Zalecenia dotyczące konfiguracji zapory sieciowej - Firewall

CSIRT CeZ

Centrum e-Zdrowia

Sektor ochrony zdrowia jest coraz bardziej narażony na cyberataki.
Dlatego należy ze szczególną uwagą zadbać o zabezpieczenia infrastruktury IT. Prawidłowa konfiguracja zapory sieciowej jest kluczowa dla skutecznej ochrony systemów przed cyberzagrożeniami.

Firewall powinien być dostosowany do potrzeb organizacji. Jego zadaniem jest m.in.:

- segmentacja sieci,
- analiza i filtrowanie ruchu,
- ochrona przed nieuprawnionym dostępem.

1. Dlaczego to ważne

Podstawowe czynności i ustawienia mają ogromny wpływ na odporność i bezpieczeństwo systemów. Niestety, często zapominamy o elementarnych zasadach konfiguracji urządzeń lub lekceważymy je, co może prowadzić do poważnych konsekwencji.

2. Najważniejsze zalecenia konfiguracyjne dla zapory sieciowej

Poniżej przedstawiamy rekomendacje dotyczące konfiguracji i utrzymania zapory sieciowej:

- → **Aktualne oprogramowanie** – regularnie aktualizuj oprogramowanie firewalla. Dzięki temu wyeliminujesz znane podatności i zyskasz dostęp do najnowszych mechanizmów ochronnych.

- → **Aktualizacja reguł bezpieczeństwa** – monitoruj i optymalizuj konfigurację reguł. Pozwoli to wykryć błędy konfiguracyjne oraz ochronić system przed nowymi, ewoluującymi zagrożeniami.

- → **Silne hasła i MFA** – stosuj bezpieczną politykę haseł zgodną z rekomendowanymi standardami bezpieczeństwa. Dla kont administracyjnych wdróż uwierzytelnianie wieloskładnikowe (MFA).

- → **Zmiana domyślnych kont** – zmieniaj nazwy i hasła domyślnych kont administracyjnych, aby uniknąć ich wykorzystania przez atakujących.

- → **Indywidualne konta użytkowników** – nie dopuszczaj do korzystania ze współdzielonych kont. Każdy użytkownik powinien mieć własne konto.

- **Minimalizacja uprawnień (PoLP)** – nadawaj uprawnienia zgodnie z zasadą minimalnych uprawnień (Principle of Least Privilege – PoLP). Ogranicz dostęp tylko do niezbędnych zasobów.

- **Kontrola kont uprzywilejowanych** – zarezerwuj konta o podwyższonych uprawnieniach, typu „admin" i „superadmin", dla wąskiego grona osób, ze względu na szeroki zakres uprawnień takich kont.

- **Blokowanie zbędnych portów** – zamknij wszystkie nieużywane porty, aby ograniczyć potencjalne wektory ataku.

- **Deszyfracja ruchu i DPI** – w zależności od możliwości sprzętowych wdróż inspekcję SSL/TLS. Dzięki temu mechanizmy DPI (Deep Packet Inspection) i IPS (Intrusion Prevention System) będą skuteczniejsze, ponieważ decyzje o przepuszczeniu lub zablokowaniu pakietów będą podejmowane w czasie rzeczywistym.

- **Dezaktywacja zbędnych usług i protokołów** – wyłącz nieużywane usługi lub ogranicz ich dostęp do zaufanych adresów IP. Dotyczy to m.in. protokołów SNMP (Simple Network Management Protocol), Telnet czy HTTP. Dopuszczaj wyłącznie bezpieczne wersje protokołów, np: TLS min. 1.2, SNMPv3, SSHv2.

- **Bezpieczna konfiguracja VPN** – stosuj protokół IPsec VPN (który zalecamy) zamiast SSL VPN, ponieważ oferuje bardziej zaawansowane mechanizmy szyfrowania i integralności danych. W SSL VPN wykryto wiele nowych podatności.
  Rekomendujemy również model HUB & SPOKE, który zapewnia centralizację zarządzania i bezpieczne zestawianie tuneli pomiędzy oddziałami.

→ **Szyfrowana komunikacja** – jeśli to możliwe, korzystaj z szyfrowanych wersji protokołów, np.

- HTTPS zamiast HTTP,
- FTPS zamiast FTP,
- SSH zamiast Telnet.

Niezaszyfrowana komunikacja zwiększa ryzyko przechwycenia danych przez atakujących.

→ **Monitorowanie anomalii** – wykorzystuj funkcje zapory sieciowej do analizy i detekcji nietypowych aktywności. Pozwala to szybciej reagować na podejrzane działania i minimalizować skutki incydentów.

→ **Logi i ich analiza** – skonfiguruj przesyłanie logów do centralnego systemu SIEM lub kolektora logów, aby umożliwić ich analizę i szybkie reagowanie na incydenty. Zapewnij prawidłową synchronizację czasu (np. z serwerem NTP), aby logi z różnych systemów były spójne i umożliwiały korelację zdarzeń. Regularnie analizuj logi i reaguj na wykryte anomalie.

→ **Bezpieczny dostęp administracyjny** – ogranicz dostęp do panelu do zarządzania firewallem tylko z wewnętrznej sieci administracyjnej. Odseparuj go na wydzielonym VLAN-ie. Włącz restrykcje dla SSH (tylko określone segmenty sieci i zaufane adresy IP).

→ **Segmentacja sieci** – podziel sieć na strefy bezpieczeństwa o różnym poziomie zaufania. Możesz wyodrębnić takie strefy jak:

- **DMZ** – firewall oddziela usługi dostępne w DMZ od internetu,
- **sieć wewnętrzną** – firewall separuje internet i strefę DMZ od sieci wewnętrznej oraz filtruje ruch między segmentami wewnętrznymi (np. serwery aplikacyjne, bazodanowe, stacje robocze, sieć administracyjna),
- **sieć IoT** – specjalna strefa dla urządzeń IoT z ograniczonym dostępem do kluczowych systemów IT (np. kamery monitoringu, inteligentne systemy HVAC),
- **sieć dla gości** – wyodrębniona sieć VLAN dla gości z dostępem wyłącznie do internetu (z blokowaniem niebezpiecznych stron i usług, np. TOR) bez możliwości komunikacji z zasobami firmy,

- **strefy poszczególnych działów** – oddzielne VLAN-y dla różnych działów w organizacji, co ułatwia kontrolę przepływu danych i zmniejsza ryzyko ataku.

→ **Zasada najmniejszego dostępu** – kontroluj ruch pomiędzy segmentami sieci i ogranicz go wyłącznie do niezbędnych usług. Każda strefa musi mieć jasno określone polityki dostępu.

→ **Monitorowanie ruchu pomiędzy strefami** – włącz firewalle warstwy aplikacyjnej oraz systemy IDS/IPS, aby wykrywać i zapobiegać atakom przechodzącym pomiędzy segmentami sieci. Skonfiguruj SMTP do przesyłania alertów krytycznych na adres administratora NGFW.

→ **Listy dostępowe ACL** – utwórz precyzyjne reguły dostępu między segmentami sieci i unikaj reguł typu „allow any any". Dodaj na końcu każdej listy regułę „deny all".

→ **Bazy reputacyjne** – jeżeli producent udostępnia bazy reputacyjne usług internetowych, takie jak „Malicious-Malicious.Server" lub podobne, włącz korzystanie z nich i ustaw ich automatyczną aktualizację. Pozwoli to blokować znane złośliwe serwery i usługi.

→ **Ochrona usług publicznych** – jeżeli firewall obsługuje taką funkcjonalność, skonfiguruj Web Application Firewall (WAF), aby chronić aplikacje webowe przed atakami typu SQL Injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery) i innymi zagrożeniami. Dostosuj reguły WAF do specyfiki aplikacji, aby zminimalizować ryzyko fałszywych alarmów i zapewnić skuteczną ochronę. Jest to istotne, ponieważ WAF analizuje ruch HTTP/HTTPS i filtruje potencjalnie złośliwe żądania. To dodatkowa warstwa ochrony dla usług udostępnianych w internecie. Regularnie aktualizuj polityki WAF.

→ **Proxy PASS** – przekieruj wszystkie usługi wystawione do internetu przez proxy urządzenia, aby zastosować certyfikat SSL i egzekwować polityki WAF dla dodatkowej warstwy ochrony.

→ **Dodatkowe profile bezpieczeństwa** – jeżeli firewall wspiera poniższe funkcjonalności, skonfiguruj je:

- **profil antywirusowy** – skanowanie ruchu pod kątem złośliwego oprogramowania,
- **profil web filteringu** – kontrola dostępu do stron internetowych na podstawie kategorii i reputacji domen,
- **profil monitorowania/blokowania aplikacji** – analiza i kontrola ruchu aplikacyjnego, aby ograniczyć dostęp do niepożądanych usług,

- **profil monitorujący zapytania DNS** – identyfikacja i blokowanie podejrzanych zapytań DNS, co pomaga w ochronie przed atakami typu DNS tunneling.

→ **Redundancja i kopie zapasowe** – zapewnij ciągłość działania i możliwość szybkiego przywrócenia funkcjonalności po awarii:

- **stosuj redundancję** – użyj co najmniej dwóch urządzeń w trybie wysokiej dostępności (HA), np. aktywny–pasywny lub aktywny–aktywny. Takie rozwiązanie pozwala na ciągłość działania nawet w przypadku awarii jednego z urządzeń. W większych środowiskach rozważ konfigurację klastra z większą liczbą urządzeń,

- **twórz kopie zapasowe** – regularnie wykonuj zaszyfrowane kopie konfiguracji firewalla i przechowuj je w bezpiecznym miejscu. Regularnie testuj proces przywracania konfiguracji, aby upewnić się, że działa poprawnie.

→ **Zarządzanie i monitoring** – monitoruj zaporę sieciową w sposób ciągły, aby zapewnić najwyższy poziom bezpieczeństwa i ciągłość działania. Wykonuj regularne skany podatności, analizuj dzienniki zdarzeń, konfiguruj alerty i reaguj na nie. Okresowo przeglądaj reguły i prowadź aktualną dokumentację procesów i konfiguracji.

→ **Izolacja globalizacyjna** – jeśli nie ma uzasadnionej potrzeby, aby udostępniać usługę do internetu, ogranicz dostęp do usług wyłącznie do regionu Polska lub Unia Europejska.

→ **Logi z urządzenia** – przechowuj logi na lokalnym serwerze syslog lub w chmurze przez minimum 30 dni.

Wymienione zalecenia dotyczące **konfiguracji zapory sieciowej** mają na celu zwiększenie bezpieczeństwa poprzez skuteczną kontrolę ruchu, ochronę przed nieautoryzowanym dostępem i minimalizowanie ryzyka ataków.

Ich wdrożenie pozwoli dostosować działanie zapory do specyficznych potrzeb organizacji, co przełoży się na większą stabilność i odporność infrastruktury na zagrożenia.