GROMAR

Jak zadbać o cyberbezpieczeństwo w firmie w 5 krokach?

Spis treści

Wstęp

Liczba zagrożeń bezpieczeństwa w sieci nieustannie rośnie, więc organizacje jeszcze bardziej starają się chronić swoje dane i zasoby. Właściciele firm czy dyrektorzy operacyjni stoją przed ogromnymi wyzwaniami związanymi z zabezpieczeniem biznesu przed wyciekami danych, cyberatakami czy złośliwymi oprogramowaniami, które na wiele miesięcy mogą sparaliżować pracę przedsiębiorstwa.

Pomimo tego, że wielu ekspertów uznaje dziś cyberbezpieczeństwo za priorytet, zarządy firm często nie dają się przekonać do nowych inwestycji, dopóki nie zdarzy się niekontrolowana kradzież lub wyciek danych. Z jednej strony w dzisiejszych czasach takie zaniechanie to dość ryzykowne posunięcie, z drugiej – globalny rozwój technologii jest na tyle dynamiczny, że bardzo łatwo zbagatelizować drobne problemy, które mogą pociągnąć za sobą gigantyczne straty finansowe dla organizacji.

Jak pokazują ogólnoświatowe badania, do większości przypadków naruszeń bezpieczeństwa danych przyczyniają się błędy pracowników.

Wystarczy spojrzeć na tytuły nagłówków newsów w sieci. Nielegalna sprzedaż danych osobowych, masowe naruszenia w informacji, hakerzy podszywający się pod przedstawicieli renomowanych firm – to wszystko przykłady nowych zagrożeń, których opanowanie wymaga dobrze wyszkolonych pracowników. A fundamentalną wiedzę możesz przekazać swoim zespołom w cyklicznych kursach cyberbezpieczeństwa, które wymagają znacznie niższych nakładów finansowych niż usunięcie skutków niechcianych incydentów.

Z myślą o ochronie Twojego biznesu i jego zasobów eksperci GroMar przygotowali skondensowaną pigułkę wiedzy, z której dowiesz się:

- Jakie kroki należy podjąć, aby w możliwie najlepszy sposób ochronić firmę przed zagrożeniami bezpieczeństwa?
- Jak przeszkolić pracowników nietechnicznych, aby czynnik ludzki przestał odgrywać najważniejszą rolę w narażaniu firm na niebezpieczeństwa?
- Dlaczego cyberbezpieczeństwo w firmie jest obecnie niezwykle istotne?
- Jakie korzyści płyną z inwestowania w poprawę cyberbezpieczeństwa w firmie?

Dlaczego cyberbezpieczeństwo w firmie jest ważne?

Co najbardziej motywuje i napędza firmy do inwestowania w **cyberbezpieczeństwo**? Oto najważniejsze trendy, które są zauważalne na całym świecie.

Wzrost liczby cyberzagrożeń

Żyjemy w czasach, w których cyberprzestępczośćrozwija się bardzo dynamicznie. Na całym świecie z roku na roku rośnie liczba zagrożeń bezpieczeństwa. Ten trend widoczny jest również w Polsce. Wiele instytutów badawczych ryzykuje nawet stwierdzenie, że hakerzy nigdy jeszcze nie byli tak aktywni jak teraz.

Według Check Point Research w czwartym kwartale 2022 r. były okresy, że cyberprzestępcy atakowali polskie firmy średnio 2 tys. razy tygodniowo.

Błyskawiczny rozwój technologii

Technologie cały czas pędzą do przodu. Organizacje są uzależnione od sieci, systemów informatycznych i nowoczesnych aplikacji. To wszystko sprawia, że stają się coraz bardziej podatne na cyberataki. Szczególnie narażone są branże, które administrują ogromnymi liczbami danych, tj. energetyka, telekomunikacja, transport, opieka zdrowotna, a także sektor bankowy, finansowy i obronny.

Według Check Point Research znacząco zwiększa się także liczba ataków na organizacje, które korzystają z rozwiązań chmurowych.

Chwiejna sytuacja geopolityczna

Cyberprzestępcy coraz częściej wywierają presję ekonomiczną i wykorzystują techniki dezinformacji. W ten sposób testują odporność krajów demokratycznych, naruszając pokój i bezpieczeństwo państw na całym świecie.

Jak wskazują eksperci Krajowego Instytutu Cyberbezpieczeństwa, cyberataki prowadzone są równolegle z działaniami militarnymi w Ukrainie. Hakerzy chcą w ten sposób zakłócić funkcjonowanie organów i infrastruktury państwowej oraz podważyć zaufanie do liderów politycznych. Destabilizacja przekłada się także na sektor prywatny.

Luka w umiejętnościach cybernetycznych

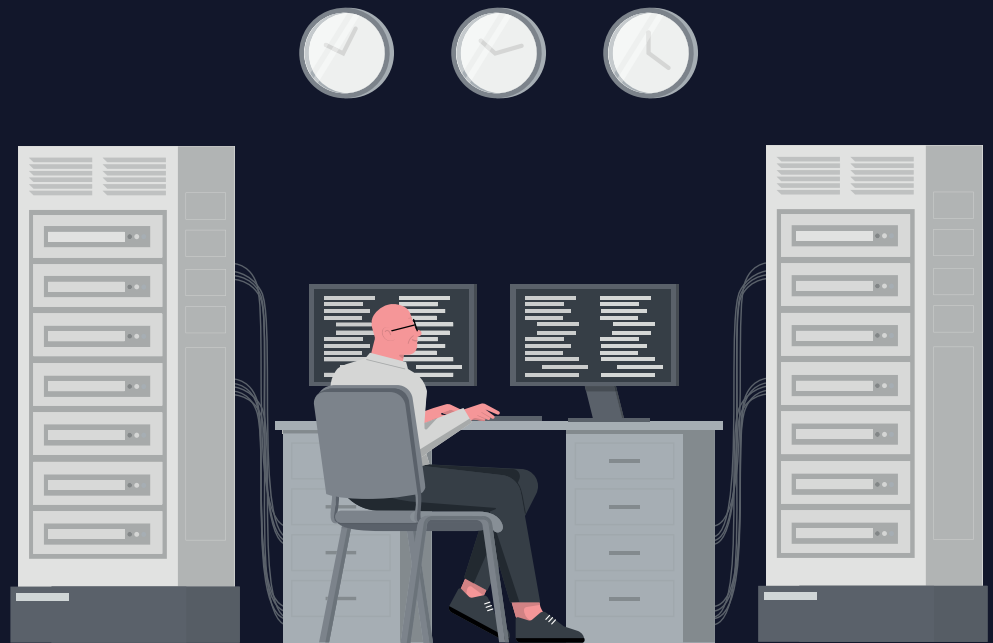
Pogłębia się luka w wiedzy pracowników organizacji dotycząca ochrony osobistej i firmowej przed zagrożeniami bezpieczeństwa. Firmy na całym świecie muszą szybko podejmować działania prewencyjne. Przy czym nie chodzi jedynie o zatrudnianie specjalistów cybersecurity, ale także o to, aby z zakresu cyberbezpieczeństwa szkolić cyklicznie wszystkich pracowników, niezależnie od zajmowanego stanowiska.

Dlaczego Twój biznes jest narażony na kradzież i wycieki danych?

Najważniejsze przyczyny naruszenia bezpieczeństwa w firmie, z którymi spotyka się praktycznie każdy przedsiębiorca.

Infrastruktura informatyczna w Twojej firmie jest wadliwa

Jeśli infrastruktura firmowa nie należy do najnowocześniejszych, może zawierać wiele wad technicznych. Są to „słabości” systemowe, które wynikają z błędów wewnętrznych oprogramowania lub złej konfiguracji ze strony użytkownika. Niewłaściwe ustawienia czasem wydają się drobnostką, jednak mogą bardzo łatwo narazić organizację na niekontrolowane wycieki danych.

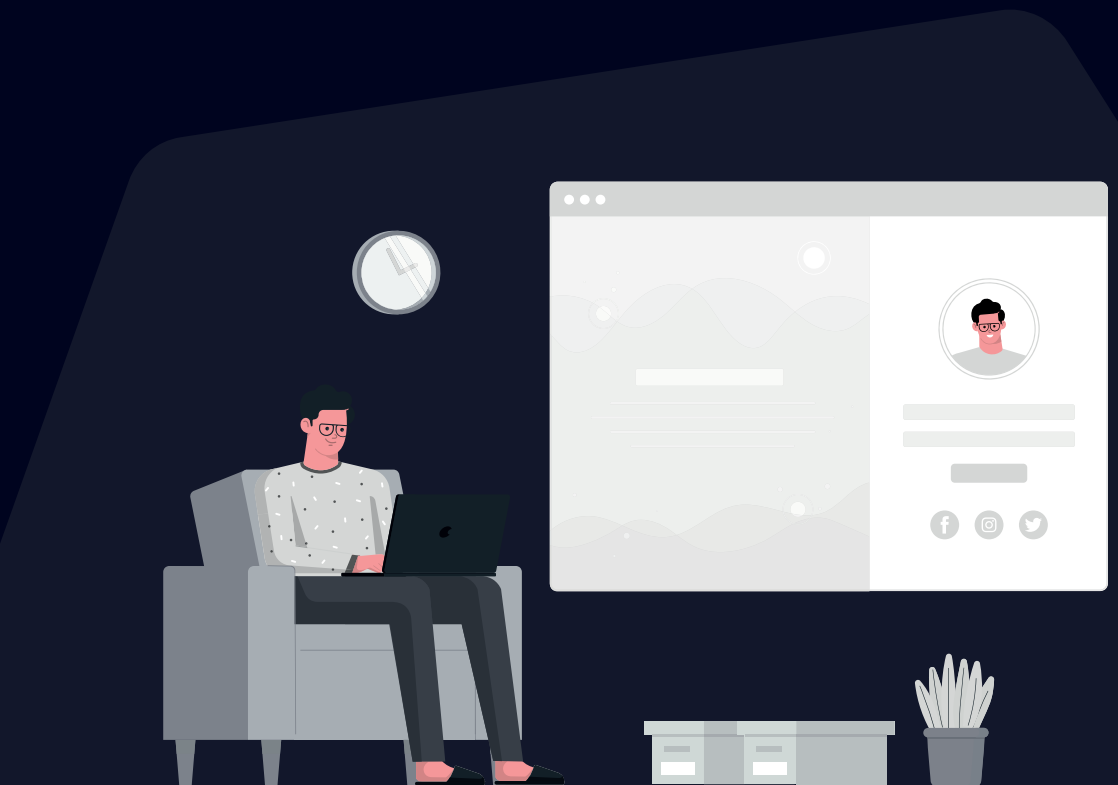


Cyberprzestępcy są coraz bardziej kreatywni

W dobie nowoczesnych technologii hakerzy nigdy nie dają za wygraną. Tworzą m.in. coraz nowsze i coraz bardziej dopracowane złośliwe oprogramowanie, które atakuje systemy firmowe. Stosują jeszcze bardziej pomysłowe i efektowne techniki ataków. W rzeczywistości każdy pracownik Twojej firmy jest narażony na kradzież danych, loginów, kont czy środków z kart płatniczych, a Twój biznes z kolei – na utratę danych kontrahentów, unikalnego know-how, danych finansowych, a nawet tajemnic handlowych.

Aplikacje, z których korzystasz, są przestarzałe lub zawierają błędy

Sprytni cyberprzestępcy zawsze poszukują przestarzałych i podatnych aplikacji, które ułatwią im włamania do zasobów firmowych. Luki w zabezpieczeniach aplikacji stanowią dla cyberprzestępców „furtki", którymi wchodzą do systemów nieświadomych niczego użytkowników w celu przeprowadzenia ataków. W ten sposób wzrasta ryzyko wystąpienia incydentu, który może mieć katastrofalne skutki dla przedsiębiorstwa i jego pracowników.



Twoi pracownicy nie mają wystarczającej wiedzy o cyberbezpieczeństwie

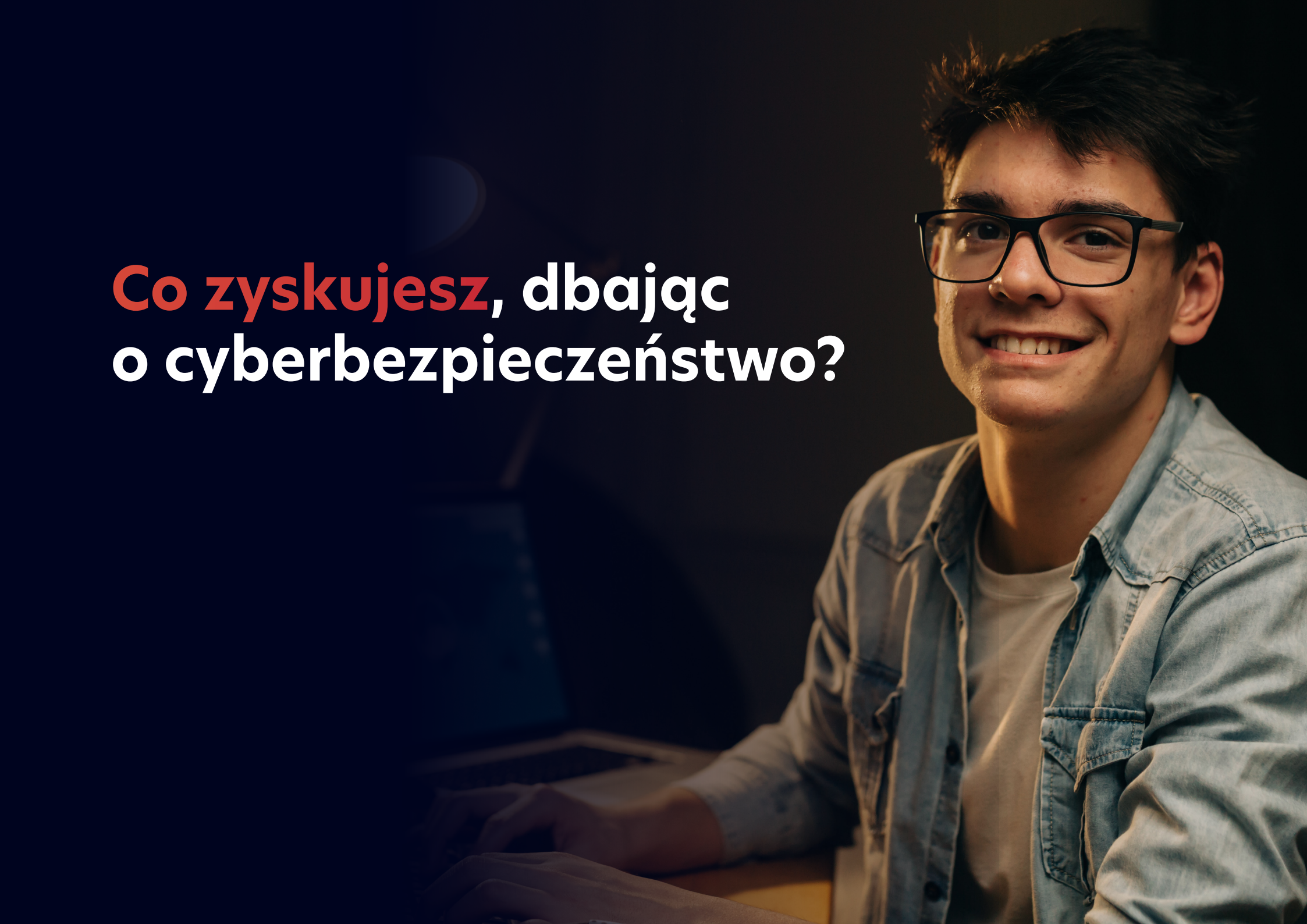
Pracownik, w którego wymierzony jest cyberatak, jest jednym z najbardziej kluczowych ogniw bezpieczeństwa w Twojej firmie, ale niestety bywa jednocześnie najsłabszym. W obecnych czasach wiedza i umiejętności pracowników bardzo szybko się dezaktualizują. W rzeczywistości Twoje zespoły nietechniczne mogą w ogóle nie mieć żadnych informacji na temat cyberbezpieczeństwa firmy. Co więcej, według badań firmy Gartner 19% umiejętności Twoich pracowników w tym zakresie, które cenisz dziś, będzie kompletnie nieprzydatnych w ciągu najbliższych 3 lat. Oznacza to, że wiedza o cyberzagrożeniach wymaga stałej aktualizacji.

Źle zabezpieczasz sprzęt firmowy i miejsca pracy

Rzeczywistość pandemiczna sprawiła, że wielu pracowników pracuje zdalnie. Twoja firma może w ten sposób zredukować koszty związane z utrzymaniem biura. Czy jednak przeznaczasz zaoszczędzone środki na zabezpieczenie sprzętu firmowego i miejsc pracy zdalnej?

Potencjalnym naruszeniem bezpieczeństwa firmy są także kradzieże lub gubienie laptopów czy telefonów przez pracowników, a także łączenie się z niebezpiecznymi sieciami internetowymi. Utrata sprzętu firmowego czy nieodpowiednia dbałość o pracowników zdalnych mogą sprawić, że cyberprzestępcy lub konkurenci uzyskają dostęp do własności intelektualnej firmy. A utrata danych jest dla większości organizacji znacznie bardziej dotkliwa niż zgubiony lub skradziony komputer.

Co zyskujesz, dbając o cyberbezpieczeństwo?



01

Zmniejszenie ryzyka

Inwestycje w cyberbezpieczeństwo redukują ryzyko i identyfikują zagrożenia, na jakie narażona jest organizacja. Dzięki nim można łatwo zaplanować wdrożenie firmowych procedur i powstrzymać lub chociaż złagodzić zagrożenia płynące z sieci i nie tylko. Działania nastawione na bezpieczeństwo pozwalają wyciągnąć wnioski na temat efektywności i wydajności pracy działów IT w Twojej firmie. Pamiętaj, że wszystko, co zagraża systemom, staje się automatycznie zagrożeniem dla działalności całej organizacji.

02

Poprawa bezpieczeństwa

W szybko zmieniającej się rzeczywistości dysponowanie narzędziami do zapobiegania oszustwom i cyberatakom w firmach jest niezwykle istotne. Stałe trzymanie ręki na pulsie pozwala ulepszać systemy chroniące firmowe dane, a także identyfikować i eliminować luki w bezpieczeństwie. Sama świadomość wdrażania przez firmę restrykcyjnych procedur z zakresu cyberbezpieczeństwa może zniechęcić potencjalnych przestępców do podejmowania działań szkodliwych dla danej organizacji.

03

Większa świadomość zagrożeń

Mądra strategia cyberbezpieczeństwa obejmuje cykliczne szkolenia pracowników, a odpowiednio przeszkolony zespół staje się kluczem do wysokiego poziomu ochrony firmy. Starannie przeprowadzone kursy zwiększają świadomość, przekazują niezbędną wiedzę i budują pewność siebie pracowników, dzięki czemu potrafią oni precyzyjnie rozpoznać na przykład ataki z użyciem socjotechnicznych manipulacji. Co więcej, dobrze zrealizowane szkolenia wzmacniają również znaczenie edukacji i rozwoju pracowników w Twojej firmie.

04

Większe zaufanie klientów

Cyberataki często osłabiają wizerunek biznesowy firmy. Incydenty mogą spowodować nie tylko utratę klientów, ale i trudności w pozyskiwaniu nowych partnerów. Wszystko przez to, że relacje biznesowe z organizacjami, które doświadczyły skutków cyberataków, są traktowane jako bardzo ryzykowne. Inwestycje w cyberbezpieczeństwo są pomocne w kontaktach z klientami. Jeśli Twoi partnerzy wiedzą, że aktywnie działasz na rzecz cyberbezpieczeństwa, ich zaufanie do Twoich produktów i usług na pewno wzrośnie.

05

Oszczędności

Koszty usunięcia skutków pojedynczego cyberataku lub innego incydentu mogą być naprawdę ogromne. Jak wynika z raportu IBM Security (2021–2022), światowe firmy tracą średnio 4 mln dolarów rocznie z powodu ataków hakerów. Środki przeznaczane na cyberbezpieczeństwo w firmie nie są zatem kosztem, lecz mądrą inwestycją. Dobre i efektywne szkolenie z cyberbezpieczeństwa czy audyt IT zawsze będą tańsze niż na przykład niwelowanie skutków wycieków danych.

KROK 1

Audyt cyberbezpieczeństwa

Audyty IT mają na celu solidne przetestowanie systemów informatycznych, sieci, stosowanych aplikacji oraz procedur bezpieczeństwa wdrożonych w firmie. Dzięki takim procesom organizacje mogą upewnić się, że ich działy IT działają płynnie i efektywnie.

Audyty cyberbezpieczeństwa są niezbędne w firmach, które chcą chronić swoje systemy informatyczne i sprzęt na najwyższym poziomie. Postrzegane są jako niezwykle istotny element strategii cyberbezpieczeństwa w firmie – zaraz obok stałej modernizacji technologii.

Co może obejmować audyt IT?

- analiza firmowej infrastruktury sieciowej i sprzętowej
- sprawdzenie bezpieczeństwa fizycznego w firmie
- analiza bezpieczeństwa witryn internetowych i poczty e-mail
- analiza dokumentacji dotyczącej cyberbezpieczeństwa
- analiza ryzyka
- raport z rekomendacjami w zakresie cyberbezpieczeństwa

Co zyskuje Twoja firma dzięki audytom IT?

- wskazanie mocnych i słabych stron aktualnych środków bezpieczeństwa
- identyfikacja błędów w infrastrukturze IT i propozycje działań naprawczych
- wyznaczenie kierunku działań zmierzających do zachowania najwyższego poziomu cyberbezpieczeństwa
- dane, które służą do tworzenia programów szkoleniowych dla pracowników
- wiarygodność i większe zaufanie wśród partnerów biznesowych

KROK 2

Zabezpieczenie infrastruktury firmowej

Bezpieczeństwo firmowej infrastruktury IT zapewnia ciągłość działania biznesu, ale często jest wręcz kluczowe dla jego dalszego istnienia. Dziś każda firma ma do czynienia ze sprzętem komputerowym, a przestępców łatwiej spotkać w Internecie niż na ulicy. Jeżeli zatem Twoja firma jest na stałe podłączona do sieci internetowej, a na pewno jest, musisz naprawdę zainteresować się tym obszarem.

Polityka bezpieczeństwa

Odpowiednie procedury cyberbezpieczeństwa w firmie pozwalają na przyswojenie przez pracowników właściwych nawyków. Dotyczy to zarówno korzystania z Internetu i aplikacji firmowych, jak i przetwarzania danych.

Aktualizacje systemów operacyjnych i aplikacji

Wszystkie sprzęty komputerowe w organizacji wymagają instalacji najnowszych aktualizacji aplikacji i sterowników. Wpływa to nie tylko na poprawę bezpieczeństwa, ale także na komfort pracy pracowników.

Aktualizacje programów antywirusowych

Firmy powinny zwracać uwagę na to, jak często aktualizowane jest oprogramowanie antywirusowe, które ma zapewnić ochronę przed trojanami, wirusami i „robakami". Dobrym pomysłem jest wybór programu antywirusowego z tzw. zaporą ogniową, czyli firewall'em, która dodatkowo chroni przed atakami hakerskimi.

Monitoring IT

Warto, aby każda organizacja stawiała na bieżące obserwowanie funkcjonowania procesów i systemów IT w firmie. Takie działanie często pozwala na szybkie rozpoznanie cyberzagrożeń, a nawet zduszenie ich w zarodku.

Zabezpieczenie poczty e-mail

Podejmując inwestycje IT, warto upewnić się, czy dostawca serwerów i poczty e-mail dla firmy gwarantuje skanowanie korespondencji przed jej pobraniem. Wybierając najlepsze rozwiązanie, można uchronić organizację przed wirusami infekującymi sieci firmowe oraz oszustwami typu phishing.

Szyfrowanie urządzeń

Właściciele firm czy menedżerowie wyższego szczebla muszą dbać o odpowiednie szyfrowanie urządzeń, które korzystają z zasobów znajdujących się w firmowej sieci. Dotyczy to nie tylko komputerów, ale także serwerów wewnętrznych czy przenośnych nośników pamięci.

Usługi chmurowe

Rozwiązania chmurowe zgodne z RODO/UODO wyjątkowo dobrze chronią dane firmowe. Warunkiem jest poprawne konfigurowanie i używanie chmury oraz eliminowanie zagrożeń wynikających z działań ludzkich.

Kopie zapasowe

Wykonywany poprawnie backup, jego regularne testowanie i posiadanie planu jego odtworzenia pozwalają na relatywnie szybkie i sprawne przywrócenie utraconych danych. Takie podejście do tematu związanego z kopiami zapasowymi sprawia, że właściciele firm mogą spać spokojnie, bez obawy przed utratą informacji.

KROK 3

Zabezpieczenie miejsca pracy

Zapewnienie pełnego bezpieczeństwa pracownikom w biurach oraz pracownikom zdalnym to ogromne wyzwanie. Pomaga w tym szereg procedur firmowych i narzędzi, które organizują codzienną pracę zespołów niezależnie od miejsca ich pracy.

Co wspiera wprowadzenie konkretnych standardów bezpieczeństwa?

VPN (Virtual Private Network)

Praca zdalna to obecnie rzeczywistość wielu organizacji. Właśnie dlatego rozwiązaniem niezbędnym w każdej firmie powinna być sieć VPN. Wirtualna sieć prywatna chroni nie tylko tożsamość pracowników, ale gwarantuje przedsiębiorstwu bezpieczny dostęp do stron internetowych, aplikacji i systemów do codziennej pracy, a także bezpieczne przesyłanie plików między rozproszonymi zespołami. Aby jednak poprawnie korzystać z VPN, należy się najpierw odpowiednio przeszkolić.

Polityka czystego biurka i czystego ekranu

Zarówno biurko, jak i ekran monitora są miejscami, w których przetwarzane są najróżniejsze rodzaje danych. Właśnie dlatego każda firma powinna dokładać wszelkich starań, aby pracownicy nie pozostawili na biurkach ważnych dokumentacji i chronili ekrany przed wzrokiem osób nieupoważnionych. Jeśli jednak Twoi pracownicy po ukończonej pracy sprzątają z biurka głównie kubki po kawie, zadbaj o odpowiednie procedury i zapoznaj z nimi swoje zespoły, aby jak najlepiej chronić firmę przed zagrożeniami.

GROMAR

Cyberbezpieczny pracownik

Interaktywne szkolenie e-learningowe
dla Twojego zespołu

Zamów teraz

Kontakt

48 42 279 70 20

sprzedaz@gromar.eu

KROK 4

Testy socjotechniczne i próby phishingowe

Jednym z największych **zagrożeń bezpieczeństwa** w firmach są działania socjotechniczne, które polegają na tym, że cyberprzestępcy wywierają wpływ na pracowników i manipulują nimi w celu kradzieży danych firmowych lub złamania najróżniejszych zabezpieczeń. W tym przypadku hakerzy nie atakują infrastruktury IT, lecz wykorzystują zachowania pracowników, ich lęki, lekkomyślność, a także brak wiedzy.

Jak wynika z danych CERT Polska, najczęstszym rodzajem oszustw jest phishing, czyli podszywanie się pod inną osobę w celu uzyskania cennych informacji firmowych.

Kampanie phishingowe cyberprzestępców w formie wiadomości e-mail, linków wysyłanych w komunikatorach internetowych czy kontaktów telefonicznych są praktycznie na porządku dziennym.

Scenariusze prawdziwych ataków hakerskich są wykorzystywane w testach socjotechnicznych i próbach phishingowych, które są działaniem symulowanym, bezpiecznymi i w pełni kontrolowanym przez firmę.

Jak mogą wyglądać testy socjotechniczne?

Test socjotechniczny polega często na kontakcie mailowym z pracownikami i próbie pozyskania danych logowania do ich kont internetowych. Symulowana wiadomość e-mail może mieć na celu także aktywowanie złośliwego oprogramowania.

Testy socjotechniczne najczęściej przeprowadzają firmy wyspecjalizowane w zakresie cyberbezpieczeństwa.

Co może obejmować audyt IT?

- Sprawdza świadomość pracowników w zakresie cyberzagrożeń.
- Umożliwia przygotowanie pełnego raportu, który obrazuje poziom wiedzy pracowników.
- Pozwala na przygotowanie kompleksowego szkolenia dla pracowników nietechnicznych, które będzie dostosowane do potrzeb organizacji.

WAŻNE! Testy socjotechniczne wykonuje się również po przeprowadzonym szkoleniu. Wówczas celem jest zbadanie, czy pracownicy w odpowiednim stopniu przyswoili treści szkoleniowe.

KROK 5

Szkolenia z zakresu cyberbezpieczeństwa dla pracowników

Szkolenia z zakresu cyberbezpieczeństwa dla pracowników

Jak wynika z badań, aż 95% przypadków naruszeń bezpieczeństwa danych w organizacjach jest spowodowanych błędami pracowników. Dlatego tak ważne jest stałe edukowanie zespołów nietechnicznych.

Postaw na e-learning

Odpowiedzią na potrzeby firm są szkolenia z cyberbezpieczeństwa dla pracowników i kadry kierowniczej od GroMar. Szkolenia są realizowane w wygodnej formie e-learningu.

Ich zakres dostosowany jest poziomu wiedzy zespołu oraz procedur wewnętrznych w organizacji. Osadzenie szkolenia na wygodnej platformie e-learningowej sprawia, że łatwo jest zmierzyć postępy uczestników.

Przykładowe tematy poruszane podczas naszych szkoleń

- Zasady tworzenia bezpiecznych haseł
- Socjotechnika
- Bezpieczna poczta e-mail
- Bezpieczna praca zdalna
- OSiNT
- Efektywne korzystanie z managera haseł
- Phishing
- Szyfrowanie dokumentów
- Zagrożenia w sieciach publicznych
- Audyt bezpieczeństwa i testy penetracyjne
- Dezinformacja i fake newsy
- Uwierzytelnianie dwuskładnikowe (2FA)
- Ransomware i malware
- Antywirusy i aktualizacje
- VPN
- Zagrożenia wewnętrzne
- Postępowanie w razie ataku
- Polityka cyberbezpieczeństwa
- Cyberataki przez telefon
- Mit zielonej kłódki
- Bezpieczna praca z chmurą
- Certyfikaty ISO 27001 oraz ISO 22301

Dlaczego szkolenie e-learningowe GroMar będzie dobrze służyć Twojej firmie?

Profesjonalizm

Autorami szkolenia są praktycy, którzy tworzą pełne strategie bezpieczeństwa IT dla firm.

Interaktywność

Szkolenie zawiera quizy, zadania, animacje i filmy, które angażują uczestników znacznie bardziej niż zwykłe webinary i wpływają na lepsze zapamiętanie treści.

Moduły

Szeroki zakres bloków tematycznych pozwala jak najlepiej dopasować kurs do potrzeb organizacji.

E-learning

Nasz kurs to idealny materiał szkoleniowy z dostępem do platformy e-learningowej, która pozwala sprawdzić, czy wszyscy uczestnicy zaliczyli szkolenie.

Prostota w odbiorze

Treści szkolenia są zrozumiałe dla wszystkich pracowników nietechnicznych w firmie.

Najwyższa jakość

Zapewniamy najwyższe standardy wizualne i techniczne kursu cyberbezpieczeństwa.

Co dają firmie szkolenia pracowników z cyberbezpieczeństwa?

- Wspierają ochronę Twojej firmy przed cyberoszustami i wyciekami danych.
- Chronią biznes przed konsekwencjami prawnymi i ogromnymi kosztami usuwania skutków incydentów.
- Zwiększają świadomość zagrożeń wśród pracowników.
- Ułatwiają uzyskanie prestiżowych certyfikatów, np. certyfikatu ISO/IEC 27001, który zapewnia, że aktywa informacyjne w firmie są odpowiednio chronione.
- Budują przewagi konkurencyjne i zaufanie w oczach kontrahentów.

Podsumowanie

W cyfrowym świecie błędy ludzkie sprawiają, że ataki cyberprzestępców są coraz skuteczniejsze. Siła przedsiębiorstwa tkwi zatem nie tylko w stosowaniu najnowszych technologii, ale w odpowiednio przeszkolonym zespole, który staje się kluczem do wysokiego poziomu cyberbezpieczeństwa firmy.

Solidne, cykliczne szkolenia z cyberbezpieczeństwa zwiększają świadomość, przekazują niezbędną wiedzę i budują pewność siebie wśród pracowników, którzy potrafią precyzyjnie rozpoznać na przykład ataki z zastosowaniem socjotechnicznych manipulacji.

Aktualne materiały edukacyjne online i stały dostęp do nich na platformie e-learningowej wzmacniają znaczenie edukacji i rozwoju pracowników w zakresie bezpieczeństwa technologii w Twojej firmie.

Im większą wiedzę ma Twój team, tym lepszym mechanizmem obronnym

Kontakt

Napisz do nas i już teraz postaw na szkolenia z zakresu cyberbezpieczeństwa dla pracowników nietechnicznych.

Zadbaj o rzetelną wiedzę pracowników biurowych i kadry zarządzającej oraz chroń swój biznes przed niechcianymi wyciekami danych, które kosztują miliony i grożą utratą reputacji.

Porozmawiajmy!

Napisz do nas na adres: **sprzedaz@gromar.eu**
lub poprzez formularz na stronie **www.gromar.eu**

Zadzwoń: **+48 42 279 70 20**