Załącznik nr 6
do Regulaminu
organizacyjnego w dziale
wewnętrznym

ZARZĄDZENIE nr 50

DYREKTORA GENERALNEGO LASÓW PAŃSTWOWYCH

z dnia 13 maja 2022 r.

w sprawie zmiany Zarządzenia nr 31

Dyrektora Generalnego Lasów Państwowych

z dnia 18 września 2017 r.

w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe

OI.0413.13.2017

(Znak: EI.413.4.2022)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach[1], w związku z § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe[2], w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, o których mowa w § 8 ust. 1 pkt 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe[3] oraz w art. 33 ust. 3 pkt 8 ustawy o lasach[4], zarządza się, co następuje:

§1

Zmienia się treść załącznika nr 1 do zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który otrzymuje brzmienie:

„Załącznik nr 1 do Zarządzenia nr 31
Dyrektora Generalnego Lasów Państwowych
z dnia 18 września 2017 r.

ZASADY FUNKCJONOWANIA ZINTEGROWANEGO SYSTEMU INFORMATYCZNEGO W LASACH PAŃSTWOWYCH

---

[1] Art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2022 r. poz. 672) stanowi, że Lasami Państwowymi kieruje Dyrektor Generalny przy pomocy dyrektorów regionalnych dyrekcji Lasów Państwowych.

[2] Statut Państwowego Gospodarstwa Leśnego Lasy Państwowe został nadany zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. § 6 Statutu stanowi, że w wykonaniu zadań określonych przez ustawę o lasach oraz przez przepisy wykonawcze do ustawy, a także inne przepisy prawa, Dyrektor Generalny wydaje zarządzenia i decyzje obowiązujące w Lasach Państwowych.

[3] § 8 ust. 1 pkt 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe stanowi, że Dyrektor Generalny ustala system informacyjny Lasów Państwowych.

[4] Art. 33 ust. 3 pkt 8 ustawy o lasach stanowi, że Dyrektor Generalny organizuje wspólne przedsięwzięcia jednostek organizacyjnych Lasów Państwowych.

§ 1.
Terminy użyte w tekście

1. **Lasy Państwowe, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **DGLP** – Dyrekcja Generalna Lasów Państwowych.
3. **rdLP** - regionalne dyrekcje Lasów Państwowych.
4. **SILP** – Zintegrowany System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu zasobów informatycznych LP.
5. **System LAS** – system i podstawowa aplikacja biznesowa LP.
6. **SZKZ** – System Zarządzania Kodami Źródłowymi SILP.
7. **SZBM** – narzędzie udostępnione poprzez przeglądarkę internetową pod nazwą „System Zgłaszania Błędów i Modyfikacji SILP".
8. **WAN LP** – sieć rozległa Lasów Państwowych, komputerowa sieć modelu TCP/IP odpowiedzialna za przesyłanie danych pomiędzy jednostkami LP.
9. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
10. **Dostęp zdalny VPN** – dostęp do **wewnętrznych zasobów SILP** z sieci Internet za pośrednictwem szyfrowanych połączeń IPSec lub SSL.
11. **WI DGLP** – Wydział Informatyki Dyrekcji Generalnej Lasów Państwowych.
12. **ZCI** - Zespół w WI DGLP do spraw Cyberbezpieczeństwa Informatycznego, odpowiedzialny za nadzór nad bezpieczeństwem SILP.
13. **SZBI** - System zarządzania bezpieczeństwem informacji, część SILP oraz systemu zarządzania odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji przez ZCI.
14. **ZILP** – Zakład Informatyki Lasów Państwowych.
15. **WI** – komórki organizacyjne rdLP właściwe do spraw informatyki oraz administracji SILP w jednostkach nadzorowanych.
16. **Administrator SILP** – pracownik WI lub wyznaczona przez kierownika jednostki osoba zarządzająca zasobami SILP w jednostce posiadająca stosowny certyfikat.
17. **Użytkownik SILP** - pracownik Lasów Państwowych, w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonująca prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.
18. **Instruktor regionalny SILP** – wyznaczony przez dyrektora rdLP pracownik biura RDLP lub jednostki nadzorowanej, który świadczy pomoc oraz prowadzi szkolenia w określonym zakresie funkcjonalnym SILP.

19. **Koordynator regionalny SZBM** - Instruktor regionalny SILP lub wyznaczony przez dyrektora rdLP pracownik biura RDLP, który koordynuje zgłoszenia w systemie SZBM wprowadzane przez pracowników jednostek własnej RDLP.
20. **Koordynator centralny SZBM** – wyznaczony przez Dyrektora Generalnego LP pracownik LP, który koordynuje zgłoszenia w systemie SZBM w przypisanym zakresie merytorycznym.

§ 2.
System Informatyczny Lasów Państwowych

1. System Informatyczny Lasów Państwowych, stanowi zbiór elementów wzajemnie współpracujących, których funkcją jest przetwarzanie danych w PGL LP przy użyciu:

   a) sprzętu,
   b) oprogramowania,
   c) elementów organizacyjnych,
   d) technik informacyjnych.

2. Podstawą prawidłowego funkcjonowania SILP, na każdym szczeblu organizacyjnym, jest:

   a) spójna polityka dotycząca wykorzystania jednolitej platformy sprzętowej, systemowej i programowej
   b) wspólne zasady gromadzenia, przetwarzania i wymiany informacji,
   c) kompleksowe współdziałanie pracowników, komórek i jednostek organizacyjnych LP.

3. Nadzór nad prawidłowym funkcjonowaniem SILP sprawują Kierownicy jednostek organizacyjnych, w szczególności w zakresie:

   a) przestrzegania zasad bezpieczeństwa,
   b) wdrażania zmian SILP,
   c) szkolenia pracowników.

§ 3.
Informatyka w Lasach Państwowych

1. W celu zabezpieczenia realizacji zadań utrzymania i rozwoju SILP:

a) Dyrektor Generalny Lasów Państwowych powołuje:
   i) WI w DGLP,
   ii) Zespół ds. Cyberbezpieczeństwa – wyodrębnioną strukturę w ramach Wydziału Informatyki DGLP
   iii) ZILP,
   iv) zespoły zadaniowe – wg potrzeb.

b) Dyrektorzy regionalnych dyrekcji Lasów Państwowych powołują:
   i) WI w rdLP,
   ii) Instruktorów regionalnych SILP i/lub koordynatorów SZBM,
   iii) zespoły zadaniowe – wg potrzeb.

c) Kierownicy pozostałych jednostek organizacyjnych ujmują w strukturze organizacyjnej kierowanej przez siebie jednostki stanowisko administratora/administratorów SILP.

2. Szczegółowe zakresy zadań wydziałów informatyki oraz administratorów SILP są określone w regulaminach organizacyjnych jednostek organizacyjnych.
3. Szczegółowe zadania ZILP precyzuje odrębne zarządzenie Dyrektora Generalnego LP.
4. Szczegółowe zakresy zadań Instruktorów regionalnych SILP określają odrębne uregulowania stanowione przez dyrektorów rdLP.
5. Instruktorzy regionalni SILP i koordynatorzy SZBM otrzymują dodatkowe wynagrodzenie.
6. Ramowe kryteria wynagradzania ustala Dyrektor Generalny LP.
7. Administratorzy SILP zobowiązani są posiadać stosowny certyfikat uprawniający do pełnienia funkcji administratora SILP. W uzasadnionych sytuacjach dopuszcza się czasowe pełnienie obowiązków administratora SILP bez przedmiotowego certyfikatu.

§ 4
Zadania komórek organizacyjnych rdLP i DGLP, w zakresie wdrażania i eksploatacji SILP

1. Kierowników komórek organizacyjnych rdLP i DGLP czyni się odpowiedzialnymi za znajomość zasad funkcjonowania i wykorzystania systemu informatycznego przez podległych pracowników, co najmniej w zakresie czynności określonych dla danego stanowiska w komórce.

2. Kierowników komórek organizacyjnych DGLP zobowiązuje się do współpracy z prowadzącymi szkolenia dla Instruktorów regionalnych SILP, w zakresie merytorycznej kompetencji danej komórki.
3. Kierowników komórek organizacyjnych rdLP zobowiązuje się do organizowania szkoleń użytkowników SILP w zakresie merytorycznej kompetencji danej komórki.
4. Kierownicy merytorycznych komórek organizacyjnych rdLP nadzorują proces wdrażania nowych funkcjonalności i zmian w SILP w jednostkach podległych w zakresie działania komórki organizacyjnej.

§ 5.
Zasady działania w zakresie użytkowania SILP

1. Pracownicy jednostek organizacyjnych Lasów Państwowych, w których zakresie działania znajdują się zagadnienia objęte SILP są zobowiązani do:
    a) opanowania umiejętności posługiwania się systemem w zakresie swego działania,
    b) prawidłowego i rzetelnego wprowadzania danych do systemu,
    c) zgłaszania wszelkich zauważonych błędów i nieprawidłowości w funkcjonowaniu SILP.

2. Bezpośredni przełożony użytkownika odpowiada za:
    a) stały nadzór nad prawidłowością posiadanych przez pracownika uprawnień w systemie, niezbędnych do prawidłowej realizacji zadań wynikających z zakresu czynności.
    b) sprawowanie nadzoru nad działaniami wymienionymi w ust. 1
    c) obsługę modułów funkcjonalnych SILP w zakresie merytorycznego działania komórki organizacyjne,
    d) dbanie o zachowanie bezpieczeństwa SILP i przetwarzanych danych.

§ 6.
Błędy i modyfikacje SILP

1. Błędy i propozycje modyfikacji SILP może zgłosić każda jednostka organizacyjna Lasów Państwowych lub użytkownik SILP.
2. Zgłoszenie błędów i propozycji modyfikacji odbywa się za pośrednictwem SZBM, lub w uzasadnionych przypadkach na pisemny wniosek skierowany drogą służbową.

§ 7.
Zgłoszenia błędów w SZBM

1. Zgłoszenia wprowadzone do SZBM podlegają weryfikacji przez koordynatorów regionalnych, stanowiących pierwszą linię wsparcia dla użytkowników.
2. Obsługą zgłoszeń o charakterze merytorycznym lub technicznym wykraczającym poza możliwości rozwiązania na poziomie koordynatorów regionalnych SZBM, zajmują się koordynatorzy centralni SZBM.
3. Koordynatorzy centralni SZBM dokonują oceny zgłoszeń pod względem merytorycznym, kwalifikując zgłoszenie do właściwego zakresu merytorycznego SILP i w przypadku uznania ich zasadności zatwierdzają do realizacji.
4. Koordynatorzy centralni SZBM przed zatwierdzeniem zgłoszenia mogą wymagać dodatkowych informacji od zgłaszającego lub przekazać zgłoszenie do konsultacji do DGLP.
5. Kompletne zgłoszenia błędów zatwierdzone przez koordynatorów centralnych SZBM są podstawą do przekazania tych zgłoszeń do podmiotu konserwującego dany zakres SILP, w celu podjęcia działań zmierzających do usunięcia błędu.
6. Tryb postępowania w zakresie sposobu i terminów realizacji zatwierdzonych zgłoszeń błędów wynika z odrębnych ustaleń z podmiotem konserwującym dany zakres SILP.

§ 8.
Modyfikacje w SILP

1. Koordynacją modyfikacji SILP zajmuje się WI w DGLP. Na podstawie zgłoszeń WI w DGLP opracowuje, w uzgodnieniu z wydziałami merytorycznymi, zlecenia do ZILP wraz z określeniem terminów realizacji.
2. Dyrektor ZILP po otrzymaniu zlecenia Dyrektora Generalnego LP dokonuje modyfikacji SILP lub wykonuje nowe oprogramowanie. Dopuszcza się zlecenie wykonania modyfikacji oprogramowania lub wykonanie nowych elementów SILP podmiotom zewnętrznym, konserwującym poszczególne elementy SILP w ramach zawartych umów lub innym podmiotom wyłonionym na podstawie odrębnych procedur.
3. W przypadku braku możliwości realizacji modyfikacji w terminie oczekiwanym w zleceniu DGLP, priorytety realizacji modyfikacji ustalają w trybie roboczym członkowie ścisłego kierownictwa DGLP na wniosek naczelnika WI w DGLP.
4. Zmiany w SILP wynikające z usunięcia błędów lub modyfikacji przekazywane są przez Wykonawców w postaci kodów źródłowych, w formacie wymaganym przez

SZKZ, wraz dokumentacją techniczną, analityczną i instrukcją użytkownika.

5. Kody źródłowe podlegają weryfikacji w SZKZ pod względem ich poprawności.
6. Po pozytywnym wyniku tej weryfikacji następuje kompilacja kodów źródłowych do wersji wykonywalnej realizowana w SZKZ i przekazanie oprogramowania do testów w ZILP oraz w jednostkach testowych LP powoływanych odrębnymi zarządzeniami Dyrektora Generalnego Lasów Państwowych.
7. Integralną częścią procesu testowania jest ocena przedłożonej dokumentacji wymienionej w ust. 4 ocena dokumentacji jest realizowana przez ZILP, jednostki testowe i zespoły zadaniowe powołane przez Dyrektora Generalnego LP.
8. Pozytywny wyników testów oprogramowania oraz pozytywna ocena dokumentacji jest podstawą przekazania modyfikacji do wdrożenia w jednostkach LP.

§ 9.
Wdrażanie zmian w systemie LAS

1. Za dystrybucję i udostępnienie nowych wersji oprogramowania aplikacji LAS odpowiada Dyrektor ZILP.
2. Pakiety instalacyjne zawierające nowe wersje oprogramowania są udostępniane za pomocą SZKZ.
3. Udostępnienie autoryzowanego pakietu instalacyjnego, za pomocą SZKZ, jest jednoznaczne z poleceniem jego instalacji i wdrożenia na wszystkich szczeblach organizacyjnych.
4. Za dostosowanie do zmian w LAS specyficznych aplikacji dedykowanych dla zakładów Lasów Państwowych (krajowych i regionalnych) i ich wdrożenie odpowiada Dyrektor ZILP.

§ 10.
Wsparcie użytkowników w procesie wdrażania i eksploatacji SILP

1. Usługi wsparcia użytkowników w procesie wdrażania i eksploatacji SILP świadczą zgodnie z właściwym zakresem merytorycznym:
   a) pracownicy wydziałów DGLP w odniesieniu do wszystkich pracowników jednostek LP,
   b) pracownicy wydziałów rdLP w stosunku do pracowników biura rdLP i jednostek nadzorowanych przez rdLP,

c) regionalni instruktorzy SILP w stosunku do pracowników biura rdLP i jednostek nadzorowanych przez rdLP,
d) członkowie zespołów zadaniowych powołanych przez Dyrektora Generalnego Lasów Państwowych w zakresie określonym przez zarządzenie, w odniesieniu do wszystkich pracowników jednostek LP,
e) koordynatorzy regionalni SZBM w odniesieniu do pracowników biura rdLP i jednostek nadzorowanych,
f) koordynatorzy centralni SZBM w odniesieniu do wszystkich pracowników jednostek LP,
g) ZILP w odniesieniu do wszystkich pracowników jednostek LP.

2. Usługi wsparcia zdefiniowane w ust. 1. mogą być realizowane za zgodą i na wniosek poprzez bezpośredni dostęp do baz danych jednostki zgłaszającej problem.

§ 11.
Instrukcje użytkownika

1. Do każdego modułu funkcjonalnego SILP jest opracowywana instrukcja użytkownika.
2. Instrukcje użytkownika opracowuje ZILP na podstawie materiałów własnych lub dokumentacji przekazywanych przez wykonawców.
3. Instrukcje są udostępniane dla użytkowników SILP w bazie wiedzy o systemie informatycznym LP.
4. ZILP zobowiązany jest do dokonywania integracji instrukcji SILP z instrukcjami przekazanymi przez wykonawców. W okresie do czasu jej publikacji dopuszcza się wykorzystanie przez użytkowników instrukcji przygotowanej przez podmiot wykonujący modyfikację."

§2

Zmienia się treść załącznika nr 5 do zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który otrzymuje brzmienie:

„WZÓR OŚWIADCZENIA PRACOWNIKA

Miejscowość ..... dnia ...../...../.....

Imię i nazwisko: .....

Jednostka Lasów Państwowych: ....

Świadoma/y odpowiedzialności karnej, cywilnej i służbowej, wynikającej z przepisów prawa dotyczących ochrony danych osobowych, ochrony informacji niejawnych, kodeksu pracy, kodeksu cywilnego, kodeksu karnego oraz regulaminu pracy w jednostce organizacyjnej LP, niniejszym:

1) przyjmuję do wiadomości, że e-maile oraz korzystanie z Internetu mogą być monitorowane zgodnie z art. 22^3 Kodeksu pracy;
2) zobowiązuję się do:
   - przestrzegania „Zasad bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych" i powstrzymania się od jakichkolwiek działań niezgodnych z Zasadami, bądź nieprzewidzianych przez Zasady,
   - przestrzegania „Regulaminu użytkowania Konta Pocztowego LP",
   - zachowania w tajemnicy wszelkich danych (w tym także, gdy ustanie mój stosunek pracy lub cywilnoprawny w jednostce Lasów Państwowych), o których użytkownik posiadł wiedzę korzystając z systemu informatycznego Lasów Państwowych,
   - zachowania w tajemnicy danych (w tym także, gdy ustanie mój stosunek pracy lub cywilnoprawny w jednostce Lasów Państwowych), które mogłyby umożliwić osobom niepowołanym dostęp do systemu informatycznego Lasów Państwowych, w szczególności: identyfikatorów, haseł, nazw komputerów i numerów IP,
   - powstrzymania się od jakichkolwiek prób przełamywania zabezpieczeń systemów informatycznych,
   - powiadamiania przełożonych o wszelkich znanych mi przypadkach, które mogłyby świadczyć o próbie przełamania bądź przełamaniu tych zabezpieczeń,
   - pokrycia wszelkich start i szkód, jakie faktycznie odniosły Lasy Państwowe na skutek nieprzestrzegania Zasad lub niewypełnienia któregokolwiek z powyższych zobowiązań."

§3

1. Zarządzenie wchodzi w życie z dniem podpisania z wyjątkiem § 3 pkt 5 załącznika nr 1 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r., który wchodzi w życie 1 stycznia 2023 r.
2. Dotychczasowy przepis § 2 pkt 6 zmienianego załącznika nr 1 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. stosuje się do 31 grudnia 2022 r.

p.o. DYREKTORA GENERALNEGO
Lasów Państwowych

Józef Kubica

Polityka kopii zapasowych SILP

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe zmienionego Zarządzeniem nr 12 z dnia 3 lutego 2022 r.

Metryka Dokumentu

Data	Autor	Wersja	Opis zmiany
2022.02.15	EI.C	2.0	Aktualizacja zasad, retencji, przechowywania i przenoszenia kopii
2017-09-13	OI.C	1.0	Pierwsza wersja dokumentu

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.04.01 10:50:40 +02'00'

.....

I. Terminy użyte w tekście

Terminy użyte w treści mają następujące znaczenie:

1. **Lasy Państwowe, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **SILP** – System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
3. **System LAS** – system, podstawowa aplikacja biznesowa LP.
4. **WAN LP** – sieć rozległa Lasów Państwowych, komputerowa sieć modelu TCP/IP odpowiedzialna za przesyłanie danych pomiędzy jednostkami LP.
5. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
6. **Administrator SILP** – pracownicy WZI lub osoby odpowiedzialne za zasoby SILP we własnej jednostce.
7. **Użytkownik SILP** - pracownik Lasów Państwowych w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonujących prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.
8. **Dane SILP stanowiące tajemnice przedsiębiorstwa** – dane stanowiące tajemnicę przedsiębiorstwa zgodnie z klasyfikacją danych określoną w Zarządzeniu nr 48 Dyrektora Generalnego Lasów Państwowych z dnia 6 października 2010 r.
9. **KNX** – „Stanowisko Leśniczego" rozwiązanie udostępniające leśniczemu niezbędne elementy Systemu Informatycznego Lasów Państwowych.
10. **Kopia bezpieczeństwa** – dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.
11. **Archiwizacja** – czynność przeniesienia danych w celu ich długotrwałego przechowywania.

II. Kopie zapasowe danych ze stacji roboczych

1. Zakres obejmujący kopie danych użytkowników SILP:
   a) **na stacjach roboczych, komputerach stacjonarnych i przenośnych**: dokumenty, lokalne bazy danych, lokalna poczta elektroniczna lub innych wybrane przez użytkownika dane,
   b) **na innych urządzeniach**: dokumenty unikatowe, czyli takie które nie mają wykonywanych kopii bezpieczeństwa, a są dokumentami służbowymi,
   c) dokumenty tworzone **przez użytkowników KNX w leśnictwach**.

2. Kopie bezpieczeństwa danych wymienionych w pkt. 1 muszą:
   a) być wykonywana przynajmniej raz na dwa tygodnie,
   b) być przechowywane przez co najmniej dwa tygodnie,

III. Kopie zapasowe danych systemów sieciowych i serwerowych SILP

1. Zakres obejmujący kopie bezpieczeństwa produkcyjnie użytkowanych systemów sieciowych i serwerowych SILP:
   a) **serwery świadczące usługi w sieci WAN LP oraz Internet** – kopii podlegają unikatowe dane niezbędne do odtworzenia w pełni funkcjonalnego systemu/serwisu w przypadku całkowitej awarii lub zniszczenia nośnika źródłowego,
   b) **urządzenia sieciowe w tym urządzenia bezdyskowe** - między innymi: routery, przełączniki sieci lokalnych Ethernet, elementy systemu telefonii IP, koncentratory WiFi oraz inne urządzenie, których odtworzenie z dokumentacji trwa więcej niż 8h. Kopii podlegają pliki konfiguracyjne umożliwiające odtworzenie w pełni funkcjonalnego urządzenia.
2. Kopie bezpieczeństwa danych wymienionych w pkt. 1 lit. a) muszą spełniać następujące warunki:
   a) retencja wykonywanych kopii musi być uzależniona od zmienności danych i ich krytycznego znaczenia jednak nie rzadziej niż raz w tygodniu,
   b) każda wykonana kopia musi być przechowywana przez co najmniej dwa tygodnie,
   c) wymagane jest, żeby system backup posiadał co najmniej dwie kopie danych wymienionych w pkt. 1 lit. a)
   d) system kopi bezpieczeństwa musi być testowany, wymaga się przeprowadzenia testowego odtworzenia przynajmniej raz na miesiąc,
3. Kopie bezpieczeństwa danych wymienionych w pkt. 1 lit. b) muszą spełniać następujące warunki:
   a) kopia bezpieczeństwa musi być wykonywana po każdej zmianie konfiguracji urządzenia lub minimum raz w miesiącu
   b) każda wykonana kopia musi być przechowywana przez co najmniej 6 miesięcy,
   c) jeżeli ostatnia wykonana kopia jest starsza niż 6 miesięcy, należy wykonać nową kopie konfiguracji ,

IV. Kopie bezpieczeństwa systemu LAS

1. Zakres obejmujący kopie bezpieczeństwa produkcyjnych danych systemu LAS:
   a) bazy danych,
   b) serwery bazodanowe,
   c) serwery aplikacyjne,
   d) serwery infrastruktury zaliczane do systemy LAS.
2. Retencja wykonywanych kopii bezpieczeństwa:
   a) kopie baz danych oraz innych danych wchodzących w zakres polityki rachunkowości należy wykonywać zgodnie z postanowieniami Polityki Rachunkowości PGL LP,
   b) pełne kopie bezpieczeństwa danych systemu LAS:
      i. „Kopia dzienna" - tworzona jest co najmniej raz dziennie, Każda kopia jest testowo odtwarzana w dniu jej wykonania,
      ii. „Kopia tygodniowa"- tworzona jest co najmniej raz w tygodniu i w formie zaszyfrowanej przenoszona jest do innej lokalizacji.
   c) pełne kopie bezpieczeństwa systemów operacyjnych serwerów bazodanowych, serwerów aplikacji, serwerów infrastruktury:
      i. „Kopia tygodniowa" - tworzona jest co najmniej raz w tygodniu i przenoszona jest do innej lokalizacji. Jeżeli przeniesienie kopii jest za pośrednictwem fizycznego nośnika przewożonego do innej lokalizacji to dane przewożone muszą być w formie zaszyfrowanej.
      ii. raz w miesiącu ostatnia utworzona kopia tygodniowa musi zostać testowo odtworzona.
3. Archiwizacja danych systemu LAS – tygodniowe kopie bezpieczeństwa muszą być przechowywane w okresie zgodnym z Polityką Rachunkowości PGL LP.

V. Bezpieczeństwo wykonywanych kopii zapasowych

1. System – klient z którego wykonuje się kopie bezpieczeństwa nie może mieć dostępu w trybie zapisu/usuwania/nadpisywania poprzednich kopii bezpieczeństwa. Uprawnienia do zapisanych kopii bezpieczeństwa musza być nadawane i kontrolowane przez system/serwer kopii bezpieczeństwa. Zalecane jest aby inicjalizacja procesu kopi zapasowej była po stronie serwera kopii zapasowej.
2. Dostęp do kopii bezpieczeństwa systemów mogą mieć jedynie uprawnieni administratorzy SILP.
3. Kopie danych muszą być przechowywane poza miejscem przetwarzania.

4. Kopie danych muszą być przechowywane w sposób bezpieczny, muszą być zabezpieczone przed negatywnym wpływem środowiska, zniszczeniem oraz dostępem osób nieuprawnionych.

Polityka dla ruchu w sieci WAN LP

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe zmienionego Zarządzeniem nr 12 z dnia 3 lutego 2022 r.

Metryka Dokumentu

Data	Autor	Wersja	OpisZmiany
2017-09-13	OI.C	1.0	Pierwsza wersja dokumentu
2022.02.15	EI.C	2.0	Zmiany dotyczące polityki dla sieci LP-G i IoT

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.03.14 11:22:42 +01'00'

.....

I. Terminy użyte w tekście

Terminy użyte w treści mają następujące znaczenie:

1. **Lasy Państwowe, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **SILP** – System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
3. **System LAS** – system, podstawowa aplikacja biznesowa LP.
4. **WAN LP** – sieć rozległa Lasów Państwowych, komputerowa sieć modelu TCP/IP odpowiedzialna za przesyłanie danych pomiędzy jednostkami LP.
5. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
6. **Administrator SILP** – pracownicy WZI lub osoby odpowiedzialne za zasoby SILP we własnej jednostce.
7. **CP** – Centrum Podstawowe przetwarzania danych.
8. **CZ** – Centrum Zapasowe przetwarzania danych.
9. **rdLP** – regionalna dyrekcja Lasów Państwowych.

II. Założenia

Sieć WAN LP działa w oparciu o model TCP/IP i jest głównym medium odpowiedzialnym za przesyłanie danych oraz komunikację pomiędzy jednostkami LP. Zbudowana jest w oparciu o infrastrukturę i usługi transmisji danych dostarczanych przez firmy zewnętrzne, działa w topologii „chmury" i umożliwia połączenia „każdy z każdym" bezpośrednio pomiędzy jednostkami LP. Używana architektura sieci wymaga implementacji zasad definiujących dozwolony ruch wewnątrz sieci WAN LP, wynikających z:

a) struktury organizacyjnej PGL LP,

b) wymagań bezpieczeństwa przetwarzanych danych,

c) wymagań dostępności i niezawodności sieci.

III. Miejsce implementacji polityk dla ruchu w sieci WAN LP

Zdefiniowane zasady dla ruchu w sieci WAN LP są implementowane na urządzeniach dostępowych do sieci WAN LP oraz na dedykowanych zaporach sieciowych

znajdujących się w CP i CZ. Urządzenia są zainstalowane w jednostkach LP i są ich własnością.

IV. Definicja polityk dla ruchu w sieci WAN LP

1. Założenia:

1.1. Polityka dla ruchu jest jednolita dla wszystkich jednostek w ramach każdej z rdLP. Z zasady jednolitej polityki w ramach rdLP wykluczone są reguły:

a) dopuszczające ruch tuneli GRE dla dostępu gościnnego WiFi,

b) reguły anty-spoofing dla ruchu z lokalizacji.

1.2. Podstawą filtrowania ruchu na urządzeniach w jednostkach LP jest warstwa sieciowa i podsieci IP.

1.3. Ruch filtrowany jest również w warstwie transportowej w oparciu o numery portów protokołów TCP i UDP dla ruchu:

a) DHCP,

b) DNS,

c) NetBIOS i SMB.

1.4. Z powodu braku jednolitej funkcjonalności wszystkich urządzeń sieciowych używanych w jednostkach LP do filtracji nie używa się trybu stanowych zapór sieciowych (ang. Stateful Inspection).

1.5. Głównym miejscem kontroli ruchu i realizacji polityk są interfejsy zewnętrzne urządzeń, przez które przychodzi ruch do lokalizacji, dlatego ruch wychodzący jest filtrowany mniej restrykcyjne niż ruch przychodzący do lokalizacji.

1.6. Ruch do sieci Internet jest filtrowany na centralnych zaporach sieciowych w CP i CZ.

1.7. W jednostkach wydzielone są funkcjonalne segmenty sieci separujące domeny rozgłoszeniowe. Możliwa jest separacja zarówno fizyczna jak i logiczna realizowana w oparciu o VLAN. Między innymi wyróżnia się funkcjonalne segmenty:

a) segment sieci LAN PC – obligatoryjny w każdej lokalizacji,

b) segment sieć telefonii IP,

c) segment sieci WiFi gościnnego,

d) segment sieci usług ogólnie dostępnych DMZ – tworzony jedynie w rdLP,

e) segment sieci zarządzającej MGMT – tworzony jedynie w rdLP,

f) segment sieci LAN dla drukarek,

g) segment sieci dla monitoringu wizyjnego,

h) segment sieci dla urządzeń IoT

1.8. Każdy segment posiada ustaloną adresację IP z bramą na urządzeniu sieciowym w lokalizacji i zdefiniowaną polityką dla ruchu. Dodatkowo interfejs na urządzeniu sieciowym z podłączeniem danego segmentu posiada ustalony opis.

1.9. Jeżeli zdefiniowane polityki nie posiadają reguły, która dopasuje filtrowany ruch jest on blokowany z logowaniem (blokowanie na końcu przetwarzania listy dostępowej).

2. Reguły

2.1. Polityka dla ruch przychodzącego do jednostki.

Opis interfejsu: WAN

Reguły dla ruchu:

a) dozwolony ruch protokołu eigrp,

b) zablokowany ruch broadcast,

c) dozwolony ruch z sieci jednostek podległych do kontrolera domeny AD w rdLP,

d) dozwolony ruch z centralnej sieci zarządzającej,

e) dozwolony ruch z sieci Mobile Access do DMZ rdLP,

f) zablokowany pozostały ruch z sieci Mobile Access,

g) dozwolony ruch protokołu ICMP dla adresacji wewnętrznej LP,

h) dozwolony ruch z adresacji wewnętrznej LP do sieci DMZ rdLP,

i) dozwolony ruch z sieci systemu LAS do sieci DMZ rdLP,

j) dozwolony ruch z sieci VPN do sieci rdLP i jednostek podległych,

k) dozwolony ruch z vCenter DGLP do sieci MGMT rdLP,

l) zablokowany pozostały ruch do sieci MGMT rdLP i DMZ rdLP,

m) dozwolony ruch z adresacji puli serwerowej sieci rdLP do sieci rdLP i jednostek podległych,

n) dozwolony ruch z adresacji interfejsów loopback ruterów LP do adresacji puli serwerowej sieci rdLP,

o) dozwolony ruch z sieci rdLP i jednostek podległych do adresacji puli serwerowej sieci rdLP,

p) dozwolony ruch z sieci MGMT rdLP do sieci rdLP i jednostek podległych,

q) dozwolony ruch z sieci centralnych usług sieciowych do adresacji puli serwerowej sieci rdLP i jednostek podległych,

r) dozwolony ruch z sieci VPN do sieci rdLP i jednostek podległych,

s) dozwolony ruch sieci telefonii IP jednostek LP do sieci telefonii IP rdLP i jednostek podległych,

t) dozwolony ruch tuneli GRE dla dostępu gościnnego WiFi,

u) dozwolony ruch TACACS do interfejsów loopback ruterów rdLP i jednostek podległych,

v) dozwolony ruch jetdirect z sieci APN do sieci rdLP i jednostek podległych,

2.2. Polityka dla ruchu z segmentu sieci LAN PC.

Opis interfejsu: PC_LAN

Reguły dla ruchu:

a) dozwolony ruch UDP do centralnych kontrolerów domeny AD,

b) dozwolony ruch do sieci MGMT dla uprawionych administratorów SILP,

c) zabroniony pozostały ruch do sieci MGMT,

d) dozwolony ruch broadcast dla DHCP,

e) zabroniony pozostały ruch broadcast,

f) dozwolony ruch do sieci usług centralnych,

g) dozwolony ruch do centralnej sieci intranet,

h) dozwolony ruch do zakresu adresacji puli serwerowej w PC_LAN własnej rdLP,

i) dozwolony ruch z zakresu adresacji puli serwerowej do całej sieci rdLP i jednostek podległych,

j) zablokowany ruch NetBios i SMB,

k) dozwolony pozostały ruch z adresacji sieci.

2.3. Polityka dla ruchu z segmentu sieci zarządzającej.

Opis interfejsu: MGMT

Reguły dla ruchu:

a) zablokowany ruch broadcast,

b) dozwolony ruch do całej sieci rdLP i jednostek podległych,

c) dozwolony ruch do centralnej sieci usług sieciowych w CP,

d) dozwolony ruch do centralnej sieci MGMT i DMZ w CP,

e) zablokowany ruch NetBios i SMB,

f) dozwolony pozostały ruch z adresacji sieci.

2.4. Polityka dla ruchu z segmentu sieci DMZ.

Opis interfejsu: DMZ

Reguły dla ruchu:

a) zablokowany ruch broadcast,

b) dozwolony ruch do centralnej sieci DMZ,

c) zablokowany ruch do sieci wewnętrznej WAN LP,

d) dozwolony pozostały ruch z adresacji sieci.

2.5. Polityka dla ruchu z segmentu sieci telefonii IP.

Opis interfejsu: VOICE

Reguły dla ruchu:

a) dozwolony ruch protokołu DHCP,

b) zabroniony inny ruch broadcast,

c) dozwolony ruch ip do sieci telefonii IP w pozostałych lokalizacjach LP,

d) dozwolony ruch ip do sieci własnej rdLP,

e) dozwolony ruch ip do sieci połączeń VPN site-to-site,

f) dozwolony ruch DNS do serwerów centralnych kontrolerów domeny AD.

2.6. Polityka dla ruchu z segmentu sieci WiFi LP-G oraz IoT

Opis interfejsu: GUEST_WIFI_LAN, IoT

Reguły dla ruchu:

a) dozwolony ruch z sieci LP-G do kontrolera WiFi,

b) zablokowany ruch do sieci WAN,

c) dozwolony ruch do internetu,

d) dozwolony ruch DHCP,

e) zablokowany pozostały ruch,

2.7. Ruch dla pozostałych segmentów sieci.

Opis interfejsu: ustalony prze ZCI

Reguły dla ruchu:

a) dozwolony jedynie ruch na potrzeby realizacji funkcji i poprawnego działania zainstalowanych w segmencie systemów,

b) zablokowany pozostały ruch.

Zasady adresacji IP w sieci LP

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe zmienionego Zarządzeniem nr 12 z dnia 3 lutego 2022 r.

Metryka Dokumentu

Data	Autor	Wersja	Opis zmian
2017-12-29	OI.C	1.0	Pierwsza wersja dokumentu
2018-02-27	OI.C	1.0.1	Poprawki dotyczące masek sieciowych dla MobileAccess SSL VPN orac OfficeMode dla klienta VPN Check Point (pkt IV.8)
2018-03-14	OI.C	1.1	Przydział adresacji IP na potrzeby sieci zarządzającej na poziomie nadleśnictw (pkt IV.3). Doprecyzowanie opisu dotyczącego sieci na potrzeby iSCSI (pkt IV.3). Przydział segmentu na potrzeby iSCSI (pkt IV.2)
2018-04-16	OI.C	1.2	Zmiany dotyczące adresacji sieci technicznej (pkt IV.3) – zmiana etykiety oraz przydział numeru VLan. Wydzielenie sieci DMZ na poziomie jednostek danego regionu
2018-12-14	EI.C	1.3	Zmiany dotyczące adresacji sieci Office Mode dla dostępu VPN (pkt. IV.8). Zmiana terminu realizacji zmian w adresacji sieci jednostek VPN.
2019-01-15	EI.C	1.4	Dodanie sieci dla urządzeń bez poświadczeń 802.1x
2019-02-01	EI.C	1.5	Dodanie zapisu dotyczącego zasady stosowania segmentów sieci (pkt. IV).
2019-02-13	EI.C	1.6	Dodanie etykiet dla nowych segmentów sieci wraz z numerami VLan. Poprawki w adresacji sieci DMZ i Kwarantanny.
2022-02-15	EI.C	2.0	Dodanie sieci dla urządzeń typu IoT i drukarek, dodanie numeracji VLAN

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.03.14 11:25:43 +01'00'

.....

I. Terminy użyte w tekście

Terminy użyte w treści mają następujące znaczenie:

1. **Lasy Państwowe, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **SILP** – System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
3. **System LAS** – system, podstawowa aplikacja biznesowa LP.
4. **WAN LP** – sieć rozległa Lasów Państwowych, komputerowa sieć modelu TCP/IP odpowiedzialna za przesyłanie danych pomiędzy jednostkami LP.
5. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
6. **ZCI** – Zespół w WI DGLP do spraw Cyberbezpieczeństwa Informatycznego, odpowiedzialna za nadzór nad bezpieczeństwem SILP.
7. **Administrator SILP** – pracownicy WZI lub osoby odpowiedzialne za zasoby SILP we własnej jednostce.
8. **Użytkownik SILP** - pracownik Lasów Państwowych w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonujących prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.
9. **KNX** – „Stanowisko Leśniczego" rozwiązanie udostępniające leśniczemu niezbędne elementy Systemu Informatycznego Lasów Państwowych.

II. Założenia

Niniejszy dokument określa zasady przydziału adresów IP w LP.

Zasady przydziału adresów/sieci IP powinny zapewniać:

— unikalność adresacji IP w ramach LP,

— spójność adresacji pod względem funkcjonalnym na różnych poziomach struktury organizacyjnej LP,

— identyfikowalność adresacji zarówno pod względem funkcjonalnym jak i organizacyjnym o ile jest to możliwe.

W zakresie konfiguracji niniejszy dokument dotyczy:

a) adresacji IP dla lokalnych segmentów sieci jednostek LP,

b) adresacji IP dla sieci połączeniowych pomiędzy urządzeniami brzegowymi w sieci LP,

c) adresacji IP dla sieci firm zewnętrznych posiadających łącza bezpośrednie do sieci WAN LP,

d) adresacji IP dla sieci w jednostkach nieposiadających łącz bezpośrednich do sieci WAN LP,

e) adresacji IP dla sieci przeznaczonych do połączeń z wykorzystaniem wydzielonej sieci GSM (prywatny APN) do sieci WAN.

III. Wymogi formalne

Za przydział adresacji IP w LP odpowiedzialny jest ZCI. ZCI prowadzi elektroniczny rejestr przydzielonych sieci/adresów IP. W jednostkach LP mogą funkcjonować tylko i wyłącznie sieci/adresy przydzielone i zarejestrowane w systemie elektronicznym.

Przydział adresacji IP odbywa się na wniosek zainteresowanej jednostki. Wniosek taki powinien określać:

— przeznaczenie segmentu sieci,
— dozwolony ruch sieciowy do/z nowego segmentu sieci,
— niezbędną pojemność segmentu oraz uzasadnienie jego stosowania.

ZCI rozpatruje wniosek a następnie podejmuje decyzję o przydzieleniu adresacji IP lub proponuje inne rozwiązanie spełniające potrzeby wnioskodawcy.

IV. Zasady adresacji

Podstawową zasadą w przypadku adresacji jest stosowanie tylko i wyłącznie wykorzystywanych przez jednostkę segmentów sieci. Segmenty sieci, które w danej jednostce nie są wykorzystywane nie powinny być konfigurowane na urządzeniach.

1. W środowisku LP wykorzystywane są następujące sieci:

   — 10.0.0.0/8 (255.0.0.0),

   — 172.16.0.0/13 (255.248.0.0).

   Stosowanie innych sieci dozwolone jest tylko w uzasadnionych przypadkach.

   W ramach niniejszego dokumentu wykorzystywane są następujące oznaczenia:

   r – numer regionu,

   n – numer jednostki LP, w przypadku rdLP n=0,

   z – numer zakładu LP,

f – numer firmy zewnętrznej,

x – numer podsieci przyznany jednostce/firmie (najczęściej jest on sumą określonej liczby i numeru jednostki/firmy zależny od funkcjonalności segmentu),

2. W środowisku LP wyróżnia się następujące podstawowe segmenty funkcjonalne:

Numer	Etykieta	Opis/przeznaczenie
50	Monitoring	Sieć monitoringu wizyjnego
150	Kwarantanna	Sieć dla urządzeń nieuwierzytelnionych
190	Storage	Sieć zasobów dyskowych iSCSI
200, 200+n	Telefonia IP	Sieć telefonii IP, video
251	Intranet	Sieć Intranet
252	MGMT	Sieć zarządzająca
253	DMZ	Sieć DMZ

3. Adresacja IP dla lokalnych segmentów sieci jednostek LP.

Lokalne segmenty sieci jednostek powinny być adresowane następująco:

Segment/podsieć	Etykieta	VLAN	Opis/przeznaczenie
10.r.n.0/24	**LAN**	1	Sieć LAN PC
10.200+r.100+n.0/25	**WiFi**	299	Sieć gościnna WiFi
10.200+r.100+n.128/25	**IoT**	298	Sieć urządzeń IoT
10.r.200+n.0/24	**Telefonia IP**	200	Sieć telefonii i wideo IP
10.r.252.0/24	**MGMT**	252	Sieć zarządzająca (na poziomie regionu)
10.r.100+n.0/24	**MGMT**	252	Sieć zarządzająca na poziomie jednostek danego regionu
10.r.253.0/24	**DMZ**	253	Sieć DMZ (na poziomie regionu)
10.100+r.n.128/26	**DMZ**	253	Sieć DMZ na poziomie jednostek danego regionu
10.r.251.0/24	**Intranet**	251	Sieć Intranet (na poziomie regionu)
10.100+r.n.0/25	**Intranet**	251	Sieć przeznaczona na inne urządzenia i usługi m.in. te, dla których nie przydzielono oddzielnej sieci/segmentu
10.r.150.0/24	**Drukarki LAN**	150	Sieć LAN drukarek (na poziomie regionu)
10.100+r.n.224/27	**Kwarantanna**	999	Sieć dla urządzeń nieuwierzytelnionych
10.100+r.100+n.0/24	**Monitoring**	50	Sieć monitoringu wizyjnego

10.r.190.0/24	**Storage**	190	Sieć zasobów dyskowych iSCSI (sieć nierutowalna, ruch we/wy tej sieci zablokowany na routerze jednostki), jednakowa dla wszystkich jednostek danego regionu

W sieci LAN PC przyjęty został następujący podział sieci na dwie pule:

— 10.r.n.1-63 – pula serwerów i urządzeń sieciowych,
— 10.r.n.64-254 – pula stacji roboczych.

Szczegółowy przydział adresów IP przedstawia poniższa tabela:

Segment/podsieć	Ostatni oktet adresu	Opis/przeznaczenie
10.r.n.	**1**	Router główny
	2-4	Routery dodatkowe
	5-9	Przełączniki sieciowe
	10-39	Serwery i drukarki, w tym drukarka fiskalna z zarezerwowanym adresem **10.r.n.30**
	40-45	Adresy zarezerwowane na potrzeby usług centralnych: - kontroler domeny **10.r.n.40**
	46-63	Serwery, drukarki i pozostałe urządzenia sieciowe
	64-254	Stacje robocze

4. Adresacja IP dla sieci połączeniowych pomiędzy urządzeniami brzegowymi w sieci LP - Łącza podstawowe i zapasowe (segment pomiędzy ruterem LP i ruterem operatora).

   Połączenia wymagają zarezerwowania wydzielonych podsieci IP z puli adresów przyznanej dla każdej struktury rdLP. Podsieć ta przyznawana będzie według poniższej zasady:

   — dla rdLP: 10.155.254.x/30 (255.255.255.252),
   — dla nadleśnictw: 10.r.155.x/30 (255.255.255.252),

5. Adresacja IP dla lokalnych segmentów sieci firm zewnętrznych posiadających łącza bezpośrednie do WAN LP.

   Lokalne segmenty sieci firm powinny być adresowane następująco:

   — 10.100.x.0/24 (255.255.255.0),

6. Adresacji IP dla sieci w jednostkach nieposiadających łącz bezpośrednich do sieci WAN LP.

   W ramach sieci WAN LP dopuszcza się wykorzystanie innych łączy niż MPLS. Sytuacje takie mogą wystąpić w przypadku braku możliwości technicznych instalacji łącza MPLS w danej lokalizacji. Jednostki takie mogą wykorzystywać łącza Internetowe w celu zestawiania bezpiecznych, szyfrowanych tuneli VPN lub GRE do wyznaczonych bram dostępowych.

   W przypadku jednostek wykorzystujących łącza alternatywne adresacje nadawane są według następującego schematu (migracja do końca czerwca 2019 r. dla jednostek posiadających adresy z 10.x.x.x):

   — jednostki LP o zasięgu krajowym:

      172.18.z0.0/24 (255.255.255.0) – sieć LAN PC,

      172.18.z1.0/24 (255.255.255.0) – sieć MGMT,

   — firmy zewnętrzne:

      172.19.rf.0/28 (255.255.255.240) – sieć firmy świadczącej usługi na poziomie regionu (usługi regionalne),

      172.18.z1.0/19 (255.255.224.0) – sieci firm świadczących usługi centralne, w ramach tej sieci będą przydzielane podsieci w zależności od potrzeb,

   — jednostki LP o zasięgu regionalnym, jednostki podległe rdLP (w tym ośrodki szkoleniowe):

      172.2x.r0.0/24 (255.255.255.0) – sieć LAN PC,

      172.2x.r1.0/25 (255.255.255.128) – sieć OfficeMode (dla dostępu VPN),

      172.2x.r1.128/25 (255.255.255.128) – sieć MGMT,

      172.2x.r2-5.0/24 (255.255.255.0) – sieci dla sal szkoleniowych z dostępem do WAN LP,

      172.2x.r6-7.0/24 (255.255.255.0) – sieci techniczne,

      172.2x.r8.0/23 (255.255.252.0) – sieć gościnna z dostępem do Internetu, bez dostępu do WAN LP

7. Dostęp do sieci WAN LP poprzez sieć GSM

   W przypadku wykorzystania sieci GSM do usług transmisji danych dla potrzeb rejestratorów stosowane są odrębne adresacje sieciowe w uzgodnieniu z operatorami świadczącymi usługi.

8. Zdalny dostęp do sieci WAN LP

Dostęp zdalny wymaga zastosowania oddzielnej adresacji IP według poniższych zasad:

— obecnie wykorzystywane sieci:

10.0.249.0/24 (255.255.255.0) – sieć dla Cisco VPN Client,

10.0.236.0/23 (255.255.254.0) – sieć OfficeMode dla klienta CheckPoint VPN,

10.0.238.0/23 (255.255.254.0) - sieć OfficeMode dla klienta CheckPoint VPN,

10.0.240.0/23 (255.255.254.0) - sieć OfficeMode dla klienta CheckPoint VPN,

10.0.224.0/22 (255.255.252.0) – sieć dla Mobile Access SSL VPN,

10.0.228.0/22 (255.255.252.0) – sieć dla Mobile Access SSL VPN.

— sieci docelowe (migracja do końca czerwca 2019 r.):
172.16.4.0/23 (255.255.254.0) – sieć OfficeMode dla klienta CISCO VPN,

172.16.64.0/18 (255.255.192.0) – sieć OfficeMode dla MobileAccess i klienta VPN – węzeł testowy,

172.17.0.0/18 (255.255.192.0) – sieć OfficeMode dla MobileAccess i klienta VPN w CP,

172.17.64.0/18 (255.255.192.0) – sieć OfficeMode dla MobileAccess i klienta VPN w CP,

172.17.128.0/18 (255.255.192.0) – sieć OfficeMode dla MobileAccess i klienta VPN w CZ,

172.17.192.0/18 (255.255.192.0) – sieć OfficeMode dla MobileAccess i klienta VPN w CZ,

W uzasadnionych przypadkach dotychczasowa adresacja może zostać utrzymana np. w jednostkach, które planowane są do włączenia do sieci WAN LP (łącza bezpośrednie).

9. Sieci w węzłach centralnych WAN LP (centrum podstawowe i zapasowe)

W węzłach centralnych WAN LP wykorzystywane są sieci z adresacji:

— 10.0.0.0/16 (255.255.0.0)

Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe.

Metryka Dokumentu

Data	Autor	Wersja	OpisZmiany
2017-09-13	OI.C	1.0	Pierwsza wersja dokumentu
2022.02.15	EI.C	2.0	Zmiany dotyczące procedury wdrożenie sieci bezprzewodowej

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.05.27 12:19:52 +02'00'

.....

Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP - Projekt techniczny

I. Kolejność postępowania przy realizacji wdrożenia sieci bezprzewodowej w jednostce LP:

1. Wybór technologii wdrożenia lokalnej sieci bezprzewodowej
2. Zgłoszenie przez jednostkę zapotrzebowania na dostęp do sieci bezprzewodowej drogą służbową do Wydziału Informatyki DGLP wskazując przy tym wybraną technologię.
3. Zakup odpowiednich urządzeń i licencji jeśli wymagane.
4. Instalacja i konfiguracja urządzeń w wymaganym zakresie oraz modyfikacja konfiguracji lokalnych przełączników sieciowych.
5. Konfiguracja serwerów DHCP, Radius i kontrolera sieci oraz routerów i firewalli.

II. Podział zadań

1. Jednostka LP, w której wdrażany jest dostęp z wykorzystaniem sieci bezprzewodowych dokonuje wyboru i zakupu urządzeń oraz montażu i podłączenia do sieci LAN jednostki, zgodnie z projektem „Zasad adresacji IP w sieci LP".W przypadku nadleśnictw jednostką wspomagającą w tym zakresie jest RDLP.
2. Jednostka pilotująca wdrożenie zainstaluje/konfiguruje:
   a. Centralny Serwer Radius
   b. Kontroler AP
   c. Centralny Serwer (lub więcej) z portalem dostępowym
   d. Centralny serwer DHCP
3. Wydział Informatyki DGLP wykonuje/nadzoruje konfigurację routera jednostki oraz firewalla centralnego.

III. Wytyczne szczegółowe

Do budowy sieci bezprzewodowej należy użyć Punktów Dostępowych (Access Point), które są zarządzane za pomocą dedykowanego kontrolera AP. Strukturę będzie uzupełniał serwer Radius posiadający dostęp do odpowiedniego kontrolera domeny, serwer DHCP oraz serwer z portalem dostępowym dla dostępu gościnnego. Jednostka LP instaluje odpowiednią liczbę AP zależnie od wymagań lokalizacji ale nie mniej niż 2 sztuki aby zapewnić redundancje podczas awarii AP. Dla użytkowników dostępne będą 3 identyfikatory sieci (SSID), które pozwolą po autentykacji na korzystanie z odpowiednich zasobów. Do autentykacji będą wykorzystywane mechanizmy: serwer Radius, klucz dostępowy o długości 10 znaków ASCII, portal dostępowy wymagający kodu dostępu.

Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP - Projekt techniczny

1. Konfiguracji kontrolera AP:
   a. Konfiguracja identyfikatora sieci LP-W:
      i. Standard zabezpieczeń WPA2 AES.
      ii. Autentykacja przez Serwer RADIUS za pomocą certyfikatu użytkownika, komputer musi być zarejestrowany w AD (Serwer Radius sprawdza komputer w AD, użytkownik w grupie AD „WiFi [nazwa RDLP , Zakłady o zasięgu krajowym, DGLP]") dla wybranych urządzeń mobilnych (własnością urządzenia jest jednostka LP), urządzenia które nie mogą być dodane do AD otrzymają wystawione certyfikaty przez Centrum Certyfikacji LP pozwalające na dostęp do sieci.
      iii. Numer VLAN i adresacja IP zgodna z siecią LAN PC jednostki.
      iv. Dostęp do sieci LAN, WAN, Internet. Podczas awarii łącza WAN podstawowego oraz awaryjnego zastępuje ją na czas awarii sieć LP-A, pozwalająca tylko na dostęp do sieci LAN PC jednostki.

   b. Konfiguracja identyfikatora sieci LP-A:
      i. Standard zabezpieczeń WPA2 AES.
      ii. Autentykacja kluczem dostępowym o długości 10 znaków ASCII.
      iii. Numer VLAN i adresacja IP zgodna z siecią LAN PC jednostki.
      iv. Dostęp do sieci LAN. Sieć wykorzystywana tylko awaryjnie tylko podczas awarii łącza WAN podstawowego oraz awaryjnego. Dostęp możliwy po otrzymaniu klucza dostępowego od Służb Informatycznych. Klucz zostaje natychmiast zmieniony na inny przez Służby Informatyczne po usunięciu awarii łączy powodując tym samym powrót do sieci LP-W.

   c. Konfiguracja identyfikatora sieci LP-G (sieć gościnna):
      i. Standard open lub zabezpieczeń WPA2 AES.
      ii. Autentykacja za pomocą "kodu dostępu" wpisywanego w portalu dostępowym. Kody dostępu dostarczane są przez Służby Informatyczne do podległych jednostek według potrzeb. Kody po użyciu automatycznie tracą ważność. Służby Informatyczne mają możliwość dezaktywacji dowolnego kodu lub grupy kodów. Ustala się minimalne następujące typy kodów:
         1. Jedno urządzenie ważny 5 dni od aktywacji
         2. Jedno urządzenie ważny 1 dzień od aktywacji
         3. Wiele urządzeń ważny 5 dni od aktywacji
         4. Wiele urządzeń ważny 1 dzień od aktywacji
      iii. Numer VLAN zgodnie z projektem „Zasady adresacji IP w sieci LP" (cały ruch tej sieci będzie przesyłany tunelem, pomiędzy ruterem brzegowym jednostki a urządzeniem terminujący w węźle centralnym DGLP).

iv. Dostęp do sieci Internet (określone serwisy, możliwy VPN client). Podczas awarii łączy WAN LP w lokalizacji sieć nie jest dostępna.

2. Logi z AP mają być wysyłane do centralnego serwera logów znajdującego się w węźle centralnym DGLP.
3. Wymagane jest uruchomienie monitorowania w trybie rzeczywistym podłączonych bezprzewodowo użytkowników do każdej z sieci.
4. Wymagane jest uruchomienie funkcjonalności dającej możliwości zablokowania dowolnego połączenia do sieci bezprzewodowej po zgłoszeniu naruszeniu regulaminu.
5. Konfiguracja serwera RADIUS według poniższych założeń:
   a. Utworzenie polityki bezpieczeństwa zwierającej kontrolę czy komputer jest w AD LP i czy użytkownik jest w grupie „WiFi [nazwa RDLP , Zakłady o zasięgu krajowym, DGLP]" lub czy urządzenie posiada ważny certyfikat wystawiony przez Centrum Certyfikacji LP.
   b. Służby informatyczne RDLP przygotują odpowiedne wpisy w AD dla własnej gałęzi.
   c. Założenie grupy „WiFi [nazwa RDLP , Zakłady o zasięgu krajowym, DGLP]", która będzie użyta jako klient grupy nadrzędnej „WiFI LP".
   d. Każdy użytkownik mający mieć dostęp do sieci bezprzewodowej LP-W musi być w tej grupie.

6. Założenie grupy nadrzędnej „WiFi LP", która będzie zawierała grupy z gałęzi jednostek „WiFi [nazwa RDLP , Zakłady o zasięgu krajowym, DGLP]". Grupa ta będzie użyta w polityce bezpieczeństwa dostępu do sieci bezprzewodowej LP-W w serwerze RADIUS oraz centralnym GPO.
7. Wpisy w centralnym GPO dla użytkowników grupy „WiFi LP", które automatycznie dopiszą sieci LP-W, LP-A do komputerów, których użytkownicy będą w tej grupie.
8. Konfiguracja tunelu dla sieci LP-G pomiędzy ruterem brzegowym jednostki a urządzeniem terminujący w węźle centralnym DGLP, który pozwoli odseparować cały ruch od sieci WAN LP.
9. Urządzenie podłączone do sieci WAN LP nie może być jednocześnie połączone z siecią Internet za pomocą innego, dodatkowego łącza.
10. Sieć bezprzewodowa nie może być traktowana jako sieć podstawowa w Jednostce LP, nie zastępuje LAN jednostki a jedynie może ją uzupełniać.

Polityka dla ruchu na styku sieci WAN LP i Internet

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe zmienionego Zarządzeniem nr 12 z dnia 3 lutego 2022 r.

Metryka Dokumentu

Data	Autor	Wersja	Opis Zmiany
2022.02.15	EI.C	2.0	Zmiany dotyczące inspekcji ruchu
2017-09-13	OI.C	1.0	Pierwsza wersja dokumentu

ZATWIERDZIŁ:

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.03.15 09:51:10 +01'00'

.....

Polityka dla ruchu na styku sieci WAN LP i Internet - Projekt techniczny

1. Założenia

Polityka dla ruchu na styku sieci WAN LP i Internet realizowana jest w sposób zapewniający:

- bezpieczeństwo i ochronę zasobów SILP,
- dostęp jednostek organizacyjnych LP do sieci Internet w ramach realizowanych przez jednostki zadań służbowych,
- dostęp z sieci Internet do usług świadczonych pracownikom/jednostkom LP,
- dostęp z sieci Internet do usług świadczonych publicznie przez LP,
- zdalny dostęp do sieci WAN LP dla użytkowników SILP,
- zdalny dostęp do sieci WAN LP dla firm zewnętrznych,
- komunikację z podmiotami zewnętrznymi,
- optymalizację wykorzystania posiadanej publicznej adresacji IP.

2. Implementacja polityk dla ruchu na styku sieci WAN LP i Internet

1. Ruch na styku sieci WAN LP i Internet odbywa się przez centralne węzły sieciowe zlokalizowane w CP i CZ.
2. Ruch jest filtrowany przez zapory sieciowe i systemy zapobiegania włamaniom (IPS).
3. Ruch podlega inspekcji w warstwach 3-7 modelu ISO/OSI.
4. Ruch może podlegać deszyfracji w celu prowadzenia inspekcji.
5. Ruch na styku sieci WAN LP i Internet może być blokowany na podstawie adresów IP i ich geolokalizacji, zakresów sieci, nazw domenowych, protokołów, numerów portów, aplikacji, treści komunikacji, roli i identyfikatora użytkownika. W szczególności blokowane są:
   a) Adresy IP i nazwy DNS
      - o niskiej reputacji według klasyfikacji producenta systemu zapory sieciowej (Check Point),
      - znajdujące się na listach publikowanych przez CISRT GOV,
      - generujące nieprawidłowy ruch sieciowy i uznane przez pracowników ZCI za powodujące zagrożenie dla bezpieczeństwa SILP.

   b) Połączenia stanowiące próby przełamywania zabezpieczeń SILP.

   c) Połączenia w ramach których przesyłane jest złośliwe oprogramowanie lub odnośniki do niego prowadzące

   d) Połączenia inicjowane z systemów operacyjnych, które nie posiadają aktualnego wsparcia (EOL).

   e) Połączenia użytkowników naruszających zasady bezpiecznej eksploatacji SILP.

   f) Aplikacje niewymagane do realizacji zadań służbowych.

   g) Witryny w sieci Internet niewymagane do realizacji zadań służbowych. Klasyfikacji treści witryn określana jest na podstawie listy utrzymywanej przez producenta systemu zapory sieciowej (Check Point). Blokowane są strony należące do kategorii:

- Anonymizer
- BitTorrent protocol
- P2P File Sharing
- Pornography
- Botnets
- Child Abuse
- Gambling
- Games
- Hate / Racism
- MySpace Games
- Nudity
- Sex
- High Risk
- Personals / Dating

Użytkownik SILP może zgłosić do wykluczenia stronę, która jest zablokowana, w formie podpisanej wiadomości e-mail na adres ei.c@lasy.gov.pl. Wnioski będą podlegały analizie przez ZCI, w przypadku stwierdzenia braku przeciwwskazań będą dodawane do wykluczeń.

6. Ruch z sieci Internet do sieci WAN LP jest blokowany z wyłączeniem usług:
   a) świadczonych publicznie,
   b) połączeń VPN
      - dla użytkowników SILP,
      - połączeń VPN dla jednostek LP nie posiadających łącz do sieci WAN,
      - połączeń VPN firm i organizacji zewnętrznych.
7. Wszystkie usługi dostępne z publicznej sieci Internet muszą znajdować się w dedykowanych segmentach sieci DMZ, bez możliwości bezpośredniego dostępu do wewnętrznych zasobów SILP.

2.1. Zasady połączeń na styku sieci WAN LP i Internet

Ruch do sieci Internet			
Źródło	**Rodzaj połączenia**	**Akcja**	**Uwagi**
Sieci jednostek LP (sieci LAN)	Usługi w sieci Internet	Filtrowany	Inspekcja ruchu szyfrowanego
Sieci DMZ	Administracyjne	Filtrowany	Na potrzeby utrzymania systemów
Sieci MGMT	Administracyjne	Filtrowany	Na potrzeby utrzymania systemów
Sieci Intranet	Administracyjne	Filtrowany	Na potrzeby utrzymania systemów
Pozostałe sieci wewnętrzne	Wszystkie	Blokowane	Wyjątki definiowane na wniosek

Ruch z sieci Internet			
Cel	**Rodzaj połączenia**	**Akcja**	**Uwagi**
Sieci jednostek LP (sieci LAN)	Wszystkie	Blokowane	
Sieci DMZ centralne	Usługi dostępne z sieci Internet	Filtrowane	Inspekcja ruchu szyfrowanego
Sieci MGMT	Wszystkie	Blokowane	
Sieci Intranet	Wszystkie	Blokowane	
Pozostałe sieci wewnętrzne	Wszystkie	Blokowane	

Zasady inspekcji ruchu szyfrowanego

Projekt techniczny

do Załącznika nr 2 do Zarządzenia nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe zmienionego Zarządzeniem nr 12 z dnia 3 lutego 2022 r.

Metryka Dokumentu

Data	Autor	Wersja	Opis zmian
2022-02-14	EI.C	1.0	Pierwsza wersja dokumentu

Paweł Jacek Pogoda

Elektronicznie podpisany przez Paweł Jacek Pogoda
Data: 2022.03.14 11:27:19 +01'00'

I. Terminy użyte w tekście

Terminy użyte w treści mają następujące znaczenie:

1. **Lasy Państwowe, LP** – Państwowe Gospodarstwo Leśne Lasy Państwowe.
2. **SILP** – System Informatyczny Lasów Państwowych, zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
3. **Sieć LP** – wszystkie sieci transmisji danych będące własnością bądź zarządzane przez LP.
4. **Publiczne zasoby SILP (DMZ)** – Zbiór elementów SILP dostępnych publicznie z sieci Internet. Zasoby umieszczone są w dedykowanym i wydzielonym fragmencie sieci, odseparowanym technicznie od sieci wewnętrznej LP.
5. **ZCI** – Zespół w WI DGLP do spraw Cyberbezpieczeństwa Informatycznego, odpowiedzialna za nadzór nad bezpieczeństwem SILP.
6. **Administrator SILP** – pracownicy WZI lub osoby odpowiedzialne za zasoby SILP we własnej jednostce.
7. **Użytkownik SILP** - pracownik Lasów Państwowych w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonujących prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.

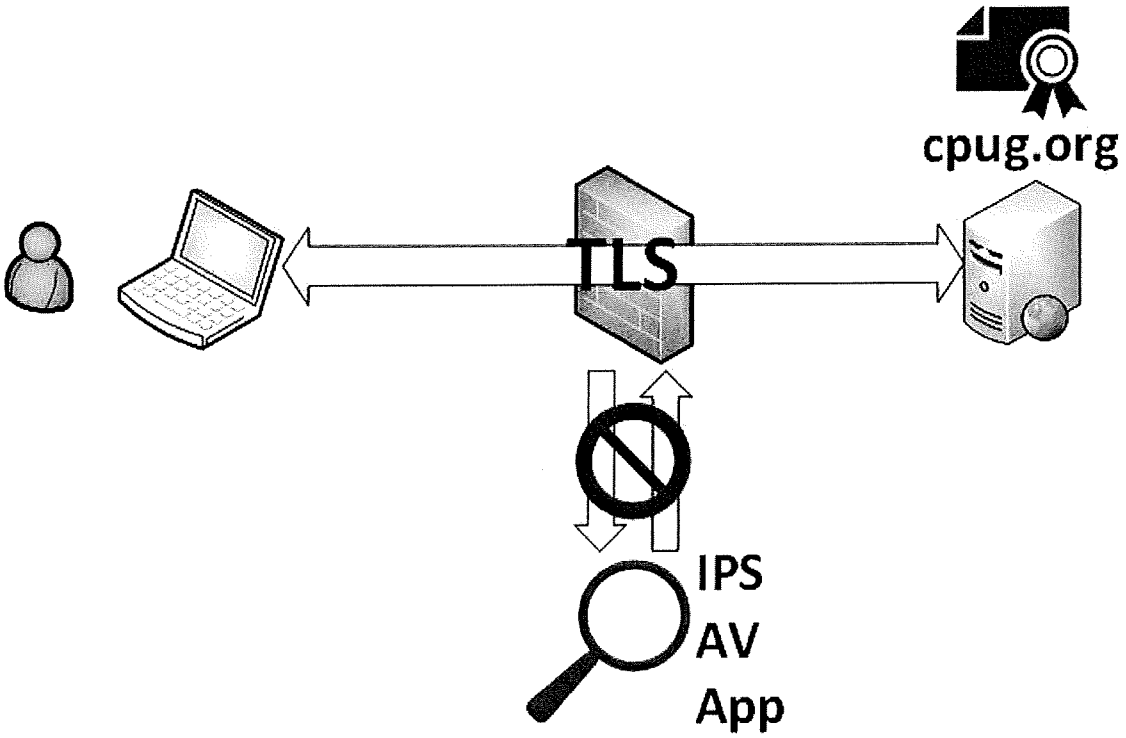
II. Założenia

1. Cel wprowadzenia inspekcji ruchu szyfrowanego

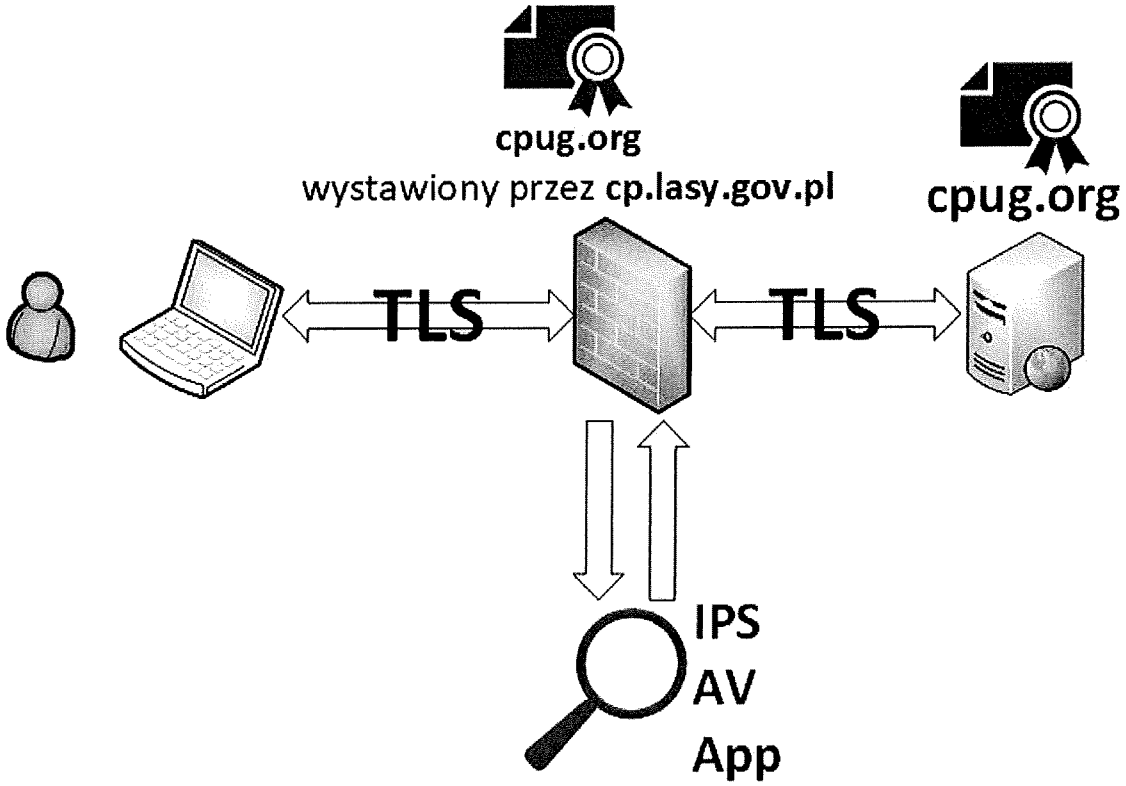
   Inspekcja ma na celu eliminację zagrożeń dla bezpieczeństwa SILP, poprzez identyfikację połączeń mogących skutkować infekcją systemów oraz połączeń inicjowanych przez złośliwe oprogramowanie. Przeważająca część ruchu sieciowego pomiędzy zasobami SILP a siecią Internet to ruch szyfrowany. Ruch taki jest szyfrowany w komunikacji pomiędzy klientem a serwerem, co uniemożliwia wykrywanie zagrożeń przez pośredniczące systemy zabezpieczeń. Z tego powodu znaczna część ruchu związanego z zagrożeniami cyberbezpieczeństwa ukrywana jest w transmisjach szyfrowanych.

2. Charakterystyka działania inspekcji HTTPS

Ruch HTTPS bez inspekcji (szyfrowanie odbywa się bezpośrednio pomiędzy klientem i serwerem docelowym):



Inspekcja ruchu HTTPS (szyfrowanie odbywa się pomiędzy klientem i modułem zabezpieczeń oraz modułem zabezpieczeń i serwerem docelowym):



Zapewnienie bezpieczeństwa i poufności:

- połączenie „klient – moduł zabezpieczeń" szyfrowane jest z użyciem certyfikatu poświadczonego przez Urzędu Certyfikacji Lasów Państwowych,
- dane poddawane są inspekcji IPS, AV, Application Control, Anty-Bot itp.
- dane poddawane inspekcji nie opuszczają modułu zabezpieczeń,
- dane typu użytkownik/hasło nie trafiają do żadnych logów modułu zabezpieczeń,
- bezpieczeństwo opiera się na zaufaniu do dostawcy rozwiązania analogicznie jak w przypadku oprogramowania np. antywirusowego, które to posiada dużo większy dostęp do danych użytkownika.

III. Zasady i implementacja inspekcji w Sieci LP

1. Konfiguracja dla stacji roboczych

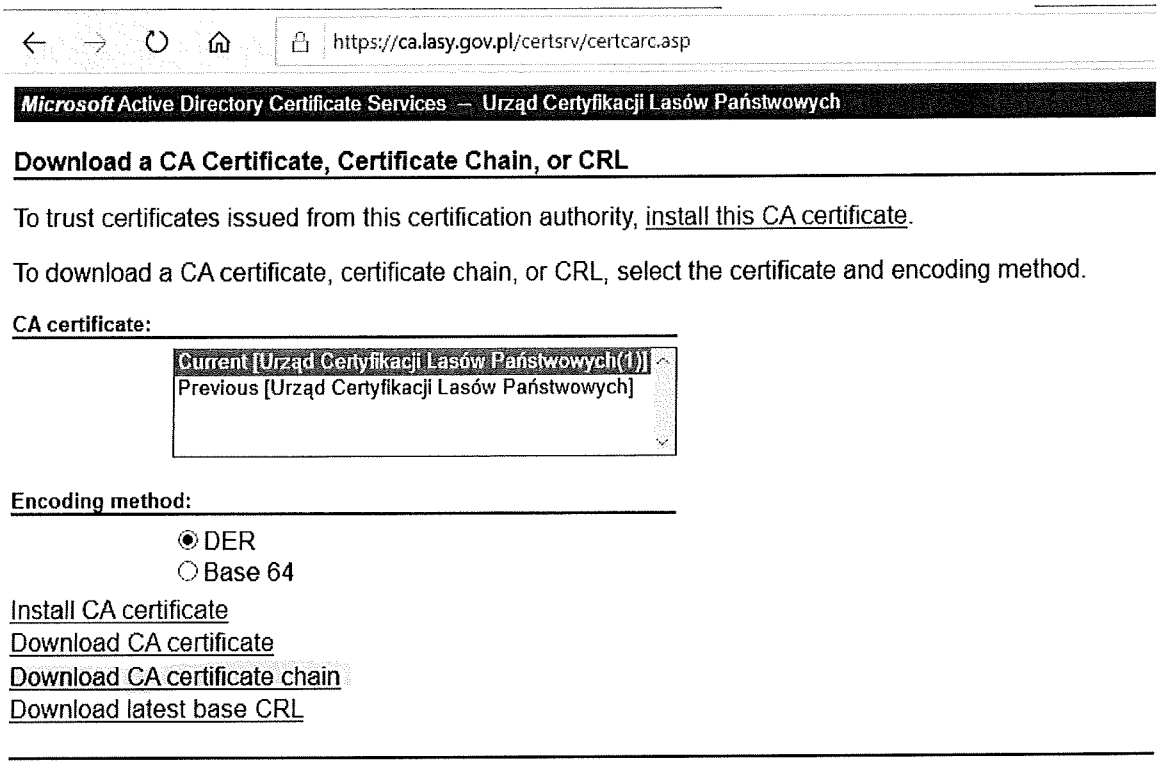
W celu zapewnienia bezproblemowego działania inspekcji HTTPS niezbędna jest odpowiednia konfiguracja stacji roboczych użytkowników SILP.

W przypadku stacji roboczych dodanych do domeny LP magazyn certyfikatów systemu Windows posiada łańcuch certyfikatów Urzędu Certyfikacji Lasów Państwowych dodany jako zaufany poprzez GPO. W takim przypadku przeglądarki internetowe korzystające z magazynu systemowego (np. Edge, Internet Explorer, Firefox, Chrome) nie wymagają konfiguracji.

W innych przypadkach wymagane jest dodanie łańcucha certyfikatów (Urzędu Certyfikacji Lasów Państwowych oraz Głównego Urzędu Certyfikacji Lasów Państwowych) do zaufanych w konfiguracji przeglądarek, z których korzysta użytkownik.

Łańcuch certyfikatów (obydwa wyżej wymienione) można pobrać ze strony:

https://ca.lasy.gov.pl/certsrv/certcarc.asp



wybierając opcję „Download CA certificate chain". Certyfikaty należy dodać jako zaufane w przeglądarce internetowej.

2. Wykluczenia z inspekcji HTTPS (tzw. „biała lista")

Nie podlegają inspekcji:

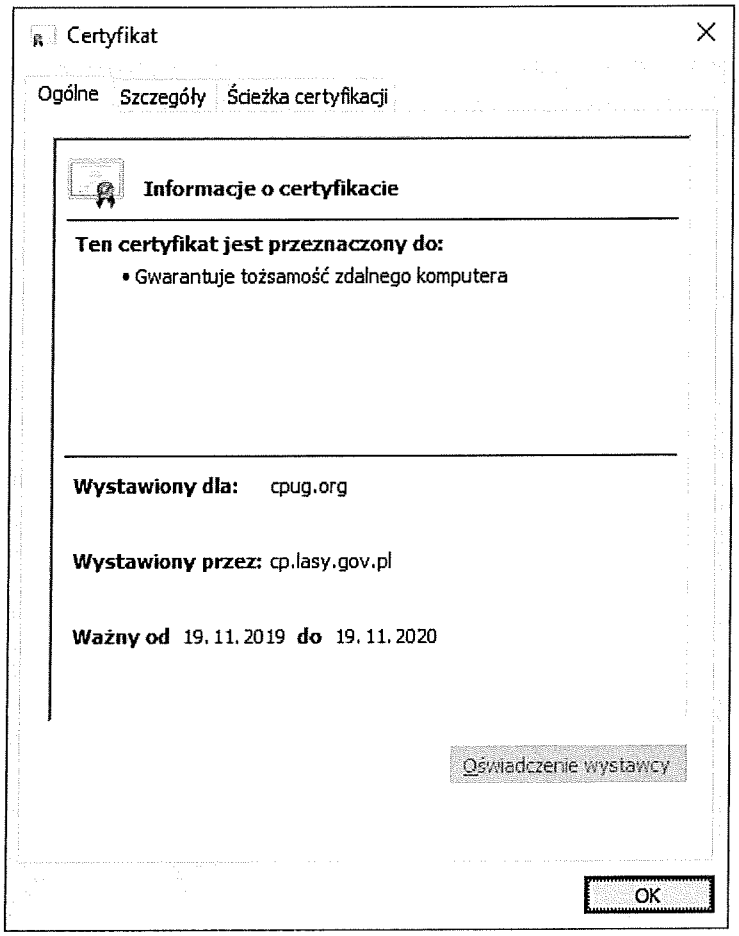
- strony z kategorii: Finanse (Financial Services), Zdrowie (Health), Wyszukiwarki (Search Engines) oraz Portale Społecznościowe (Social Media), lista dostarczana jest przez producenta oprogramowania, weryfikację kategorii dla konkretnego przypadku można sprawdzić w serwisie producenta:
  https://urlcat.checkpoint.com/
  (serwis wymaga rejestracji, konto użytkownika jest darmowe, konta powinny być

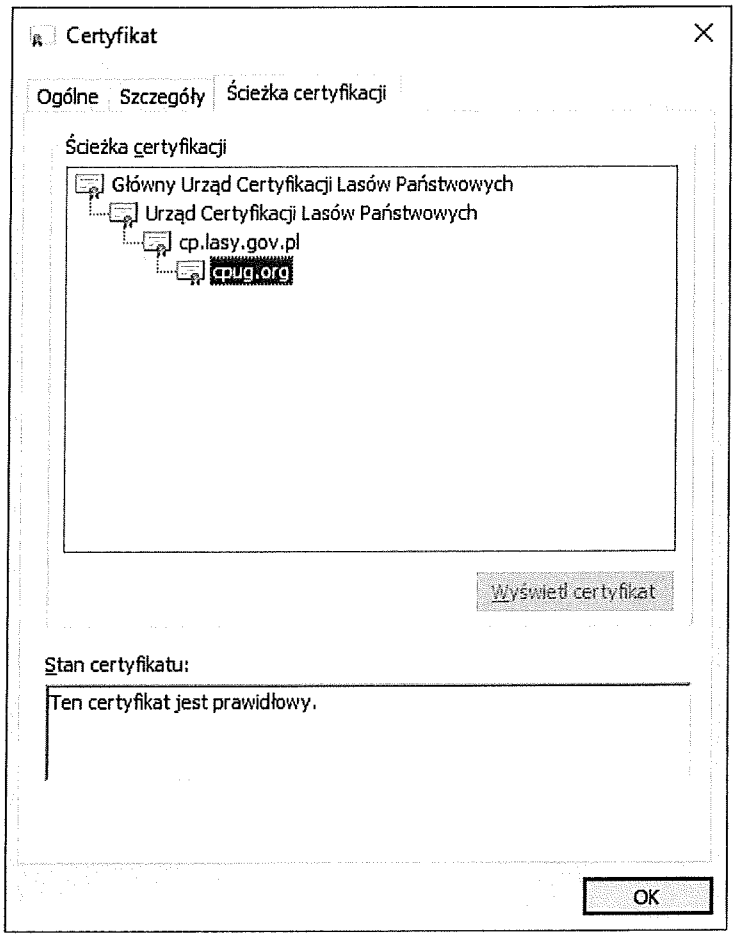
zakładane dla służb informatycznych dyrekcji regionalnych oraz zakładów LP według potrzeb),

- lista stron i domen z pliku: **\\ad.lasy.gov.pl\G0000\Programy\CHECKPOINT\Inspekcja HTTPS\Wykluczenia - Lista adresów i domen.xlsx**
- wnioski o dodatkowe wykluczenia mogą być zgłaszane przez Kierownika/Naczelnika służb informatycznych dyrekcji regionalnych (w przypadku zakładów LP o zasięgu krajowym przez osobę wyznaczoną przez kierownika/dyrektora zakładu) w formie wiadomości e-mail na adres ei.c@lasy.gov.pl, Temat: „Wykluczenia inspekcji HTTPS". Wiadomość powinna być podpisana certyfikatem korporacyjnym LP,
- wnioski będą podlegały analizie przez komórkę ds. Cyberbezpieczeństwa a po stwierdzeniu braku przeciwwskazań będą dodawane do wykluczeń.

3. Identyfikacja

W celu sprawdzenia czy inspekcja jest aktywna należy wyświetlić informacje o certyfikacie strony:





W powyższym przypadku inspekcja dla strony cpug.org jest włączona. Jeżeli wyświetlony certyfikat będzie oryginalnym certyfikatem kwalifikowanym oznaczać to będzie, że inspekcja dla takiej strony nie jest włączona. Dodatkowo jeżeli stacja użytkownika nie będzie prawidłowo skonfigurowana to przeglądarka internetowa wyświetli ostrzeżenie, że certyfikat strony jest nieprawidłowy.

4. Konfiguracja dla Publicznych zasobów SILP w strefie DMZ

a) W celu lepszego przeciwdziałania zagrożeniom dla Publicznych zasobów SILP udostępniających usługi w sieci Internet, została uruchomiona inspekcja ruchu szyfrowanego kierowanego do tych serwisów.
b) System prowadzący inspekcję ruchu terminuje szyfrowane połączenia, które są inicjowane z sieci Internet do systemów SILP w sieci DMZ. W tym celu uwierzytelnia się jako serwer jego certyfikatem i prowadzi dalszą komunikację z klientem, wykonując inspekcję jej treści. Warunkiem koniecznym do prowadzenia takiej inspekcji, jest przekazanie do ZCI certyfikatów SSL (wraz z powiązanymi kluczami prywatnymi) wystawionych dla serwisów udostępniających usługi w publicznej sieci Internet. Przed przekazaniem klucza prywatnego, należy bezwzględnie ustalić z ZCI bezpieczny kanał wymiany informacji.
c) W uzasadnionych przypadkach komunikacja może zostać wykluczona z prowadzenia inspekcji ruchu szyfrowanego. Wnioski o wykluczenie mogą być zgłaszane przez

właściwe WI RDLP (lub w przypadku zakładów LP o zasięgu krajowym przez osobę wyznaczoną przez kierownika jednostki) w formie wiadomości e-mail na adres ei.c@lasy.gov.pl, Temat: „Wykluczenia inspekcji HTTPS - DMZ". Wiadomość powinna być podpisana certyfikatem korporacyjnym LP. Wnioski będą podlegały analizie przez komórkę ds. Cyberbezpieczeństwa a po stwierdzeniu braku przeciwwskazań będą dodawane do wykluczeń.