Teraz Polska!
MFA: „must-have” dla każdego

Ransomware - wielkie zagrożenie dla firm i organizacji w Polsce. Jak się zabezpieczyć?

11.06.2025

Przemysław Kucharzewski
Channel Sales Manager
Rublon Sp. z o.o.

Czym jest MFA

Uwierzytelnianie wieloskładnikowe (ang. multi-factor authentication, MFA) – używanie dodatkowych składników w procesie uwierzytelniania (weryfikacji tożsamości).

Np. uwierzytelnianie dwuskładnikowe (2FA) może polegać na podaniu hasła jednorazowego (ang. one-time password, OTP) przy logowaniu się do poczty elektronicznej.

MFA jest sposobem ochrony dostępu do zasobów cyfrowych, ponieważ utrudnia zalogowanie się do tych zasobów przez nieuprawnione osoby, które zdobyły identyfikator użytkownika i hasło uwierzytelniające. W przypadku stosowania uwierzytelniania wieloskładnikowego użytkownik oprócz podania identyfikatora oraz hasła musi (w kolejnych etapach) podać dodatkowy składnik.

Czym jest MFA

Do uwierzytelniania MFA mogą zostać wykorzystane metody, które można skategoryzować wg następujących kryteriów:

- „coś, co użytkownik wie”: dane, które zna tylko użytkownik np. hasło, kod PIN;
- „coś, czym użytkownik jest”: dane biometryczne, unikalne cechy fizyczne użytkownika np. odcisk palca, skan tęczówki oka, skan twarzy itp.
- "coś, co użytkownik posiada”: przedmiot lub urządzenie do uwierzytelniania np. token, aplikacja na smartfonie, klucz, karta bankomatowa itp.

Można dodać:

- „miejsce, w jakim użytkownik aktualnie się znajduje”: np. wykorzystanie (lokalizacja GPS, numer IP) do potwierdzenia typowych lokalizacji użytkownika.
- Okno czasowe logowania

Dlaczego MFA?

Przeciwdziałanie:

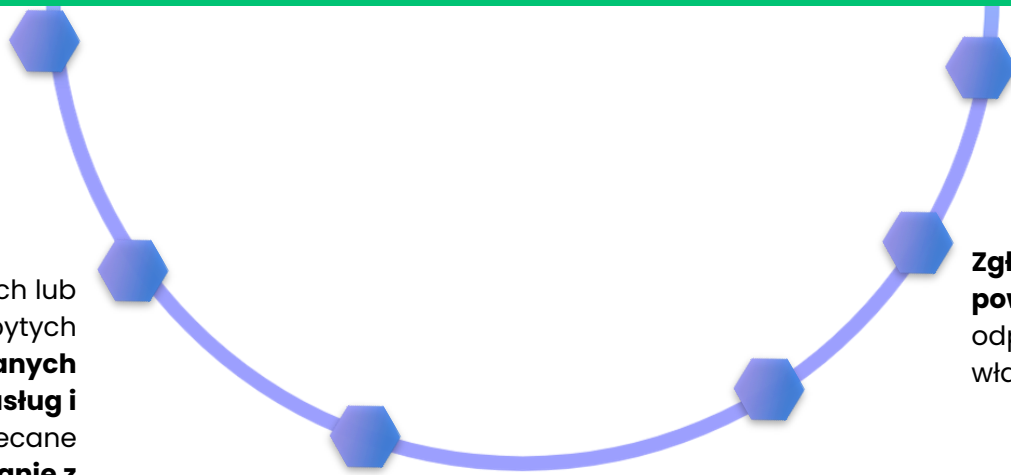
- Phishing
- Wyciek haseł
- Kradzież haseł
- Łamanie haseł
- Keylogger
- Błędy ludzkie

Raport Verizon's 2022 Data Breach Investigations Report ujawnił, że większość (82%) naruszeń danych była związana z czynnikiem ludzkim, na który składają się skradzione dane logowania, phishing, nadużycia i błędy.

Obowiązki podmiotów w NIS2

Obowiązkowe **szkolenia** dla kadry kierowniczej oraz zalecane dla pracowników

Stosowanie własnych lub nabytych **certyfikowanych produktów, usług i procesów ICT;** zalecane **korzystanie z kwalifikowanych usług zaufania;**



W stosownych wypadkach **powiadomienie odbiorców usług** o poważnych incydentach oraz środkach zaradczych;

Proporcjonalne **środki zarządzania ryzykiem w cyberbezpieczeństwie** uwzględniające:
-ryzyko,
-wielkość podmiotu,
-prawdopodobieństwo wystąpienia incydentów i ich dotkliwość;

Zgłaszanie incydentów poważnych do odpowiedniego CSIRT/ właściwego organu;

Zawiadamianie o **uczestnictwie w mechanizmach wymiany informacji**

Środki zarządzania ryzykiem

polityki analizy ryzyka i bezpieczeństwa systemów informatycznych

bezpieczeństwa łańcucha dostaw, w tym aspektów związanych z bezpieczeństwem stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

podstawowych praktyk cyberhigieny i szkoleń w zakresie cyberbezpieczeństwa;

obsługi incydentu;

bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowania w przypadku podatności i ich ujawnienia

polityk i procedur stosowania kryptografii i, w stosownych przypadkach, szyfrowania;

w stosownych przypadkach - stosowanie uwierzytelnienia wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych

ciągłości działania np. zarządzania kopiami zapasowymi i przywracania normalnego działania po wystąpieniu sytuacji nadzwyczajnej i, zarządzania kryzysowego

polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

bezpieczeństwa zasobów ludzkich, polityki kontroli dostępu i zarządzania aktywami;

NIS2 a MFA

Art. 21

“1. Państwa członkowskie zapewniają, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.
(...)

2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:
(...)

j) w stosownych przypadkach **– stosowanie uwierzytelniania wieloskładnikowego lub ciągłego**, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.”

DORA a MFA

“Art. 9 (...)
2. Podmioty finansowe opracowują, pozyskują i wdrażają polityki, procedury, protokoły i narzędzia w zakresie bezpieczeństwa ICT, których celem jest zapewnienie odporności, ciągłości działania i dostępności systemów ICT, w szczególności tych, które wspierają krytyczne lub istotne funkcje, oraz utrzymanie wysokich standardów dostępności, autentyczności, integralności i poufności danych, zarówno gdy są przechowywane, jak i wykorzystywane lub przesyłane.

3. Aby osiągnąć cele, o których mowa w ust. 2, podmioty finansowe stosują rozwiązania i procesy ICT, które są odpowiednie, zgodnie z art. 4. Te rozwiązania i procesy ICT:
(...)

d) wdrażają polityki i protokoły dotyczące silnych mechanizmów uwierzytelniania, oparte na odpowiednich standardach i specjalnych systemach kontroli oraz środkach ochrony kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka związanego z ICT.”

Jaki system MFA wybrać?

Przyjazny użytkownikom i administratorom

Użytkownicy samodzielnie wykonują rejestrację urządzeń uwierzytelniających

Wiele metod uwierzytelniania: Mobile Push, Email Link, klucze sprzętowe WebAuthn/U2F itd..

Wszechstronny

zintegrowany z większością technologii stosowanych w przedsiębiorstwach (np. poprzez SAML, LDAP, RADIUS, Web SDK, API oraz dedykowane pluginy i konektory): systemy, VPN, aplikacje.

Nowatorski i elastyczny

rozwijany w metodologii Agile, co umożliwia szybkie wydawanie ulepszeń wynikających z zapotrzebowań rynku i nowych technologii.

Opłacalny

zapewniający atrakcyjne warunki licencyjne i handlowe, umożliwiające wybranie planu cenowego optymalnie dopasowanego do wielkości i budżetu

MFA dla Twoich technologii

VPN poprzez RADIUS/LDAP/SAML	cisco	CITRIX	paloalto NETWORKS	f5
Microsoft własne konektory	Windows	Microsoft Remote Desktop Services	Office 365	Outlook
Web własne konektory	Confluence	Jira	WordPress	Custom (SDK)
Cloud poprzez SAML	Office 365	G Suite	salesforce	pingdom
Linux własne konektory	>ssh	Red Hat Enterprise Linux	debian	ubuntu

Zobacz więcej na https://rublon.com/pl/dokumentacja/

Metody uwierzytelniania

Mobile Push

Powiadomienie wysyłane na urządzenie mobilne, z przyciskami do zatwierdzenia lub odrzucenia dostępu

Mobile Passcode

Jednorazowe hasło numeryczne, generowane w oparciu o standard TOTP (RFC 6238), zmieniające się co 30 sekund

FIDO Security Key

Niepodatny na phishing sprzętowy klucz bezpieczeństwa zgodny ze standardem FIDO2 (WebAuthn, U2F)

YubiKey OTP

Długie hasło jednorazowe (OTP) wpisywane przez klucz sprzętowy YubiKey po dotknięciu

Phone Call

Połączenie wykonane na numer telefonu stacjonarnego lub komórkowego użytkownika z prośbą o naciśnięcie klawisza

SMS Passcode

Jednorazowe hasło numeryczne wysyłane na numer telefonu użytkownika w postaci SMS

SMS Link

Jednorazowy link wysyłany na numer telefonu w postaci SMS, z przyciskiem do zatwierdzenia dostępu

Email Link

Jednorazowy link wysyłany na adres email użytkownika, z przyciskiem do zatwierdzenia dostępu

Komponenty rozwiązania

Rublon Prompt

Widok wyświetlany po wprowadzeniu poprawnych danych logowania. Użytkownicy mogą wybrać preferowaną metodę uwierzytelniania i samodzielnie rejestrować nowe uwierzytelniacze.

Rublon Authenticator

Aplikacja mobilna dostępna dla systemów Android i iOS. Można ją pobrać ze sklepów Google Play, App Store lub AppGallery.

Rublon Admin Console

Centrum kontroli do zarządzania bezpieczeństwem organizacji. Administratorzy mogą konfigurować i zarządzać aplikacjami, użytkownikami, grupami użytkowników, urządzeniami i politykami bezpieczeństwa.

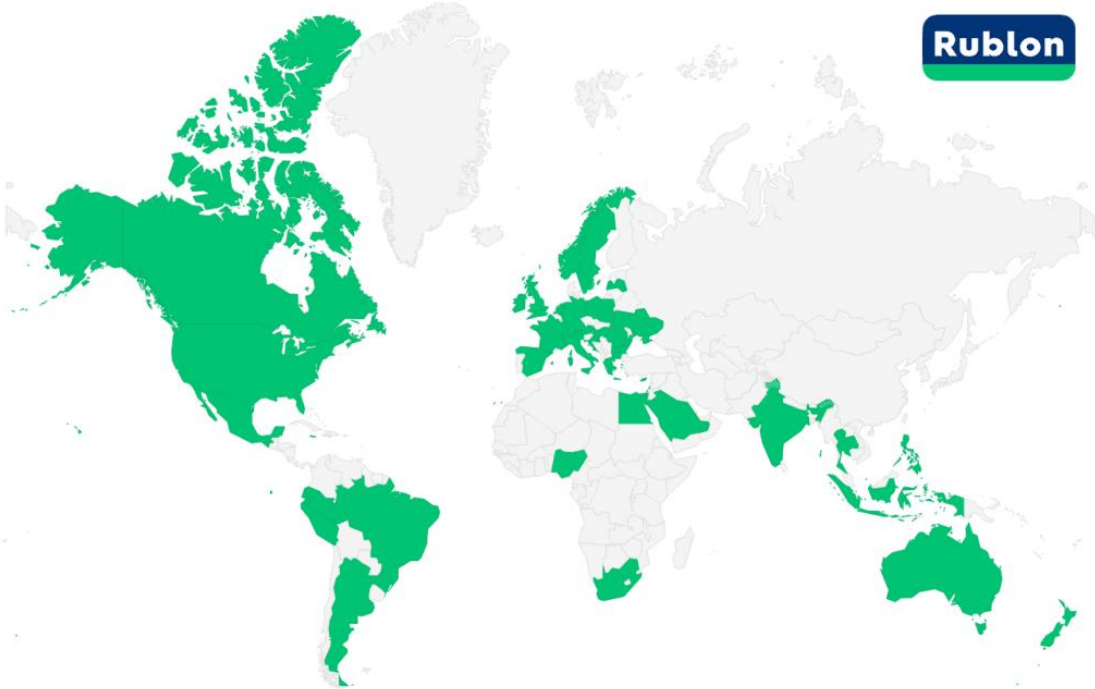
Czym jest Rublon

Real User Business Logon (w skrócie Rublon) należy do Grupy Astec. Astec to grupa firm technologicznych, które specjalizują się w

- tworzeniu oprogramowania na zamówienie,
- integracji i dostosowywaniu oprogramowania dla przedsiębiorstw,
- projektowaniu doświadczeń użytkowników,
- marketingu online,
- cyberbezpieczeństwie.

Klientami Astec są m.in. BMW, GE i Huawei.

Wdrożenia



500+ wdrożeń w 50+ państwach

Plany na przyszłość

- Portal MSP
- Zarządzanie kluczami bezpieczeństwa
- Eksport dzienników audytu do rozwiązań SIEM
- Kontrola dostępu oparta o lokalizację
- Zaufane urządzenia
- Rozwój rozwiązań Single Sign-On (SSO)
- Konektor macOS
- Bezhasłowe uwierzytelnianie (Passwordless)
- Bezagentowe wdrożenie MFA
- Inteligentny silnik oceny ryzyka

Rublon

Zalety Rublon

- Jedno miejsce zarządzania dostępami,
- Wiele możliwości uwierzytelniania,
- Liczne integracje,
- Elastyczność,
- SDK dla aplikacji stworzonych w Java, .NET i PHP,
- AD Sync, Entra ID Sync
- Model licencjonowania,
- Konkurencyjna cena,

Zalety Rublon

- Zapewnia zgodność z NIS2, DORA, NIST SP 800-63, HIPAA, GDPR,
- Certyfikacja ISO27001,
- MFA dla sesji Windows Client (RDS, RRAS),
- Wsparcie kluczy bezpieczeństwa zgodnych ze standardem FIDO,
- Wsparcie wielu dostawców tożsamości: FreeRADIUS, Active Directory, OpenLDAP, FreeIPA,
- Integracje za pomocą różnych protokołów integracyjnych (RADIUS, SAML, LDAP),
- 30-dniowy trial dla dowolnej liczby użytkowników
- Proof-of-Concept
- Polskojęzyczne wsparcie techniczne
- Elastyczność

Kontakt

Przemysław Kucharzewski
Channel Sales Manager

p.kucharzewski@rublon.pl
+48 515 166 966