Lasy Państwowe

Ochrona węzłów centralnych

Łukasz Adamczyk
Zakład Informatyki Lasów Państwowych
Operator Centrum Przetwarzania Danych (ZU)

Rogów, 09.10.2026 r.

Agenda

- Triada CIA jako fundament bezpieczeństwa (wstęp).
- Filary bezpieczeństwa ochrona bezpośrednia i pośrednia węzłów centralnych.
- Mechanizmy ochrony węzłów centralnych.
- Podsumowanie.

Wstęp

fundament bezpieczeństwa

Cyber operacje to działania w cyberprzestrzeni lub poprzez nią.

Działania te mają wywołać określony efekt.

Ów efekt definiowany jest przez prowodyra (sponsora, stronę wykonującą działania).
Efekty mogą obejmować pozyskanie informacji, paraliż lub modyfikację systemów.

Są to więc działania wymierzone w kwestie ujęte w triadzie CIA (C-I-A).

Wstęp

fundament bezpieczeństwa

Poufność (ang. **Confidentiality**), Integralność (ang. **Integrity**), Dostępność (ang. **Availability**) to podstawowe elementy bezpieczeństwa systemów, sieci i komputerów.

W zabezpieczaniu systemów chodzi o to, by uniknąć ryzyka ujawnienia informacji (naruszenie poufności), ryzyka utraty danych bądź ich modyfikacji (naruszenie integralności) lub ryzyka utraty dostępu do systemów bądź danych (naruszenie dostępności).

Wobec tego **cyber operacje defensywne mają na celu utrzymanie wysokich parametrów C-I-A, a ofensywne ich naruszenie.**

Wstęp

fundament bezpieczeństwa

Dlaczego **węzeł centralny** jest tak ważny i należy go chronić ?

Węzeł centralny to miejsce koncentracji kluczowych usług i przepływu danych w PGL LP

- dostęp użytkowników za pomocą bram VPN oraz Portalu Leśniczego,
- dostęp do Internetu oraz usług działających w chmurze,
- systemy administracyjne i zarządzania,
- punkt przejścia ruchu między różnymi strefami bezpieczeństwa sieci,
- usługi uwierzytelniania,
- aplikacje biznesowe i bazy danych m.in.: nowy Portal Leśno-Drzewny, SILP, Leśnik+ oraz inne,
- portale i witryny korporacyjne

Wstęp

fundament bezpieczeństwa

Atak na infrastrukturę centralną **Lasów Państwowych** może mieć większy zasięg niż atak na pojedynczy oddział.

Awaria lub kompromitacja może oddziaływać na dużą część organizacji.

Im większa koncentracja usług i ruchu w jednym miejscu, tym większe znaczenie mają **odporność, segmentacja, kontrola przepływu ruchu**.

Podstawą bezpieczeństwa jest **ochrona która musi realizować trzy cele** i naszym zadaniem jest dopilnowanie i rozwój zabezpieczeń węzła centralnego tak aby odpowiedzieć sobie na pytania:

- *Czy dane są chronione przed nieuprawnionym dostępem ?*
- *Czy dane i komunikacja nie zostały zmodyfikowane ?*
- *Czy usługi pozostają dostępne pomimo awarii lub ataku ?*

Lasy Państwowe

Filary bezpieczeństwa

Bezpośrednia i pośrednia ochrona węzłów centralnych

Usługa Protect DDoS
(Operator Netia)

- Akwizycja danych z systemów bezpieczeństwa, system umożliwia korelację, analiza logów oraz zdarzeń;

SIEM
(Security Information and Event Management)

- Farma loadballacer'ów sprzętowych, która odpowiada za dostarczenie i optymalizację ruchu do aplikacji zapewniając wysoką dostępność oraz kontrolę ruchu do usług m.in.: PLD, SILP, Poczta, EMM oraz innych usług krytycznych;

- Firewall-e oddziałowe zabezpieczające strefę sieci WAN między oddziałami oraz do COPD (L3);

ADC
(Application Delivery Controller)

COPD
(Centrum Operacyjne Przetwarzania Danych)

Centralne NGFW
(Firewall NextGeneration)

Oddziałowe NGFW (UTM)
(Firewall NextGeneration)

Endpoint AV
(Multi-Vendor)

- Infrastruktura zapewniająca wysoką dostępność usług centralnych na poziomie ośrodków danych CP i CZ;

- Farma centralnych firewall-i oraz bram dostępowych łącząca i chroniąca strefy wewnętrzne w obrębie sieci COPD, do i z sieci WAN (L3) przed zagrożeniami pochodzącymi m.in. z sieci Internet

- Portal dostępowy dla pracowników oraz firm zewnętrznych (ok ~ 5 tys. zalogowanych użytkowników dziennie);

- Bramy dostępu dla połączeń IPsec VPN Klient (ok ~ 3 tys zalogowanych użytkowników dziennie);

- Bramy dostępowe IPsec Site-to-Site łączące oddziały LP, inne instytucje;

EDR/XDR
(Endpoint Detection System)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Usługa DDoS Protect
(Operator Netia)

Chroni przed atakami wolumetrycznymi typu **Denial of Service**.
Usługa Netii zawiera zestaw mechanizmów chroniących infrastrukturę przed atakami polegającymi na masowym zalewaniu ruchem z wielu rozproszonych źródeł na publicznie dostępne usługi należące do organizacji PGL LP.

Głównym celem ataku **typu DoS** jest **wyczerpanie dostępnych zasobów**, tak aby użytkownicy korzystający z systemu utracili dostęp do usługi. Usługa DDoS Protect i odparcie ataku realizowane jest jeszcze na infrastrukturze Operatora.

Statystycznie do ataków typu DoS na infrastrukturę Lasów Państwowych dochodzi **średnio kilka razy w miesiącu**.

Jeden z większych ataków typu DoS na infrastrukturę Lasów Państwowych miał miejsce w **roku 2022r.**

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu

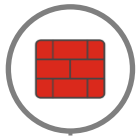
Poza usługą DDoS Protect świadczoną przez operatora usług Netia, posiadamy **dodatkowe mechanizmy umożliwiające** uruchomienie środków **mitygacyjnych ruch** w celu jeszcze większego zmniejszenia **wolumenu ataku typu DoS**

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych



Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- **Inspekcja SSL**

Obecnie ogromna część komunikacji sieciowej to szyfrowany ruch HTTPS (SSL/TLS).
Z jednej strony jest to **bardzo dobre dla bezpieczeństwa**, iż ruch jest szyfrowany z drugiej stwarza problem.
Firewall widzi ruch, ale nie widzi zawartości komunikacji (payload).

Inspekcja SSL umożliwia **deszyfrację** ruchu, **badanie Payload'u** za pomocą mechanizmów detekcji a następnie ponowne **szyfrowanie** ruchu.

Dzięki temu mechanizmowi inspekcja SSL **umożliwia narzędziu jakim jest firewall** głębszą **analizę** faktycznej zawartości **komunikacji**.

Z perspektywy bezpieczeństwa organizacji pozwala to pośrednio na wykrywanie zagrożeń ukrytych w szyfrowanym ruchu tj. exploity, malware, komunikacja C&C, manipulacje aplikacją lub wykorzystanie podatności usług, serwerów.

Generalną zasadą, którą powinniśmy się kierować jest **deszyfracja ruchu, który nie jest nam znany.**

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- **IPS – Intrusion Prevention System**

IPS aktywnie **analizuje ruch sieciowy w celu wykrywania i blokowania prób wykorzystania znanych podatności**.
IPS również może aktywnie zapobiegać atakowi.

IPS analizuje m.in.:
charakterystykę ruchu,
sygnatury exploitów,
anomalię protokołów,
payload komunikacyjny,
próby wykorzystania CVE*

Aktualnie systemy bezpieczeństwa z których korzystamy posiadają codziennie aktualizowaną
bazę wiedzy o zagrożeniach modułu IPS, składającą się z:
~ 20 000 rekordów sygnatur CVE*

*CVE (Common Vulnerabilities and Exposures) to międzynarodowy standard i słownik unikatowych identyfikatorów służący do katalogowania publicznie znanych luk bezpieczeństwa w sprzęcie i oprogramowaniu

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- **Anti-Bot / Anti-Virus**

Anti-Virus odpowiada za **wykrywanie i blokowanie znanego złośliwego oprogramowania**, zanim trafi do określonego celu. **Działa na etapie pre-infekcji** głównym zadaniem jest zatrzymanie malware'u zanim dojdzie do infekcji hosta.

Anti-Bot działa z innej perspektywy, nie skupia się na samym pliku malware, ale na zachowaniu zainfekowanego hosta w sieci. **Działa na etapie pre-infekcji i post-infekcji**, którego głównym zadaniem jest **wykrycie połączeń** oraz blokowanie komunikacji z infrastrukturą Command & Control (C&C) na poziomie sieci.

Anti-Bot wykrywa zagrożenia na podstawie m.in.:
reputacji adresów IP, reputacji URL, reputacji i analizy DNS, znanych adresów C&C, wzorców komunikacji botnet'u oraz zachowań charakterystycznych dla zainfekowanych hostów.

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- **Anti-Bot / Anti-Virus**

Anti-Virus oraz **Anti-Bot** stanowią dwie uzupełniające się warstwy ochrony, AV koncentruje się na zapobieganiu infekcji. AB może zadziałać nawet po infekcji. Identyfikuje urządzenia, które zostały już zainfekowane i blokuje ich komunikację.

Aktualnie systemy bezpieczeństwa z których korzystamy posiadają codziennie aktualizowaną **bazę wiedzy o zagrożeniach**, składającą się z

~ 62 000 000 adresów IP,
~ 249 000 000 adresów URL,
~ 14 000 000 adresów URL malware,
~ 250 000 000 domen,
~ 30 500 000 wirusów,
+
własne listy artefaktów IoC (Indicator of Compromise) oraz listy dostarczane przez zaufane podmioty zewnętrzne (CSIRT GOV itp.)

COPD
(Centrum Operacyjne Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- Anti-Bot / Anti-Virus
- **Application Control**

Application Control to moduł, który **pozwala kontrolować ruch na poziomie aplikacji**, nie tylko adresów IP, portów i protokołów. Moduł **wykorzystuje mechanizmy głębokiej inspekcji do identyfikacji**, monitorowania oraz blokowania tysięcy aplikacji i usług internetowych.

Największą zaletą Application Control jest **możliwość budowania polityki na podstawie tego, co użytkownik faktycznie robi**, a nie tylko gdzie się łączy.

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- Anti-Bot / Anti-Virus
- Application Control
- **Threat Prevention**

Threat Prevention nie jest pojedynczym modułem. To kompleksowa wielowarstwowa architektura ochrony przed zagrożeniami, łącząca **wiele silników bezpieczeństwa działających na różnych etapach cyberataku**.

Komponenty Threat Prevention:
IPS - Czy ktoś próbuje wykorzystać podatność ?
Anti-Virus – Czy przesłany obiekt zawiera malware ?
Threat Emulation – Czy nieznany plik zachowuje się jak malware ?
Threat Extraction – Czy można bezpiecznie usunąć aktywną zawartość pliku ?
Anti-Bot – Czy zainfekowany host komunikuje się z C&C ?

Rozwiązanie zakłada, że nawet jeżeli jedna warstwa zostanie ominięta, kolejne mechanizmy nadal mogą wykryć i zatrzymać zagrożenie.

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- Anti-Bot / Anti-Virus
- Application Control
- Threat Prevention
- **Polityki bezpieczeństwa**

W węźle centralnym nie wykorzystujemy jedynie „polityki firewall”. W architekturze występuje kilka typów polityk bezpieczeństwa, które realizują różne zadania:

Access Control Policy – Czy komunikacja jest dozwolona ?
Threat Prevention Policy – Czy komunikacja zawiera zagrożenie ?
HTTPS Inspection Policy – Czy ruch szyfrowany powinien być analizowany ?
NAT Policy – Jak realizowana jest translacja adresów ?
QoS Policy
Desktop Security Policy
Mobile Access Policy

Polityki bezpieczeństwa stanowią centralny mechanizm egzekwowania zasad ochrony – od kontroli dostępu, przez szyfrowanie ruchu, aż po aktywne wykrywanie i blokowanie cyberzagrożeń. Realizowane i tworzone przez zespoły Operacyjne.

COPD
(Centrum Operacyjne
Przetwarzania Danych)

Lasy Państwowe

Architektura ochrony

Mechanizmy ochrony węzłów centralnych

Centralne NGFW
(Firewall NextGeneration)

Mechanizmy ochrony

- Mitygacja ruchu
- Inspekcja SSL
- IPS – Intrusion Prevention System
- Anti-Bot / Anti-Virus
- Application Control
- Threat Prevention
- Polityki bezpieczeństwa

Geo-klaster niezawodnościowy
oparty o hyperskalowalną platformę bezpieczeństwa

- Skalowanie poziome (wiele fizycznych FW w jeden logiczny) platforma pozwala dynamicznie zwiększyć wydajność zapór bez przebudowy przebudowy struktury sieci.
- Wysoka dostępność i dystrybucja obciążenia, działa w architekturze typu Active-Active (niezawodność na poziomie 99,9%) synchronizacja aktywnych połączeń między bramami w ramach Security Grupy.
- Możliwość budowy dużych klastrów Security Gateway w przypadku awarii dodanie nowego urządzenia do Grupy zajmuje parę minut.

COPD
(Centrum Operacyjne Przetwarzania Danych)

Podsumowanie

Aby zachowanie ochrony i parametrów **C-I-A** było możliwe na wysokim poziomie, przy coraz bardziej złożonych środowiskach IT wymagane jest wdrażanie coraz bardziej wyrafinowanych rozwiązań i procedur w zakresie bezpieczeństwa cybernetycznego, szczególnie w dzisiejszej erze szybkiego rozwoju AI.

Stwarza to **potrzebę uzyskania pełnego obrazu infrastruktury i możliwości reagowania na zagrożenia** o każdej porze dnia, niezależnie od tego gdzie się one znajduje.

Lasy Państwowe

Dziękuję za uwagę

Zakład Informatyki Lasów Państwowych
Sękocin Stary, ul. Leśników 21C
05-090 Raszyn
tel. +48 22 270-71-00, IP: 1828100
biuro@zilp.lasy.gov.pl