i gorąco zachęcam do wzięcia w nich udziału :)

Tym zdecydowanym na dalsze zagłębienie się w temat warto też spojrzeć na certyfikacje związane z bezpieczeństwem - nawet jeżeli nie zdecydujemy się na zakup certyfikatu, lista zagadnień koniecznych do uzyskania go może okazać się przydatna w znalezieniu tematów wartych poznania.

4. Czy istnieje jakiś jeden, niezawodny sposób na ochronę przed atakami cybernetycznymi?

Wojciech Badura

Specjalista ds. cyberbezpieczeństwa.

Ochrona przed atakami cybernetycznymi to jedno z kluczowych wyzwań, przed którymi stoją współczesne firmy. Niestety, nie istnieje jedno, niezawodne rozwiązanie gwarantujące pełne bezpieczeństwo. Najskuteczniejszym podejściem jest strategia stosowana w Comarchu - „defense in depth", która polega na stosowaniu wielu różnych mechanizmów zabezpieczających, aby nawet w przypadku naruszenia jednej warstwy ochrony, kolejne uniemożliwiały atakującemu dostęp do krytycznych danych i systemów.

Obecnie większość ataków rozpoczyna się od kampanii phisingowych, dlatego warto zadbać o edukację pracowników w zakresie cyberzagrożeń. Niesety najczęściej nasi pracownicy stanowią najsłabsze ogniwo w systemie bezpieczeństwa. Pracownicy powinni być świadomi ryzyka i unikać otwierania podejrzanych wiadomości e-mail oraz klikania w nieznane linki.

Podstawowym elementem cyberbezpieczeństwa jest stosowanie silnych haseł i uwierzytelniania wieloskładnikowego (MFA), co znacząco utrudnia przejęcie kont przez cyberprzestępców.

Równie ważne jest regularne aktualizowanie systemów i oprogramowania, ponieważ wiele ataków wykorzystuje luki w zabezpieczeniach, które producenci często eliminują w nowych wersjach oprogramowania.

Niestety dzisiaj dość często zdarza się, że przedsiębiorcy próbują zaoszczędzić korzystając z niewspieranych systemów operacyjnych czy uzyskanych z nielegalnego źródła licencji.

Dodatkowym zabezpieczeniem jest tworzenie kopii zapasowych danych – w przypadku ataku ransomware firma może szybko odzyskać utracone informacje bez konieczności płacenia okupu. Ibard może zapewnić bezpieczną przystań na nasze dane dzięki automatycznemu tworzeniu kopii zapasowych za pomocą aplikacji

Dodatkową warstwę ochrony stanowią zapory sieciowe (firewall) i oprogramowanie antywirusowe, które pomagają wykrywać i blokować złośliwe oprogramowanie na wczesnym etapie. Nie warto opierać swojej firmowej sieci tylko na routerze od operatora. Istotne jest także stosowanie zasady minimalnych uprawnień, czyli ograniczanie dostępu użytkowników tylko do tych zasobów, które są im niezbędne do pracy. Konieczne jest też stworzenie kont każdemu praownikowi z osobna. Korzsytanie ze wspólnych kont znacząco utrudni identyfikację wektora ataku.

Dla tych któryz naprawdę dbają o bezpiecznieństwo monitorowanie sieci firmowej i wdrożenie systemów wykrywania zagrożeń (IDS/IPS) znacząco podniesie bezpieczeństwo i pozwala na szybką reakcję na podejrzane aktywności.

Wspólne zastosowanie tych metod znacząco zmniejsza ryzyko cyberataków i pomaga firmie funkcjonować w bezpiecznym środowisku cyfrowym. Choć nie da się całkowicie wyeliminować zagrożeń, świadome podejście do cyberbezpieczeństwa i wdrożenie strategii „defense in depth" może skutecznie zabezpieczyć przedsiębiorstwo przed poważnymi konsekwencjami ataku.

5. Jak na co dzień możemy chronić swoją tożsamość i dane w sieci?

Tomasz Piszczek

Młodszy specjalista ds. cyberbezpieczeństwa.

Nie ukrywajmy, cyfrowy świat, znany jako Internet, jest niezwykle wygodny i pomocny, ale tylko wtedy, gdy korzystamy z niego rozsądnie. Dzięki szeroko pojętemu Internetowi mamy dostęp do wielu możliwości, które jeszcze niedawno były poza naszym zasięgiem. Te nowe możliwości mogą przynieść zarówno liczne korzyści, jak i zupełnie nowe problemy. W dzisiejszych czasach rozwój Internetu postępuje w zawrotnym tempie – możemy błyskawicznie wyszukiwać dowolne informacje, cieszyć się ulubioną muzyką czy spotykać online z kuzynem mieszkającym na przedmieściach Chicago. Niestety, ten komfort nie jest darmowy – za każdym razem pozostawiamy w sieci cząstkę siebie. Nasz cyfrowy ślad, zawierający mniej lub więcej prywatnych informacji, często staje się ceną, którą płacimy za tę wygodę.

Wielu z nas nie zdaje sobie sprawy, że w Internecie dostęp do treści czy kontakt z innymi użytkownikami zawsze wiąże się z pewnym kosztem – i to często wyższym, niż moglibyśmy przypuszczać. Czy kiedykolwiek zastanawialiście się, czy naprawdę darmowe treści są tak naprawdę darmowe? Jaką walutą płacimy za tę wygodę? I przede wszystkim – jak łatwo można stracić kontrolę nad swoim cyfrowym „alter ego"? Takie pytania powinny skłonić nas do refleksji nad tym, jak skutecznie chronić naszą tożsamość oraz udostępniane dane. Kluczowe jest, abyśmy byli świadomi zagrożeń i potrafili podejmować odpowiednie działania zwiększające bezpieczeństwo, zwłaszcza w przypadku dzieci, które dopiero zaczynają swoją przygodę z cyfrowym światem. Nie zapominajmy jednak o sobie – my, dorośli, również powinniśmy stosować się do tych zasad, dając tym samym dobry przykład.

Internet to przestrzeń, w której (tak jak w życiu) należy zachować zdrowy rozsądek połączony z zasadą ograniczonego zaufania wobec wyświetlanych treści i kontaktu z innymi użytkownikami. Podczas codziennego korzystania z sieci możemy natknąć się na strony czy linki – od rzetelnych i pomocnych, po te, które bazują na naszej ufności lub nieuwadze. Dlatego warto zawsze weryfikować wiarygodność źródeł, unikać bezrefleksyjnego klikania w linki oraz ostrożnie podchodzić do próśb o udostępnienie danych osobowych, szczególnie gdy towarzyszy im emocjonalny nacisk lub presja czasu.

Dobrą praktyką jest ostrożność w udostępnianiu informacji, szczególnie na portalach społecznościowych. Unikajmy publikowania szczegółowych danych, takich jak adres zamieszkania, dane kontaktowe czy informacje o majątku. Takie dane powinny być udostępniane tylko wyjątkowo, z zachowaniem ostrożności i zdrowego rozsądku. Należy także unikać chwaleniem się nowym samochodem, domem czy dużymi zakupami, które mogą przyciągnąć niepożądaną uwagę. Niezwykle ważne jest także, aby nie publikować zdjęć dokumentów tożsamości, takich jak dowód osobisty czy prawo jazdy, które mogą zostać wykorzystane do kradzieży tożsamości.

Cyberprzestępcy często stosują phishing, podszywając się pod zaufane instytucje, by wyłudzić nasze dane. Dlatego nigdy nie klikajmy w linki zawarte w podejrzanych wiadomościach e-mail czy SMS-ach. Jeśli otrzymamy wiadomość rzekomo od banku, zawsze samodzielnie wpisujmy adres strony w przeglądarkę, a najlepiej wykonajmy telefon do banku. Zawsze weryfikujmy, czy dana osoba lub organizacja jest rzeczywiście tym, za kogo się podaje.

Pamiętajmy, że wirtualny świat rozwija się w zawrotnym tempie, a wraz z nim pojawiają się nowe zagrożenia. Warto być na bieżąco z nowinkami technologicznymi i regularnie poszerzać swoją wiedzę na temat bezpieczeństwa cyfrowego. Tylko w ten sposób możemy w pełni cieszyć się korzyściami płynącymi z Internetu, minimalizując jednocześnie ryzyko utraty danych czy naruszenia naszej prywatności.

Poznajmy się!

Centrum Szkoleniowe Comarch jest częścią struktury firmy Comarch SA. Od lat znajdujemy się w ścisłej czołówce dostawców usług szkoleniowych. Oferujemy szeroki zakres specjalistycznych szkoleń w wielu miastach Polski. Realizujemy potrzeby szkoleniowe wielu polskich i zagranicznych firm, stale podnosimy jakość szkoleń, obserwując poziom wskaźnika Net Promoter Score (NPS). Słuchamy opinii uczestników i dyskutujemy z przedstawicielami firm zamawiających szkolenia. Nasi trenerzy to ludzie z pasją i doświadczeniem. Dbamy o to, aby informacje merytoryczne na szkoleniach były uzupełnione praktycznymi przykładami.

Do zobaczenia w Centrum Szkoleniowym!

COMARCH
Szkolenia