Zalecenia bezpieczeństwa i konfiguracji usług VPN

W związku ze wzmożonymi atakami na SSL VPN oraz inne formy zdalnego dostępu, zalecamy wdrożenie kompleksowych środków ochrony. Obserwujemy wykorzystywanie zaawansowanych metod pozyskiwania danych uwierzytelniających, a także rozproszonych adresów IP, które utrudniają skuteczną obronę opartą jedynie na filtrowaniu geolokalizacji czy ograniczaniu częstotliwości prób logowania.

I. Podstawowe założenia

1.1. Aktualność oprogramowania

1. Utrzymywanie serwerów i klientów VPN w najnowszych, stabilnych wersjach.
2. Regularne instalowanie poprawek bezpieczeństwa zarówno na poziomie systemu operacyjnego, jak i dedykowanych urządzeń czy aplikacji VPN.

1.2. Silne mechanizmy kryptograficzne

1. Wyłączenie starszych protokołów (SSLv2, SSLv3, TLS 1.0, TLS 1.1) po włączeniu nowszej wersji.
2. Korzystanie co najmniej z TLS 1.2, a docelowo TLS 1.3.
3. Stosowanie zestawów szyfrów zalecanych przez organizacje takie jak NIST i CIS (np. AES-256, ChaCha20) oraz funkcje skrótu z rodziny SHA-2 lub SHA-3.

1.3. Wieloskładnikowe uwierzytelnianie (MFA)

1. Wdrożenie MFA jest rekomendowane jako standardowy mechanizm logowania dla wszystkich kont.
2. Stosowanie uznanych i sprawdzonych rozwiązań w zakresie wieloskładnikowego uwierzytelniania (MFA), w tym m.in. TOTP, kluczy U2F/FIDO2 czy certyfikatów zabezpieczonych hasłem lub PIN-em.
3. Okresowe testowanie skuteczności zastosowanego MFA oraz weryfikacja jego konfiguracji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

II. Zarządzanie kontami i uwierzytelnianiem

2.1. Ścisła kontrola dostępu do kont

1. Obowiązywanie polityka minimalnych uprawnień (least privilege) we wszystkich obszarach działalności.
2. Regularne suwanie lub blokowanie nieużywanych kont (np. byłych pracowników, konta testowe).
3. Stosowanie ściśle określonych reguł wobec haseł, obejmujących m.in. odpowiednią długość, różnorodność znaków oraz wykluczenie haseł powszechnych.

2.2. Ograniczenia dostępu oparte na ryzyku

1. Konfiguracja dostępu powinna opierać się o kontekst (używane urządzenie, adres IP, lokalizacja), jeśli pozwalają na to warunki techniczne i polityka bezpieczeństwa.
2. Wdrożenie systemów analizujących wzorce logowania w celu szybkiego wykrywania podejrzanych prób (np. częste logowania z odległych geolokalizacji w krótkim czasie).
3. Konfigurowanie powiadomień w przypadku przekroczenia ustalonych progów błędnych logowań czy innych nietypowych zachowań.

III. Bezpieczeństwo infrastruktury VPN

3.1. Hardening

1. Wymagane jest ograniczenie uruchomionych usług na serwerze VPN wyłącznie do niezbędnych elementów.
2. Wdrożenie list kontroli dostępu (ACL) lub firewalli, tak aby przepuszczać ruch wyłącznie na koniecznych portach i protokołach.
3. Umieszczenie serwera VPN w strefie DMZ, co ogranicza ryzyko przeniknięcia niepowołanego ruchu do kluczowych segmentów sieci.

3.2. Bezpieczna obsługa certyfikatów

1. Generowanie i przechowywanie kluczy prywatnych w zaufanych środowiskach, np. w infrastrukturze HSM (Hardware Security Module).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2. Odnawianie certyfikatów z odpowiednim wyprzedzeniem.
3. Wymagana jest dostępność mechanizmów unieważniania certyfikatów (CRL/OCSP).

3.3. Segmentacja i ograniczanie dostępu do zasobów

1. Skonfigurowanie reguł routingu w taki sposób, aby konta VPN miały dostęp jedynie do niezbędnych zasobów, aplikacji czy serwerów.
2. Wdrożenie w środowiskach rozbudowanych wielu odrębnych instancji VPN dla różnych jednostek organizacyjnych lub zastosowanie zasad Zero Trust.
3. Przeprowadzanie okresowych testów bezpieczeństwa pod kątem podatności w konfiguracji VPN.

3.4. Logowanie i analiza zdarzeń

1. Rejestrowanie przez serwer VPN wszystkich kluczowych operacji, takich jak logowania, błędne próby czy zmiany konfiguracji.
2. Przechowywanie logów tak długo, jak to konieczne, aby skutecznie umożliwić analizę ewentualnych incydentów w dłuższej perspektywie czasu.
3. Stworzenie klarownych procedur działania w przypadku wykrycia incydentów związanych z VPN.
4. Natychmiastowa blokada w przypadku podejrzenia kompromitacji konta lub urządzenia.

IV. Podstawowe założenia

4.1. Aktualność oprogramowania

3. Utrzymywanie serwerów i klientów VPN w najnowszych, stabilnych wersjach.
4. Regularne instalowanie poprawek bezpieczeństwa zarówno na poziomie systemu operacyjnego, jak i dedykowanych urządzeń czy aplikacji VPN.

4.2. Silne mechanizmy kryptograficzne

4. Wyłączenie starszych protokołów (SSLv2, SSLv3, TLS 1.0, TLS 1.1) po włączeniu nowszej wersji.
5. Korzystanie co najmniej z TLS 1.2, a docelowo TLS 1.3.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6. Stosowanie zestawów szyfrów zalecanych przez organizacje takie jak NIST i CIS (np. AES-256, ChaCha20) oraz funkcje skrótu z rodziny SHA-2 lub SHA-3.

4.3. Wieloskładnikowe uwierzytelnianie (MFA)

4. Wdrożenie MFA jest rekomendowane jako standardowy mechanizm logowania dla wszystkich kont.
5. Stosowanie uznanych i sprawdzonych rozwiązań w zakresie wieloskładnikowego uwierzytelniania (MFA), w tym m.in. TOTP, kluczy U2F/FIDO2 czy certyfikatów zabezpieczonych hasłem lub PIN-em.
6. Okresowe testowanie skuteczności zastosowanego MFA oraz weryfikacja jego konfiguracji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706