Autentykacja wieloskładnikowa:

Prosta, elastyczna i mocna ochrona

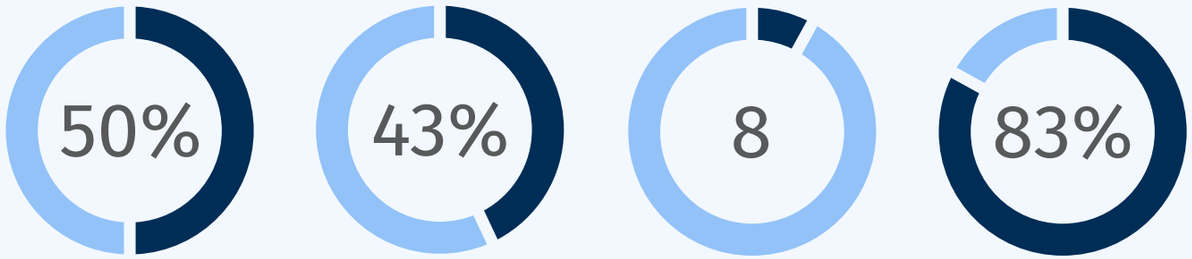
Niezbędna ochrona dla małych i średnich przedsiębiorstw

EBOOK

Wysoki koszt niskiego bezpieczeństwa

Cyberataki każdego dnia stają się coraz bardziej zaawansowane. Sprytni cyberprzestępcy w alarmującym tempie wykorzystują słabe, przestarzałe metody i standardy zabezpieczeń do uzyskiwania dostępu do kont i wrażliwych informacji.

Dramatyczny wzrost liczby cyberataków oznacza, że zwiększone środki bezpieczeństwa nie są jedynie zalecane - są one kluczowe. Szczególnie dotyczy to małych i średnich przedsiębiorstw (MŚP), które teraz, jak nigdy dotąd, doświadczają skutków finansowych, reputacyjnych i operacyjnych.



Wzrost liczby cyberataków w ciągu ostatniego roku[1]

Cyberataki skierowane przeciwko małym przedsiębiorstwom

Godziny straconego czasu po typowym naruszeniu bezpieczeństwa

Procent MŚP nieprzygotowanych finansowo na odbudowę po ataku [2]

Te statystyki są przerażające, ale istnieje rozwiązanie: 80-90% wszystkich cyberataków można zapobiec dzięki zastosowaniu autentykacji wieloskładnikowej (MFA).

HID

[1]https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5cdc68866b61

[2]https://cybersecurity-magazine.com/10-small-business-cyber-security-statistics-that-you-should-know-and-how-to-improve-them/

[3]https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of

Zrozumienie uwierzytelniania wieloskładnikowego Multi-Factor Authentication (MFA):

Zamiast korzystać z jednego czynnika uwierzytelniania, rozwiązania uwierzytelniania wieloskładnikowego weryfikują tożsamość za pomocą kombinacji co najmniej dwóch różnych metod, w tym:

COŚ, CO MASZ
- Karta inteligentna
- Klucz bezpieczeństwa
- Karta kontroli dostępu
- Token OTP
- Telefon komórkowy

COŚ, CO WIESZ
- PIN
- Hasło
- Pytania bezpieczeństwa

COŚ, CZYM JESTEŚ
- Odcis palca
- Rozpoznawanie twarzy
- Rozpoznawanie głosu

Firmy mogą wymagać dowolnej kombinacji metod uwierzytelniania w dowolnej kolejności.

Karta + Hasło + Odcisk palca

Telefon komórkowy+ PIN + Pytanie bezpieczeństwa

Klucz FIDO + PIN

Te warstwy uwierzytelniania współpracują ze sobą, aby zmniejszyć poziom ryzyka. Nawet jeśli jeden czynnik uwierzytelniania zostanie naruszony, użytkownik musi podać inny, zanim uzyska dostęp — chronione dane i zasoby pozostają bezpiecznie zabezpieczone.

Faster With FIDO

Fast IDentity Online (FIDO) zastępuje logowanie wyłącznie za pomocą hasła bezpiecznym i prostym uwierzytelnianiem w witrynach i aplikacjach. Wykorzystuje ona wolne i otwarte standardy, aby zwiększyć bezpieczeństwo i wygodę zarówno dla konsumentów, jak i organizacji. Więcej informacji można znaleźć na stronie: fidoalliance.org/how-fido-works

MFA: zabezpieczanie tego, co jest dla Ciebie ważne

MFA może być i powinno być wykorzystywane wszędzie tam, gdzie dostęp do wrażliwych zasobów musi być chroniony przed cyberatakami i błędami ludzkimi. Małe i średnie firmy używają usługi MFA do zabezpieczania takich rzeczy, jak np:

- **Bazy danych i aplikacje —** bezpieczny dostęp do baz danych, oprogramowania księgowego i kadrowego, aplikacji chmurowych, internetowych i lokalnych za pomocą kart inteligentnych, kluczy bezpieczeństwa, tokenów OTP lub uwierzytelnień mobilnych
- **Komputery i urządzenia pracowników —** chroń urządzenia w domu i zdalnych biurach, dodając do tradycyjnego hasła drugą warstwę uwierzytelniania za pomocą klucza bezpieczeństwa lub karty inteligentnej
- **Urządzenia dla wielu użytkowników —** umożliwiają pracownikom szybkie i bezpieczne logowanie się do współdzielonych komputerów i urządzeń w środowiskach takich jak handel detaliczny, produkcja, służba zdrowia i inne.
- **Sieci i serwery —** Bezpieczne sieci VPN i serwery ułatwiają pracownikom dostęp do zasobów potrzebnych do pracy z dowolnego miejsca — nawet podczas korzystania z sieci publicznej

MFA to złoty standard, ale wdrożenie jest opóźnione

Można sobie wyobrazić, że przy wysokim ryzyku i prostych rozwiązaniach większość małych i średnich firm skorzystałaby z usługi MFA. W rzeczywistości niedawne badanie przeprowadzone przez Cyber Readiness Institute (CRI)4 wykazało, że tylko 46% wdrożyło politykę, ponieważ:

1. NIE SĄ ŚWIADOMI, ŻE ISTNIEJE

55% małych i średnich firm pozostaje bez ochrony, ponieważ po prostu nie są świadome istnienia usługi MFA i jej korzyści.

2. ONI TEGO NIE ROZUMIEJĄ

30% właścicieli firm stwierdziło, że nie korzysta z usługi MFA, ponieważ nie wie, jak to działa. W rzeczywistości istnieje wiele różnych typów usługi MFA, od prostych, łatwych do wdrożenia opcji plug-and-play po bardziej złożone wbudowane moduły. Ponadto firmy mogą wybierać spośród różnych form (takich jak karty, klucze i aplikacje mobilne) oraz metod (takich jak FIDO, PKI, OTP, powiadomienia push lub dane biometryczne).

3. UWAŻAJĄ, ŻE TO NIEWYGODNE

20% MSP uważa, że MFA jest zbyt niewygodne. W rzeczywistości wszyscy jesteśmy z tym bardziej zaznajomieni, niż nam się wydaje. W końcu każdy, kto kiedykolwiek używał PIN-u i karty w bankomacie, korzystał z MFA. Cały proces zajmuje kilka sekund i może zapobiec kosztownym cyberatakom, które mogłyby zrujnować reputację firmy, a nawet spowodować jej całkowite zamknięcie.

[4]https://cyberreadinessinstitute.org/resource/global-small-business-multi-factor-authentication-mfa-study/

MFA jako rozwiązanie dla małych i średnich firm: korzyści

MFA może służyć jako kamień węgielny silnego programu bezpieczeństwa cybernetycznego dla firm każdej wielkości, ale szczególnie dla małych i średnich firm o wyjątkowych wyzwaniach i warunkach. Wdrożenie go pozwala organizacjom zwiększyć bezpieczeństwo i wygodę na różne sposoby.

ZABEZPIECZAJ BEZ HASŁA

Przeciętny człowiek musi znać ponad 100 haseł[5] w swoim życiu osobistym i zawodowym. Aby ułatwić sobie życie, wielu użytkowników ucieka się do używania łatwych do zapamiętania haseł lub używa tego samego hasła w wielu miejscach — od logowania do sieci służbowej po osobiste konta bankowe. Niestety, ułatwia to również życie tym, którzy próbują ukraść informacje. Zapominanie haseł oznacza również resetowanie haseł, a resetowanie haseł kosztuje czas i zasoby.

Dzięki MFA możesz wyeliminować poleganie na hasłach i zapewnić bezpieczeństwo danych — jednocześnie poprawiając komfort użytkowania.

ZACHĘCAJ DO BEZPIECZNIEJSZEJ PRACY ZDALNEJ

Nowoczesny pracownik pracuje z dowolnego miejsca i w dowolnym czasie. Obecnie bardziej niż kiedykolwiek pracownicy często korzystają z urządzeń osobistych i służbowych, aby uzyskać dostęp do sieci i aplikacji, czasami za pośrednictwem mniej bezpiecznych połączeń internetowych. Ponieważ nawet najbardziej doświadczony zespół ds. cyberbezpieczeństwa nie zawsze jest w stanie kontrolować, gdzie ludzie się logują, kolejną najlepszą rzeczą jest skonfigurowanie środków bezpieczeństwa, które zwiększą bezpieczeństwo bez względu na to, gdzie znajdują się pracownicy.

ELIMINUJ ZAGROŻENIE

Uwierzytelnianie wieloskładnikowe utrudnia potencjalnym cyberprzestępcom kradzież danych firmowych poprzez uzyskanie dostępu do krytycznego oprogramowania i sprzętu, w tym urządzeń sieciowych. Według firmy Microsoft[6], MFA uszczelnia wszystkie słabe punkty wejścia do niezabezpieczonego systemu i może zapobiec 99,9% ataków na konto.

[5]https://tech.co/password-managers/how-many-passwords-average-person

[6]https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Znalezienie idealnie dopasowanego rozwiązania i dostawcy

Decyzja o wdrożeniu MFA jest łatwa; wybór odpowiedniego rozwiązania i dostawcy może wydawać się zniechęcający. MFA nie jest uniwersalnym rozwiązaniem i istnieje wiele zmiennych w procesie selekcji. Pamiętaj, aby współpracować z dostawcą oferującym wszystko, czego potrzebujesz, w tym:

- **Łatwość użytkowania —** Twoje rozwiązanie MFA powinno nie tylko oferować wybór metod uwierzytelniania, w tym opcje bezhasłowe i odporne na phishing oparte na FIDO lub PKI, ale powinno być również łatwe do przyjęcia i użytkowania. W końcu ten środek ochronny istnieje dla Twojej pewności i wygody użytkownika — a nie po to, by komplikować życie.
- **Wiele metod i formatów —** nie ograniczaj się do małego wyboru metod uwierzytelniania (takich jak OTP i powiadomienia push) ani formatów (takich jak karty lub telefony komórkowe). Wybierz dostawcę oferującego różnorodne opcje i możliwość korzystania z różnych opcji dla różnych użytkowników i potrzeb w zakresie bezpieczeństwa.
- **Łatwe wdrażanie i zarządzanie —** wdrożenie niektórych rozwiązań zajmuje miesiące; Twoje bezpieczeństwo nie może czekać tak długo. Inne rozwiązania wymagają intensywnego szkolenia, instalacji nowego serwera lub zmiany kodu w istniejących aplikacjach. Wybierz rozwiązanie, które można uruchomić w ciągu kilku dni, a nie miesięcy.
- **Kompletne rozwiązanie —** upewnij się, że nowa konfiguracja zabezpieczeń obejmuje wszystkie zasoby, od komputerów po telefony i wszystkie zintegrowane aplikacje i sieci.
- **Zgodność —** szczególnie w branżach podlegających regulacjom zgodność ma kluczowe znaczenie. Wybierz odpowiednie rozwiązanie i dostawcę spełniające stale zmieniające się przepisy branżowe, w tym ochrony danych, takich jak RODO.
- **Możliwość adaptacji —** Twoje potrzeby w zakresie bezpieczeństwa prawdopodobnie będą się zmieniać w czasie, a niektórzy użytkownicy lub części Twojej firmy mogą wymagać wyższych zabezpieczeń niż inne. Upewnij się, że Twój dostawca umożliwia odpowiednie dostosowanie.

Zaawansowane uwierzytelnianie: ważne kryteria, które należy wziąć pod uwagę przy wyborze dostawcy

Aby uzyskać szczegółowe informacje na temat wyboru odpowiedniego dostawcy, zapoznaj się z białą księgą firmy HID, Advanced Authentication Buyers Guide.

Zrównoważ bezpieczeństwo i wygodę z silnym uwierzytelnianiem MFA firmy HID, dostarczonym przez Alarmnet

Jako światowy lider w zakresie obsługi zaufanych tożsamości, firma HID oferuje szerokie i solidne portfolio rozwiązań MFA, w tym karty inteligentne Crescendo® z obsługą FIDO i PKI oraz klucze bezpieczeństwa, a także oprogramowanie MFA, takie jak DigitalPersona®.

Wielokrotnie nagradzana DigitalPersona pomaga firmom z sektora opieki zdrowotnej handlu detalicznego, call center, instytucji rządowychi innych, aby zabezpieczyć logowanie do komputerów stacjonarnych, stron internetowych, sieci VPN, sieci oraz aplikacji w chmurze i lokalnych. To łatwe do wdrożenia i zarządzania rozwiązanie do uwierzytelniania wieloskładnikowego zapewnia zgodność ze zmieniającymi się standardami bezpieczeństwa, mandatami i przepisami oraz obsługuje najszerszy wachlarz metod uwierzytelniania i formatów, w tym dane biometryczne, urządzenia mobilne, identyfikatory dostępu, karty inteligentne i klucze bezpieczeństwa.

Oprócz zabezpieczania dostępu do poufnych danych, aplikacji i poczty e-mail, karty inteligentne HID Crescendo o wysokim stopniu bezpieczeństwa mogą również służyć jako identyfikatory pracowników w celu zabezpieczenia dostępu do budynków — pomagając właścicielom firm połączyć fizyczny i logiczny dostęp oraz chronić zarówno obiekty, jak i dane za pomocą jednego uwierzytelniania.

Gotowy na zwiększenie bezpieczeństwa? Skontaktuj się z nami, aby poprosić o wersję próbną już dziś i odkryj, jak MFA może działać dla Twojej firmy.

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +353 91 506 900
Asia Pacific: +852 3160 9800
Latin America: +52 55 9171-1108

For more global phone numbers click here

2022-11-15-iams-multi-factor-auth-smb-oob-eb
PLT-06814

Part of ASSA ABLOY