PRZEWODNIK

Jak chronić biznes przed cyfrowymi zagrożeniami w 2023?

GRANDMETRIC
STAY CONNECTED.

SPIS TREŚCI

Dlaczego cyberbezpieczeństwo jest tak ważne?

Intensywna digitalizacja i wykorzystanie sieci w niemal wszystkich sferach życia wiąże się ze zwiększoną potrzebą ciągłej, aktywnej obrony przed cyfrowymi zagrożeniami.

W fabrykach, magazynach, galeriach handlowych, biurowcach czy w domach - jesteśmy odpowiedzialni za zabezpieczenia nie tylko fizyczne, ale też cyfrowe.

Tym bardziej, że ataki przeprowadzają obecnie nie pojedynczy hakerzy, ale zorganizowane grupy przestępcze, czerpiące zyski z atakowania infrastruktury coraz większej grupy firm, które nie są zabezpieczone. Wielkość firm nie ma dla nich najmniejszego znaczenia.

Zwięźle rzecz ujmując, zaniedbania w dziedzinie bezpieczeństwa informatycznego to zaproszenie cyberprzestępców do zarabiania naszym kosztem.

Przeczytaj nasz przewodnik i zabezpiecz się, by nie musieć uczyć się na błędach!

Zespół Grandmetric

Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to całokształt działań, których celem jest ochrona danych, użytkowników i systemów firmowych przed atakami cyfrowymi czy utratą danych z powodu awarii.

Jeśli sądzisz, że ta kwestia Cię nie dotyczy, jesteś w błędzie. Cyberatak to tylko kwestia czasu.

Policz, z ilu urządzeń podłączonych do Internetu korzystasz. Zastanów się, na ile maili dziennie odpowiadasz. Ile nieznajomych osób pisze do Ciebie w mediach społecznościowych. Pewnie korzystasz w biurze z prywatnego telefonu, nie zdając sobie sprawy, że może być zainfekowany. Ktoś bez problemu podłącza do lokalnej sieci prywatny komputer, na którym potencjalnie szaleją wirusy albo niebezpieczne oprogramowanie.

Co to jest cyberbezpieczeństwo?

A może po prostu w piątek po południu, kiedy dopada Cię zmęczenie, zdarza Ci się klikać w załączniki do maili albo w linki od nadawców, którzy tylko z pozoru wyglądają znajomo i w związku z tym - niegroźnie.

Hakerzy atakują polskie firmy zdecydowanie częściej niż się wydaje: średnio **938 razy** tygodniowo. To wzrost o **35%** w stosunku do stycznia 2022 r. – podaje Check Point Research.

Każda tego typu sytuacja to potencjalny atak. Każda z nich jest niebezpieczna dla biznesu, bo stanowi furtkę do firmowych danych, do spisanych procedur i know-how oraz chronionych RODO danych osobowych pracowników i kontrahentów. Wyciek takich danych to milionowe kary, które nie ominą ani wielkich firm takich jak mBank, ani mniejszych organizacji, takich jak Twoja firma.

Zgodnie z art. 83 ust. 4 i 5 RODO Prezes Urzędu Ochrony Danych Osobowych może nałożyć 2 rodzaje administracyjnych kar pieniężnych za naruszenie RODO:

- w wysokości do **10 mln euro**, a w przypadku przedsiębiorstwa – do **2%** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, lub
- w wysokości do **20 mln euro**, a w przypadku przedsiębiorstwa – do **4%** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Jakie są realne skutki ataków na firmy?

W ciągu kilku ostatnich lat diametralnie wzrosła liczba udanych cyberataków w celu wymuszenia okupu. Około **60%** zaatakowanych organizacji łamie się pod presją cyberprzestępców i płaci haracz.

Jak podaje portal Niebezpiecznik.pl, gangi ransomware wykradają miesięcznie olbrzymie ilości danych – ponad 10 terabajtów. Aby lepiej to zobrazować – 10 TB to 10 000 godzin materiałów wideo w jakości Full HD (każda godzina zajmuje około 1GB) lub 2 500 godzin wideo w jakości 4K.

Działa na wyobraźnię, prawda?

W 2022 roku aż **69%** polskich firm zanotowało przynajmniej jeden incydent naruszenia cyberbezpieczeństwa

Według firm, to właśnie **ransomware** stanowi obecnie największe zagrożenie cyberbezpieczeństwa.

W 2022 roku **1/3** firm odnotowała wzrost intensywności cyberataków na swoje systemy.

Jakie są realne skutki ataków na firmy?

Co grozi firmie, która wpuści do swojej infrastruktury hakera?

Straty finansowe - haracze, odzyskiwanie danych, przywracanie działania zainfekowanej infrastruktury, zatrudnianie specjalistów ds. cyberbezpieczeństwa, utrata przychodów kosztują, i to niemało.

Kary finansowe za wyciek danych osobowych - na podmioty, które niewystarczająco zabezpieczyły informacje chronione na mocy RODO, nakładane są wysokie kary.

Utrata dostępu do danych i systemów informatycznych - zakłóca działalność biznesową na długi czas, może nawet doprowadzić do bankructwa zaatakowanej firmy.

Zatrzymanie produkcji - wiąże się z utratą dochodów i kosztami ponownego uruchomienia działalności.

Wyciek danych objętych umowami o poufności - oznacza kroki prawne wynikające z niedotrzymania warunków umów.

Straty wizerunkowe - cierpi reputacja firmy, spada zaufanie inwestorów, klientów i kontrahentów.

- Straty finansowe
- Zatrzymanie produkcji
- Kary finansowe za wyciek danych objętych RODO
- Kroki prawne ze strony klientów za wyciek danych objętych umowami o poufności
- Utrata dostępu do danych i systemów informatycznych
- Straty wizerunkowe

Najbardziej powszechne zagrożenia

Złośliwe oprogramowanie, czyli *malware* - to oprogramowanie zaprojektowane po to, by wyrządzić szkody na zainfekowanym urządzeniu użytkownika. Zaliczają się do nich wirusy, konie trojańskie (tzw. trojany), oprogramowanie szpiegujące (*spyware*) czy wymuszające okup (*ransomware*).

Oprogramowanie wymuszające okup, czyli *ransomware* - to oprogramowanie, przy pomocy którego przestępcy blokują dostęp do danych lub systemów komputerowych. Ich najczęstszą motywacją są szybkie pieniądze, żądają więc od ofiar okupu w zamian za odszyfrowanie danych. Cyberatak *ransomware* to coraz bardziej powszechna i zaawansowana technologicznie forma przestępstwa hakerskiego.

Z raportu KPMG „Barometr cyberbezpieczeństwa 2022” wiemy, że prawie **2/3** badanych organizacji odnotowało incydenty naruszenia bezpieczeństwa, a niemal **1/3** przyznała, że w przeszłości padła ofiarą ataku typu *ransomware*.

Najbardziej powszechne zagrożenia

Wyłudzanie informacji, czyli *phishing* - to technika cyberataków, której celem jest wyłudzenie poufnych informacji.
Ataki z użyciem *phishingu* mają nas "złowić" w momencie, kiedy się tego nie spodziewamy. Działając z zaskoczenia atakujący będzie chciał nas zmusić do:

- Podania danych logowania (np. do banku) na spreparowanej stronie www.
- Podania danych karty płatniczej.
- Podania danych osobowych (np. numeru dowodu osobistego, numeru PESEL, nazwiska panieńskiego matki i innych danych, które są wykorzystywane przez instytucje finansowe do weryfikacji tożsamości).
- Pobrania pliku ze złośliwym oprogramowaniem, np. faktury, wezwania do zapłaty, oferty.

Odmowa usługi, czyli atak typu DoS (*Denial of Service*) - to uniemożliwienie użytkownikowi dostępu do danych lub usług. Najczęściej polega na celowym przeciążeniu infrastruktury sieciowej i zablokowaniu w ten sposób możliwości dostania się do niej. W ekstremalnych przypadkach może doprowadzić do zablokowania dostępu do systemu na długi czas.

Przykłady ataków na polskie przedsiębiorstwa

Hakerzy nie mają sentymentów i nie oszczędzą nikogo. Ich ofiarą padają nie tylko “zwykłe” przedsiębiorstwa, ale także instytucje edukacyjne, a nawet te zajmujące się ratowaniem życia.

Cybertak na Lotnicze Pogotowie Ratunkowe (02.2022)
Przez ponad tydzień po ataku cyberprzestępców jednostki LPR w całym kraju były pozbawione możliwości korzystania ze swoich systemów komputerowych. Niedostępne były systemy kluczowe dla działania pogotowia, jak system przesyłania informacji o prowadzonych interwencjach, strona www i poczta elektroniczna. Hakerzy zażądali okupu w wysokości 390 tysięcy dolarów, czyli około 1,5 mln złotych.

Cyberatak na Instytut Centrum Zdrowia Matki Polki w Łodzi (11.2022)
Celem hakerów padł łódzki Instytut Centrum Zdrowia Matki Polki. By zminimalizować skutki cyberataku, szpital zdecydował się na czasowe wyłączenie systemów informatycznych i obsługiwanie pacjentów przy wykorzystaniu tradycyjnej papierowej dokumentacji. Poważnie zakłóciło to normalne funkcjonowanie tej instytucji, opóźniając wydawanie dokumentacji medycznej, wypisywanie pacjentów i szereg innych, niezwykle wrażliwych procedur.

Przykłady ataków na polskie przedsiębiorstwa

Cybertak na Urząd Marszałkowski Województwa Mazowieckiego (12.2022)

Hakerzy zaszyfrowali dostęp do systemu Elektronicznego Zarządzania Dokumentami w Urzędzie Marszałkowskim Województwa Mazowieckiego. Doprowadziło to do wyłączenia infrastruktury projektowej Węzła Regionalnego, a ponad 300 jednostek samorządu terytorialnego straciło do niej dostęp musząc odłączyć się od sieci. Urząd Marszałkowski stracił również akces do danych osobowych, którymi administrował. Oficjalnie nie potwierdzono ich wycieków ani ujawnienia, urząd poinformował jednak, że “istnieje duże prawdopodobieństwo, że dane przetwarzane w systemach objętych incydentem są w posiadaniu osób trzecich.”

Cyberatak na system Śląskiej Karty Usług Publicznych (02.2023)

Cyberprzestępcy zaatakowali system Śląskiej Karty Usług Publicznych, służącej między innymi do płatności za parkowanie czy bilety komunikacji miejskiej w Metropolii Górnośląsko-Zagłębiowskiej. Blokada utrudniała codzienne życie prawie 2 milionów mieszkańców tego obszaru przez niemal dwa tygodnie. System przywrócono do działania przy pomocy tworzonych codziennie kopii zapasowych, a dane osobowe pasażerów nie były zagrożone tylko dzięki temu, że system ich nie gromadził.

Od czego zacząć?

Dobra wiadomość jest taka, że działania zwiększające cyfrowe bezpieczeństwo można łatwo wdrożyć bez ogromnych inwestycji. A podstawowy poziom bezpieczeństwa można (i należy!) wdrożyć za darmo w każdej organizacji. Jak?

1. **Nie korzystaj z jednego hasła do wszystkich systemów**
Taką sytuację można porównać do otwierania wszystkich zamków w mieszkaniu jednym kluczem. Niezbyt efektywne, prawda? Z drugiej strony, zrozumiałe jest, że trudno zapamiętać kilkanaście (czy nawet kilkadziesiąt!) skomplikowanych haseł do wielu systemów. Skutecznym rozwiązaniem tego problemu jest używanie menedżerów haseł, takich jak np. Bitwarden, Dashlane czy LastPass.

Hakerzy na całym świecie inicjują ok. **2 miliony** ataków rocznie. Autorzy raportu Accenture „State of Cybersecurity Resilience 2021" szacują, że w 2023 r. globalny koszt cyfrowych przestępstw przekroczy **11 trylionów dolarów**, by w 2027 podwoić się i sięgnąć niemal **24 trylionów dolarów**.

Od czego zacząć?

2 **Nie otwieraj podejrzanych linków i załączników do maili**
Zwłaszcza, jeśli są wysyłane przez nieznane osoby, z podejrzanych domen lub zawierają ograniczone czasowo, nad wyraz kuszące oferty. Unikaj pobierania oprogramowania z podejrzanych źródeł.

3 **Uaktualniaj swoje oprogramowanie i system operacyjny**
Regularnie korzystaj z najnowszych wersji zabezpieczeń i wsparcia producentów sprzętu. Dbaj o higienę swojej sieci i odpowiednio zarządzaj uprawnieniami dostępu do firmowych zasobów.

4 **Korzystaj z oprogramowania antywirusowego**
Podstawową ochronę zapewnią Ci nawet darmowe programy antywirusowe, jak Avast, Comodo czy Avira.

5 **Stwórz i egzekwuj politykę korzystania wyłącznie z zaufanego sprzętu**
Jeśli to nie jest konieczne, niech pracownicy nie korzystają w biurze z prywatnych urządzeń czy nośników danych. Ich status i kondycja nie są znane, a łatwo mogą stać się źródłem infekcji.

6 **Regularnie twórz kopie zapasowe swoich danych**
Najlepiej na zewnętrznych dyskach twardych albo w chmurze. Idealnie – wg **zasady 3-2-1**. Dla wszystkich danych stwórz trzy kopie, na dwóch różnych nośnikach danych, z jedną kopią przechowywaną poza główną siedzibą organizacji.

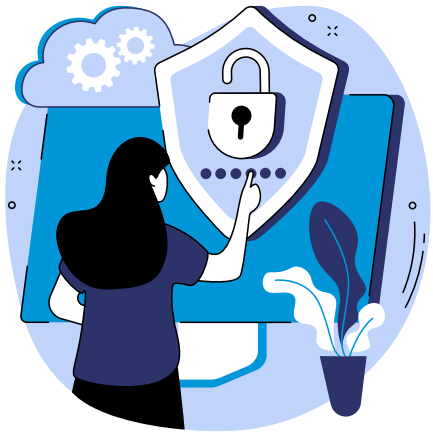
7 **Zawsze zmieniaj hasła systemowe**
Na routerach, punktach dostępowych, drukarkach i innych urządzeniach - nigdy nie korzystaj z hasła producenta, bo zna je każdy administrator, a już na pewno taki o nieczystych intencjach.

Rozwiązania cyberbezpieczeństwa dla firm

Dbanie o cyberbezpieczeństwo to nie domena smutnych panów we flanelach. To obowiązek każdego menadżera i właściciela firmy. Zresztą, możesz mieć najlepszego specjalistę informatyka czy administratora, ale on też będzie bezradny, jeśli nie dasz mu narzędzi, by chronił firmę przed atakami. A te nastąpią, raczej prędzej niż później.

Trzymanie żółtych karteczek z hasłem przy komputerze wcale nie jest taką rzadkością, jak mogłoby się wydawać.

Podobnie korzystanie z tego samego, prostego hasła jak *piesek123* albo *adminadmin* czy łączenie się ze służbowego laptopa do dowolnej otwartej sieci bezprzewodowej. Takie zachowania to proszenie się o kłopoty.



Średni czas złamania prostego hasła przez hakera to zaledwie kilka sekund - w tak krótkim czasie może zalogować się do poczty e-mail, pobrać dane osobowe, czy zablokować dostęp do zasobów firmowych. Słowem, sparaliżować działanie całego przedsiębiorstwa, narazić je na finansowe i wizerunkowe straty.

Średni atak *ransomware* na polskie firmy oznacza straty rzędu **1,5 miliona** złotych. Ryzyko jest wymierne!

Dlatego tak ważne jest, by oprócz bezpiecznych narzędzi firmowych takich jak laptopy, telefony i skrzynka mailowa zapewnić pracownikom bezpieczny dostęp do urządzeń, sieci i informacji, które są dzisiaj najcenniejszą walutą.

1

Zabezpiecz sieć przed atakami - *firewall*

Dzisiaj metody atakujących są coraz bardziej różnorodne, zwykły *firewall* to zdecydowanie za mało. Dlatego powstała klasa urządzeń *Next-Generation Firewall* (NGFW), które oprócz klasycznej zapory posiadają szereg zaawansowanych zabezpieczeń takich jak:

- **Zaawansowane filtrowanie treści i kontrola aplikacji** – *firewall* potrafi rozpoznawać i blokować ruch generowany przez aplikacje, które nie są zaufane lub są niebezpieczne.
- **Wykrywanie i blokowanie zaawansowanych zagrożeń** – NGFW używa różnych technik, takich jak analiza zachowania aplikacji i wykrywanie złośliwych adresów IP, aby zidentyfikować i blokować zagrożenia.
- **Integracja z innymi warstwami ochrony sieci**, np. systemami klasy NAC.

Przeczytaj nasz bezpłatny przewodnik po firewallach dla MŚP

Pobierz

2

Zarządzaj dostępem do sieci - system klasy NAC (*Network Access Control*)

Sprawdzi się w organizacjach, które muszą szczególnie dbać o separację ruchu i poziomy dostępu do sieci i zasobów. Stosunkowo prosty w konfiguracji, ma znaczący wpływ na zapewnienie bezpiecznego dostępu dla użytkowników o różnych uprawnieniach, w tym dla gości.

System NAC, taki jak np. Cisco ISE daje wgląd w to, co dzieje się w sieci – kto jest połączony, jakie aplikacje ma zainstalowane i uruchomione etc. Udostępnia również istotne dane kontekstowe, jak tożsamość użytkowników i urządzeń, zagrożenia i luki w zabezpieczeniach, dzięki czemu można szybciej identyfikować i eliminować zagrożenia.

3

Uchroń się przed *phishingiem* - blokowanie zagrożeń

Można się przed nim zabezpieczyć za pomocą rozwiązań, które na podstawie miliardów przeanalizowanych przypadków potrafią znacznie lepiej niż człowiek rozpoznać zagrożenie i zablokować je, zanim wywoła spustoszenie w Twojej organizacji.

Takim rozwiązaniem jest np. Cisco Umbrella, które wykorzystuje zaawansowane mechanizmy uczenia maszynowego, żeby skutecznie wykrywać niebezpieczne aktywności w Internecie i blokować je zanim pracownicy dadzą się na nie nabrać.

Możesz bezpłatnie przetestować Umbrellę przy wsparciu Grandmetric

Sprawdź

4

Zabezpiecz się nie tylko hasłem - uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe (*Multi-Factor Authentication*, czyli MFA) to środek bezpieczeństwa, który zapewnia podwójną lub potrójną weryfikację tożsamości użytkownika, zanim pozwoli mu się na dostęp do danych. Użycie dodatkowego składnika uwierzytelniającego (fizycznego lub cyfrowego tokenu, kodu SMS, biometrii czy powiadomienia *push* w aplikacji) dobrze się sprawdza szczególnie w przypadku zabezpieczenia dostępu zdalnego poza siedzibą organizacji.

Cisco proponuje rozwiązanie do uwierzytelniania wieloskładnikowego Cisco DUO, którego mocną stroną jest możliwość integracji z większością aplikacji, bez nadmiernego obciążania działu IT. Dzięki temu narzędziu użytkownik zwolniony jest z obowiązku zapamiętywania długich i skomplikowanych haseł. W praktyce eliminuje to problem zapisywania skomplikowanych haseł na karteczkach albo używaniem jednego hasła wszędzie, gdzie to możliwe.

5

Chroń użytkowników sprzętów podłączonych do Internetu – ochrona urządzeń brzegowych

Endpoint Security to znane od wielu lat zabezpieczenia urządzeń końcowych z dostępem do Internetu, takich jak telefony komórkowe, laptopy, komputery stacjonarne czy drukarki.
W dobie rozwoju Internetu Rzeczy (eng. IoT, *Internet of Things*), do grona endpointów zaliczamy też urządzenia medyczne, bankomaty, smartwatche, a nawet lodówki i pralki.
Dodatkowy czynnik ryzyka stanowi też obecna w wielu miejscach polityka BYOD (*Bring Your Own Device*), polegająca na łączeniu się do systemów firmowych z dowolnych urządzeń, również prywatnych.
Cisco ma w swoim portfolio zaawansowane rozwiązania Cisco Secure Endpoint, które pozwala śledzić wszystkie urządzenia podłączone do sieci w jednej konsoli, instalować na nich aktualizacje i wymuszać korzystanie z polityki bezpieczeństwa firmy.

Zobacz przegląd 6 rozwiązań bezpieczeństwa od Cisco

Co zrobić, gdy padniesz ofiarą *phishingu* lub *ransomware*?
Niezwłocznie zgłoś sprawę na policję oraz do zespołu CERT Polska na stronie internetowej **https://incydent.cert.pl**

Jak wybrać odpowiednie rozwiązania bezpieczeństwa?

Mnogość istniejących na rynku rozwiązań cyberbezpieczeństwa może wydać się przytłaczająca.

- **Które obszary chronić w pierwszej kolejności?**
- **Czy wszystkie są tak samo istotne?**
- **Czy rozwiązania różnych producentów będą ze sobą współpracować?**
- **Czy trzeba wymienić używany dotąd sprzęt?**

To bardzo częste pytania i bez odpowiedniego kontekstu i przygotowania nie można na nie jednoznacznie odpowiedzieć.
Na część trudno odpowiedzieć samodzielnie.

Jeśli zastanawiasz się, czy obecne rozwiązania spełniają realne potrzeby Twojej organizacji, najwyższy czas im się przyjrzeć!

Nasi inżynierowie pomogą Ci nie tylko postawić diagnozę, ale też dobrać i wdrożyć konkretne rozwiązanie dopasowane do Twojej organizacji.

Porozmawiajmy

JAK MOŻEMY CI POMÓC?

Zajmujemy się projektowaniem, automatyzacją i utrzymywaniem bezpiecznych sieci przewodowych, bezprzewodowych i systemów IoT.

Prowadzimy kompleksowe projekty transformacji technologicznej IT oraz projektujemy bezpieczne sieci w nowych budynkach.

Dostarczamy sprzęt informatyczny oraz rozwiązania bezpieczeństwa, integrujemy je z istniejącymi systemami, konfigurujemy i dbamy o ich utrzymanie.

Dowiedz się więcej

KONTAKT

Zastanawiasz się, które usługi cyberbezpieczeństwa przyniosą rzeczywiste korzyści Twojej organizacji?

Zaplanuj bezpłatną konsultację z naszym ekspertem.

61 271 04 43

sales@grandmetric.com

Skontaktuj się z nami