**Załącznik Nr 2A**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zadanie nr 1 - Rozszerzenie funkcjonalności dotychczas użytkowanego oprogramowania Eset Endpoint Antywirus.**

1. **Okres obowiązywania nowej licencji 60 m-cy**
2. **Ilość licencji – 220.**
3. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
4. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
5. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
7. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
8. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
9. Rozwiązanie musi wspierać zarządzanie urządzeniami z systemem iOS i Android.
10. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
11. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
12. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
13. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
14. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
15. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
16. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
17. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
18. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

**II. Ochrona stacji roboczych**

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
11. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
12. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
13. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
14. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
15. Moduł HIPS musi posiadać możliwość pracy w jednym z poniższych trybów:
16. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
17. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
18. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
19. tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
20. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
21. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
22. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
23. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
24. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
25. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
26. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
27. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
28. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
29. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
30. Rozwiązanie musi posiadać ochronę antyspamową dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
31. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
32. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
33. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
34. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
35. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
36. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
37. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
38. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**III. Ochrona serwera**

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7 i 8, CentOS 7 i 8, Ubuntu Server 16.04 LTS i nowsze, Debian 9, Debian 10, SUSE Linux Enterprise Server (SLES) 12, Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

**Dodatkowe wymagania dla ochrony serwerów Windows:**

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

**Dodatkowe wymagania dla ochrony serwerów Linux:**

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

**IV. Szyfrowanie**

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**V. Endpoint Detection and Response**

1. Rozwiązanie musi posiadać moduł EDR dla systemów Windows oraz MacOS współpracujący z systemem do ochrony stacji roboczych tego samego producenta.
2. Rozwiązanie musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
3. Rozwiązanie musi posiadać serwer administracyjny z możliwością wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
4. Rozwiązanie musi posiadać serwer administracyjny z możliwością wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Rozwiązanie musi zapewniać wykluczenia dotyczące procesu lub procesu „rodzica”.
6. Rozwiązanie musi umożliwiać utworzenie wykluczenia automatycznie rozwiązujące alarmy, pasujące do utworzonego wykluczenia.
7. Rozwiązanie musi zapewniać kryteria wykluczeń konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Rozwiązanie musi umożliwić administratorowi weryfikację uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
9. Rozwiązanie musi umożliwiać administratorowi, w ramach plików wykonywalnych oraz plików DLL, możliwość oznaczenia ich jako bezpieczne, pobrania do analizy oraz ich zablokowania.
10. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.
11. Rozwiązanie musi posiadać konsolę administracyjną z możliwością audytowania innych administratorów konsoli.
12. Rozwiązanie musi posiadać konsolę administracyjną z możliwością połączenia się do stacji roboczej i wykonywania poleceń powershell.

**VI. Ochrona urządzeń mobilnych opartych o system Android**

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
6. usunięcie zawartości urządzenia,
7. przywrócenie urządzenie do ustawień fabrycznych,
8. zablokowania urządzenia,
9. uruchomienie sygnału dźwiękowego,
10. lokalizację GPS.
11. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
12. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
13. nazwę aplikacji,
14. nazwę pakietu,
15. kategorię sklepu Google Play,
16. uprawnienia aplikacji,
17. pochodzenie aplikacji z nieznanego źródła.

W ramach wdrożenia rozwiązanie zostanie zainstalowane oraz skonfigurowane w środowisku Zamawiającego a personel zostanie przeszkolony z jego obsługi.

**Zadanie nr 2 - Dostarczenie systemu typu PAM umożliwiającego zarządzanie oraz kontrolę nad dostępem uprzywilejowanym do środowiska IT Zamawiającego.**

## **I. Ogólne - architektura**

1. System PAM musi być rozwiązaniem bezagentowym tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy bez potrzeby instalacji oprogramowania (agenta) na systemie, do którego będzie nawiązywana sesja, umożliwiającym uwierzytelnianie wieloskładnikowe i obsługujące wiele platform i systemów operacyjnych. System PAM ma zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego m.in. routery, przełączniki, zapory sieciowe, aplikacje, bazy danych itp.
2. System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze VMware. Przez zamkniętą platformę rozumiemy wyspecjalizowane rozwiązanie, w ramach którego zainstalowana jest całość oprogramowania (system operacyjny, baza danych, aplikacja), realizująca wszystkie funkcjonalności systemu.
3. System na potrzeby realizacji swoich funkcji nie może wymagać zestawienia tunelu VPN pomiędzy siecią LAN organizacji, a komputerem zewnętrznego dostawcy. Nie może też wykorzystywać technologii chmurowej do nawiązania połączenia.

## **II. Licencjonowanie**

1. System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 5 administratorów, którzy będą korzystali z Systemu PAM, minimum dla następującej liczby funkcjonalności:
2. Ochrona kont uprzywilejowanych,
3. Ochrona kluczy SSH,
4. Zarządzanie i monitorowanie sesji uprzywilejowanych,
5. Rejestrowanie sesji uprzywilejowanych,
6. Raportowanie wykorzystania kont uprzywilejowanych
7. Dostarczone licencje na System PAM do ochrony kont uprzywilejowanych nie mogą mieć ograniczeń czasowych. Dostarczone licencje będą udzielone bezterminowo.
8. Dostarczone licencje na system PAM nie mogą w żaden sposób limitować ilości chronionych systemów docelowych.
9. **Wsparcie producenta na okres 36m-cy.**

## **III. Funkcjonalności**

1. System PAM musi zapewniać możliwość zarządzania (w szczególności):
2. Użytkownikami na systemach operacyjnych: Windows, Unix/Linux,
3. Kontami domenowymi: MS Active Directory,
4. Kontami lokalnymi: VMware ESX/ESXi,
5. Kontami na urządzeniach m.in.: Cisco, Aruba, Fortigate, IBM, Brocade,
6. Kontami baz danych: Microsoft SQL, Oracle, MySQL, PostgreSQL
7. Kontami do zarządzania i monitorowania serwerów: m.in. iLO, iDRAC,
8. Kontami w innych nie wymienionych systemach/urządzeniach do których dostęp odbywa się po protokołach: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
9. System PAM musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz użytkowników zewnętrznych, rejestrując obsługiwane sesje, oraz obsługując minimum następujące protokoły: SSH, RDP,VNC, TELNET, HTTP/HTTPS.
10. System PAM musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami:
11. przeglądarka internetowa,
12. klient RDP,
13. klient protokołu SSH/Telnet (np. putty)
14. System PAM musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, Tacacs Active Directory, OpenID.
15. System PAM powinien zapewniać możliwość dwuskładnikowego uwierzytelniania.
16. System PAM musi obsługiwać monitorowanie i ochronę nawet kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego, do różnych systemów poprzez wiele lub jedno konto uprzywilejowane.
17. System PAM musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd do haseł uprzywilejowanych.
18. System PAM musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
19. System PAM musi posiadać log dla wszystkich zdarzeń systemowych.
20. System PAM musi umożliwiać wskazanie kont użytkowników, które realizowały logowanie do stacji/serwera.
21. System PAM musi umożliwiać raportowanie wszystkich zmian wprowadzonych przez administratorów.
22. System PAM musi umożliwiać raportowanie wszystkich logowań do systemu.
23. System PAM musi umożliwiać raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego.
24. Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.
25. System PAM musi umożliwiać ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
26. System PAM musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką m.in.:
27. umożliwiać zdefiniowanie wymagań na: długość hasła, znaki w haśle (małe i duże litery, cyfry, znaki specjalne),
28. generować automatycznie hasła kont systemów docelowych w sposób pseudo losowy,
29. generować unikalne hasła dla konta systemów docelowych,
30. wymuszać automatyczną zmianę hasła po jego podglądzie
31. System PAM musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.
32. System PAM musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym (audyt poleceń).
33. Audyt poleceń musi umożliwiać podjęcie co najmniej akcji, zablokuj polecenie i rozłącz sesję po wykryciu audytowanego polecenia a także automatyczne umieszczenie na liście blokowanych użytkowników użytkownika, który próbował wykonać blokowane polecenie.
34. System PAM musi umożliwiać nagrywanie sesji wraz z podglądem sesji aktywnej oraz możliwość jej przerwania.
35. Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego.
36. System PAM musi rejestrować znaki wprowadzone z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem występowania wskazanych słów kluczowych.
37. System PAM musi umożliwiać odtworzenie zarejestrowanych nagrań sesji.
38. Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, iż zaoferowany produkt posiada wsparcie producenta na terenie Polski.
39. System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności:
40. zarządzać kontami uprzywilejowanymi w ramach organizacji,
41. monitorować wykorzystanie kont uprzywilejowanych,
42. nagrywać i archiwizować sesje zdalne,
43. gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów oraz nowych usług,
44. System PAM musi umożliwiać personalizację wyglądu aplikacji co najmniej po przez umieszczenie logo zamawiającego w głównym oknie aplikacji.

W ramach wdrożenia rozwiązanie zostanie zainstalowane oraz skonfigurowane w środowisku zamawiającego a personel zostanie przeszkolony z jego obsługi.

**Zadanie nr 3 - Dostarczenie rozwiązania typu SIEM umożliwiającego centralne zarządzanie logami pochodzącymi z różnych źródeł, analitykę oraz korelację między nimi.**

**Wsparcie producenta na okres 12 m-cy.**

# **I. Funkcjonalności**

1. System musi być oparty o nowoczesną nierelacyjną bazę danych typu noSQL
2. System musi pracować w oparciu o architekturę Linux.
3. System musi mieć możliwość centralnego zbierania i zarządzania logami
4. System działać w trybie zbliżonym do rzeczywistego
5. System musi mieć możliwość działania jako niezależne instancje zainstalowane w oddziałach Zamawiającego wraz z możliwość centralnego dostępu.
6. Instancje systemu muszą mieć możliwość działania w przypadku odłączenia scentralizowanego dostępu.
7. System musi zapewniać efektywną obsługę co najmniej 1000 EPS lub 20  GB danych dziennie
8. System musi zapewniać retencję danych w okresie minimum 365  dni.
9. Oferowana licencja nie może ograniczać ilości zarejestrowanych lub jednoczesnych użytkowników systemu.
10. System musi umożliwiać rozbudowę bez potrzeby wyłączania lub restartu środowiska.
11. Architektura rozwiązania musi umożliwiać rozdzielenie ról systemu pomiędzy osobne komponenty (serwery/maszyny wirtualne). Należy przewidzieć rozdzielenie przynajmniej 3 typów ról: Agregacja, Prezentacja, Retencja.
12. Dołączenie nowego węzła przetwarzania, prezentacji lub przechowywania pozwalającego na skalowanie wydajności. Rozszerzenie takie powinno odbywać się bez konieczności restartu działającego systemu.
13. System musi zapewniać wysoką dostępność na poziomie Agregacji i Retencji
14. System musi zapewniać buforowanie agregowanych danych na okres minimum 2 dni w przypadku awarii któregokolwiek z komponentów oraz ich uzupełnienie w po przywróceniu pełnej sprawności systemu .
15. Komunikacja pomiędzy wszystkim komponentami musi być szyfrowana z wykorzystaniem protokołu TLS w wersji minimum 1.2.
16. Szyfrowanie komunikacji z przeglądarką internetową użytkownika musi wykorzystywać protokołów TLS w wersji minimum 1.3.
17. System musi posiadać interfejs graficzny dostępny z poziomu przeglądarki internetowej min. Firefox, Chrome, Internet Explorer.
18. Interfejs musi posiadać angielską lub polską wersję językową.
19. System powinien być tworzony zgodnie z zaleceniami standardu OWASP Testing Guide, a w szczególności OWASP - TOP 10 (Open Web Application Security Project). Projektowany System powinna spełniać wymagania standardu OWASP ASVS (Application Security Verification Standard) w wersji 4.0 co najmniej na poziomie pierwszym (L1).
20. Dostęp do systemu musi być zabezpieczany hasłem lub certyfikatem.
21. Autoryzacja do systemu musi być zintegrowana z: Microsoft AD, LDAP, Radius
22. Hasła typu Windows AD bind muszą być przechowywane w postaci zaszyfrowanej.
23. System musi wspierać mechanizm logowania typu Single Sign On.
24. System musi umożliwiać zarządzanie czasem automatycznego wygasania sesji użytkowników.
25. System musi posiadać dedykowany widok zarządzania użytkownikami i rolami.
26. System powinien umożliwiać zarządzenie uprawnieniami do modyfikacji wytworzonych w systemie obiektów tj. wyszukiwania, wizualizacje, dashboardy. Dla utworzonych ról musi istnieć możliwość przypisania wspomnianych obiektów w podziale na dostęp typu „read only” oraz „pełny”. Obiekty, do których grupa nie ma dostępu, nie mogą być widoczne dla użytkownika.
27. System musi zapewniać pełen audyt aktywności jego użytkowników, w tym: udanych/nieudanych logowaniach, pełnej historię operacji, realizowanych zapytań, zmian uprawnień.
28. System musi umożliwiać ręczne ustawianie poziomu szczegółowości gromadzonych danych audytowych.
29. System musi posiadać autoryzowane przez producenta narzędzie/moduł do kontroli wydajności dostarczonego systemu. Wsparcie producenta musi obejmować zakresem również to narzędzie.
30. System musi zapewniać mechanizmy umożliwiające pracę w trybie multitenant.
31. System musi pozwalać na tworzenie parserów z poziomu GUI
32. System musi zapewniać budowę modeli prognostycznych w oparciu o metody matematyczne i statystyczne tzw. Machine Learning.
33. System musi zapewniać wizualizację danych w postaci, oryginalnych logów, list, wykresów i diagramów.
34. System musi umożliwiać graficzną wizualizację zidentyfikowanych połączeń sieciowych pomiędzy adresami IP.
35. Wizualizacja danych powinna być również możliwa dla wartości tekstowych jak i liczbowych przekazywanych w logach.
36. System musi umożliwiać funkcjonalność eksportu danych o Zdarzeniach i Incydentach do formatu CSV i HTML m.in. w celu analizy wyników działania reguł korelacyjnych.
37. System musi zapewniać parsowanie spływających do niego wiadomości w formatach:
38. Syslog,
39. WEF,
40. Flat file,
41. Event log,
42. WMI,
43. SNMP trap,
44. XML,
45. JSON,
46. JDBC/ODBC,
47. CSV,
48. Email,

Jak również musi pozwalać na implementację innych formatów w przypadku zaistnienia takiej potrzeby ze strony Zamawiającego.

1. System musi zbierać logi z rozwiązań chmurowych opartych minimum o AWS oraz Microsoft Azure.
2. System musi umożliwiać prezentację logu o zdarzeniu w interfejsie użytkownika w takiej formie w jakiej ten log został przesłany do Systemu tj. wyświetlenie logu w postaci surowej (RAW) przed parsowaniem.
3. System musi do przyjmowania zdarzeń wykorzystywać zarówno mechanizmy agentowe jak i bezagentowe.
4. System musi umożliwiać definiowanie parserów dla niestandardowych formatów logów w oparciu o składnię wyrażeń regularnych oraz formatów wymiany danych dla wszystkich obsługiwanych formatów.
5. Interfejs musi umożliwić parsowanie warunkowe na podstawie dopasowania wartości pól. Po dopasowaniu wzorca dalsze parsowanie powinno być konfigurowalne w celu wyboru optymalnej metody parsowania, np.: REGEX, JSON, XML oraz umożliwiać zastosowanie innego parsera.
6. System musi posiadać predefiniowany zestaw parserów zdarzeń.
7. System musi mieć funkcjonalność Bad IP Reputation tj. porównywania adresów IP z bazami reputacyjnymi dostarczonymi przez producenta
8. System musi wspierać geolokalizację zdarzeń na bazie adresów IP.
9. System musi umożliwiać normalizowanie wiadomości po sparsowanych polach, np. dzięki zmianie wartości tych pól oraz wzbogacaniu tych danych o dodatkowe pola bazując na całych wartościach lub wzorcach wyszukiwania.
10. System musi umożliwiać przeszukiwanie Danych Wejściowych z uwzględnieniem filtracji po sparsowanych polach.
11. Proces parsowania musi umożliwiać wzbogacanie treści obieranych Wiadomości poprzez matematyczne operacje wykonywane na innych polach.
12. Proces parsowania musi umożliwiać anonimizację Danych Wejściowych celem ukrycia fragmentów informacji, których składowanie nie jest konieczne lub narusza wewnętrzny procedury bezpieczeństwa.
13. System powinien pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinijkowych
14. System powinien pozwalać na rozpoznanie formatów czasu i daty oraz normalizowanie ich do jednego wspólnego formatu.
15. Incydent, który powstał w wyniku korelacji, musi dać się wyszukiwać korzystając ze standardowego dostępnego w systemie mechanizmu wyszukiwania. System musi umożliwiać budowanie na jego podstawie kolejnych reguł korelacyjnych lub generowania alarmów.
16. System musi posiadać funkcjonalność korelacji danych w czasie rzeczywistym.
17. System musi umożliwiać tworzenie nowych reguł korelacyjnych oraz modyfikowanie istniejących.
18. System musi umożliwiać tworzenie własnych reguł korelacyjnych na bazie reguł odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie, w tym:
19. Wykrycia dowolnej treści w logach,
20. Wykrycia wystąpienia wartości pola na wybranej liście,
21. Wykrycia niewystępowania wartości pola na wybranej liście,
22. Wykrycia zmiany jednego z kilku pól,
23. Wykrycia zdarzeń występujących z zadaną częstotliwością,
24. Wykrycia zdarzeń, których liczba zmienia się w wskazany sposób względem czasu poprzedniego,
25. Wykrycia zaniku Wiadomości,
26. Wykrycia nowej wartości pola w zadanym okresie czasu,
27. Wykrycia incydentu będącego pochodną zdarzeń występujących w określonej kolejności
28. System musi pozwalać na tworzenie własnych algorytmów ewaluacji Incydentów.
29. Reguły korelacji oraz algorytmy ewaluacji incydentów muszą być możliwe do dodawania lub modyfikacji z poziomów zarówno GUI jak i API.
30. System musi pozwolić na określenie okna czasowego oraz warunków dla zdarzeń, które mają zostać poddane regułom korelacyjnym.
31. System musi pozwalać na realizację zapytań obejmujących całą historię gromadzonych w nim danych
32. System musi umożliwić korelację Zdarzeń pochodzących z różnych źródeł informacji z anomaliami wykrywanymi m.in. w. Netflow oraz wykrytymi podatnościami zidentyfikowanymi przez skaner podatności
33. System musi zapewnić mechanizmy obsługi incydentów i wymiany informacji pomiędzy, operatorami systemu w tym przypisanie incydentu do operatora i zmiana jego statusu.
34. System musi posiadać funkcjonalność tworzenia scenariuszy obsługi incydentu tzw. Playbook
35. System musi automatycznie podpowiadać odpowiednie scenariusze obsługi incydentów.
36. Scenariusze muszą mieć możliwość ich symulacji i weryfikacji, m.in. na przykładowym zasobie IT.
37. System musi pozwalać na tworzenie własnych scenariuszy obsługi oraz edycję istniejących.
38. Rozwiązanie musi posiadać funkcjonalność wysyłania powiadomień o Incydentach do innych systemów bądź zdefiniowanych użytkowników (co najmniej: powiadamianie email, opcjonalnie SMS, czat).
39. System musi umożliwiać testowanie reguł korelacyjnych i alertów na etapie ich tworzenia. Wynik testu nie może tworzyć wpisu o sytuacji alarmowej i ewentualnego incydentu.
40. System musi pozwalać na zautomatyzowane szacowanie ryzyka dla dowolnych kryteriów w ramach przetwarzanych zdarzeń. W rozwiązaniu musi być obecna funkcjonalność. kategoryzacji obiektów (adresy IP, loginy i inne pola), dla których mechanizm szacowania ryzyka uwzględni podane wagi.
41. System umożliwia konfiguracje automatycznych akcji, które są wykonywane na monitorowanych systemach w przypadku detekcji zagrożenia wskazanego w regule
42. Tworzone incydenty będące wynikiem pracy reguł bezpieczeństwa muszą posiadać wbudowany poziom istotności. Musi istnieć możliwość modyfikacji poziomu istotności dla każdej reguły.
43. System musi zapewniać funkcjonalność generowania raportów z dowolnych danych gromadzonych w systemie.
44. Raporty muszą być generowane ręcznie oraz automatycznie według zdefiniowanego harmonogramu.
45. System musi generować raporty do formatów minimum PDF oraz JPEG z jednoczesną możliwością opatrywania dokumentu logo Zamawiającego oraz komentarzami.
46. System musi zapewniać wbudowany mechanizm archiwizacji danych w postaci plików płaskich oraz ich zarządzaniem z poziomu konsoli użytkownika.
47. Mechanizm archiwizacji musi posiadać funkcjonalność przesyłania danych online do archiwum według zadanych kryteriów w sposób automatyczny lub ręczny.
48. Mechanizm archiwizacji musi umożliwiać pozwalać na przywracanie danych do systemu celem analizy online.
49. Mechanizm archiwizacji musi zapewniać funkcjonalność wyszukiwania w spakowanych danych bez potrzeby ich wcześniejszego rozpakowania.
50. System musi umożliwiać zakup licencji wieczystych wraz ze wsparciem community producenta na okres 1 roku.
51. Oferowana licencja nie może ograniczać ilości urządzeń będących źródłem logów.
52. System musi umożliwiać czasowe przyjęcie zwiększonej ilości danych o minimum 30% bez potrzeby zwiększania zasobów sprzętowych lub licencyjnych.
53. Wsparcie producenta musi być realizowane w języku polskim przez dedykowanych inżynierów.
54. Support producenta musi być świadczony w formule minimum 8/5.
55. Wsparcie nie może być limitowane ilością zgłoszeń i musi być realizowane zdalnie oraz w siedzibie Zamawiającego.
56. Musi istnieć możliwość automatycznego importu informacji IoC (ang. Indicator Of Compromise), a następnie automatyczne przeszukiwanie wśród zgromadzonych zdarzeń w wyznaczonym czasie.
57. System musi posiadać natywną integrację z bazą MISP min. Adresy IP, hash zainfekowanych plików, adresy domen, adresy URL.
58. System musi umożliwiać integrację z Mitre ATT@CK

W ramach wdrożenia rozwiązanie zostanie zainstalowane oraz skonfigurowane w środowisku zamawiającego a personel zostanie przeszkolony z jego obsługi.

**Zadanie nr 4** **- Dostarczenie oprogramowania umożliwiającego tworzenie kopii zapasowych wybranych komputerów.**

**Wsparcie producenta na okres 60 m-cy**

# **I. Ogólne**

1. Oprogramowanie może być dostarczane w dwóch scenariuszach cloud lub on-premise z opcja migracji w obie strony.
2. Istnieje możliwość migracji w obie strony pomiędzy środowiskiem on-premise oraz cloud.
3. Interfejs systemu dostępny jest w języku: polskim/angielskim
4. Oprogramowanie nie wymaga konkretnej platformy sprzętowej, nie jest profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych.
5. Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych opartych o systemy min centOS 7, Redhat 6, Windows Server 2019.
6. System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji.
7. Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju).

# **II. Wsparcie techniczne**

1. Pomoc techniczna w językach: polskim/angielskim
2. Materiały samopomocowe: polskim/angielskim

# **III. Zarządzanie**

1. Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli administracyjnej.
2. Zarządzanie całym systemem poprzez dashboardy.
3. Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego.
4. System posiada wbudowane predefiniowane zadania backupowe.
5. System umożliwia tworzenie zadań backupowych w oparciu o kalendarz.
6. Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem.
7. Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem.
8. Monitorowanie postępu działania zadania.
9. Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: Zadanie zostało zakończone pomyślnie, z ostrzeżeniami, z błędem, anulowane, nie zostało uruchomione.
10. System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego.
11. Możliwość zdefiniowania okna backupowego dla każdego z zadań
12. Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów
13. System pozwala na klonowanie planów kopii zapasowych
14. System umożliwia reset hasła administratora w przypadku jego utraty
15. Oprogramowanie umożliwia definiowanie retencji według schematów: GFS(Grandfather-Father-Son), FIFO(First-In, First-Out).
16. Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami.
17. Oprogramowanie umożliwia tworzenie grup urządzeń
18. System umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, takimi jak administrator systemu, administrator kopii, administrator odzyskiwania.

# **IV. Składowanie danych**

1. Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie.
2. System umożliwia składowanie danych:
3. Lokalnie (SMB, NFS, ISCSI, zasób S3);
4. W chmurze (Amazon Web Service, magazyn zgodny z S3, rozwiązanie dostarczone przez producenta)
5. System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji.
6. System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
7. System umożliwia replikacje danych między magazynami.

# **V. Odtwarzanie**

1. Odtwarzanie granularne pojedynczych plików z kopii obrazu dysku, pojedynczych wiadomości z kopii skrzynek Microsoft 365.
2. Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów Windows 7 oraz nowszych oraz Windows Server 2019 oraz nowszych.
3. Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
4. Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub nośnika USB.
5. Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.
6. Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK).
7. Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL).
8. Odtwarzanie zasobów plikowych z prawami dostępu.
9. Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows).
10. Odtwarzanie danych według harmonogramu.
11. Przywracanie danych z określonego urządzenia/użytkownika.
12. Przywracanie kopii z wybranego magazynu.
13. Przywracanie danych Microsoft 365:
14. do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku pst, mbox;
15. do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),
16. System posiada możliwość nieodwracalnego kasowania danych.

# **VI. Backup**

1. Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla:
2. Systemów operacyjnych: (Windows 7, Windows serwer 2019, Cent0S 7, Redhat 6, Debian 9 oraz nowszych;
3. Środowisk wirtualnych Hyper-V oraz Vmware 6.7 oraz nowszych;
4. Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla baz danych**:** MS SQL, MySQL, PostgreSQL, Firebird.
5. Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości 128, 192, 256 bit.
6. Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów ZStandard, LZ4.
7. Oprogramowanie umożliwia zarządzanie poziomem kompresji.
8. Wykonywanie kopii zapasowej otwartych plików (VSS).
9. System umożliwia uruchamianie skryptów przed i po backupie.
10. System umożliwia uruchamianie skryptów po wykonaniu migawki VSS.
11. System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów.
12. Backup jednego oraz wielu dysków/całego systemu operacyjnego (Windows) ze wsparciem dla partycji MBR oraz GPT.
13. Backup plikowy.
14. Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe.
15. Oprogramowanie umożliwia konsolidację wersji kopii zapasowych.
16. Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
17. Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego.
18. Oprogramowanie pozwala na backup zaszyfrowanych partycji.

# **VII. Licencjonowanie**

1. Sposób licencjonowania opiera się na:
2. Ilości serwerów/endpointów- dla fizycznych urządzeń;
3. Ilości fizycznych hostów - dla środowisk wirtualnych.
4. Licencje powinny pozwalać na zabezpieczenie 50 stacji roboczych w opcji dożywotniej.

**VIII. Wsparcie techniczne**

1. Świadczone jest w języku polskim, bezpośrednio przez producenta.
2. Zapewnia dostęp do aktualizacji oprogramowania.
3. Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
4. Obowiązuje przez okres **60 miesięcy.**

**Zadanie nr 5** - **Dostarczenie urządzenia typu NAS umożliwiającego przechowywanie kopii zapasowych.**

|  |  |  |
| --- | --- | --- |
| **L.p.** | **Wymagane minimalne parametry techniczne** | |
| 1 | Procesor | Procesor o taktowaniu nie mniejszym niż 1,7GHz |
| 2 | Procesor liczba rdzeni | Nie mniej niż 4 |
| 3 | Pamięć RAM | Nie mniej niż 4 GB ECC RAM (RDIMM) |
| 5 | Pamięć RAM - możliwość rozszerzenia | nie mniej niż do 16GB |
| 6 | Pamięć Flash | Nie mniej niż 512MB |
| 7 | Liczba zatok na dyski twarde | Minimum 8, minimalna ilość dysków 8 |
| 8 | Obsługiwane dyski twarde | 8x 3,5" SATA 6Gb/s |
| 9 | Parametry dysków | min 6TB 7200RPM, 256MB cache |
| 11 | Porty LAN | przynajmniej 2 x SFP+ 10GbE, 2 x 1GbE |
| 12 | Możliwość montażu kart rozszerzeń na PCI-E | Tak, minimum 1 port |
| 14 | Porty USB 3.0 | Minimum 2 |
| 15 | Przyciski | Reset, Zasilanie |
| 16 | Typ obudowy | RACK, 2U |
| 17 | Dopuszczalna temperatura pracy | od 0 do 40˚C |
| 18 | Wilgotność względna podczas pracy | 5-95% R.H. |
| 19 | Zasilanie | Redundantny zasilacz hot swap o mocy min. 250W każdy |
| 22 | Szyny montażowe | W zestawie |
| 23 | Obsługa sieci | TCP/IP (IPv4 IPv6),  10 Gigabit NIC z obsługą ramek Jumbo (LACP, Load Balance, Failover, Round Robin)  Protokoły: SMB2/SMB3, NFS v3/NFS v4, FTP, FTPS, TFTP, HTTP, HTTPS, SSH, iSCSI, SNMP, SMTP i SMSC  Przypisywanie usług do interfejsów |
| 24 | Zarządzanie zasilaniem | Wake on LAN Tryb Stand-By dla dysków wewnętrznych Automatyczne włączenie urządzenia po utracie zasilania Wsparcie dla UPS (USB, SNMP) |
| 25 | Zarządzanie prawami dostępu | Wsadowe tworzenie użytkowników  Import/Eksport użytkowników  Quota na użytkowników  Zarządzanie prawami dostępu do użytkowników dla SMB i FTP Wsparcie dla Microsoft Active Directory Klient LDAP |
| 26 | Zarządzenie urządzeniem | Webowy panel administracyjny (wielookienkowy i wielozadaniowy) SNMP (v2 i v3),  Monitor zasobów,  Klient Syslog  Kopia zapasowa ustawień,  Możliwość zarządzania przez CLI |
| 27 | Zarządzanie przestrzenią dyskową | Monitor wykorzystania zasobów,  Obsługa RAID 0, 1, 5, 50, 6, 60, 10, |
| 29 | ​iSCSI (IP SAN) | iSCSI target z obsługą multi-LUN na target (do 256 LUN),  mapowanie LUN,  Rozszerzanie pojemności LUN online,  Wsparcie dla SPC-3  Wsparcie dla MPIO i MC/S |
| 30 | Backup  i replikacja | Replikacja zdalna przez Rsync i RTRR  Harmonogram backupu |
| 38 | Zarządzanie prawami dostępu | Ograniczenie dostępnej pojemności dysku dla użytkownika  Importowanie listy użytkowników  Zarządzanie kontami użytkowników  Zarządzanie grupą użytkowników  Zarządzanie współdzieleniem w sieci  Tworzenie użytkowników za pomocą makr  Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL |
| 39 | Obsługa Windows AD | Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web  Obsługa uwierzytelniania NTLMv2, Funkcja serwera LDAP |
| 43 | Administracja systemu | Połączenia HTTP/HTTPS  Powiadamianie przez e-mail (uwierzytelnianie SMTP)  Powiadamianie przez SMS  Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze  SNMP (v2 & v3)  Obsługa UPS z zarządzaniem SNMP (USB)  Obsługa sieciowej jednostki UPS  Monitor zasobów  Kosz sieciowy dla CIFS/SMB oraz AFP  Monitor zasobów systemu w czasie rzeczywistym  Rejestr zdarzeń  System plików dziennika  Całkowity rejestr systemowy (poziom pliku)  Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line  Aktualizacja oprogramowania  Możliwość aktualizacji oprogramowania  Ustawienia: Backup, przywracania, resetowania systemu |
| 45 | Zabezpieczenia | Filtracja IP  Ochrona dostępu do sieci z automatycznym blokowaniem  Połączenie HTTPS  FTP z SSL/TLS (Explicit)  Obsługa SFTP (tylko admin)  Szyfrowanie AES 256-bit  Szyfrowana zdalna replikacja (Rsync poprzez SSH)  Import certyfikatu SSL  Powiadomienia o zdarzeniach za pośrednictwem Email i SMS |
| 48 | gwarancja | **60 m-cy** gwarancji NBD |
| 49 | Certyfikaty | Certyfikacja ISO/EIC 27001/2013 lub równoważny |

**Zadanie nr 6 - Rozbudowa poprzez dostarczenie i skonfigurowanie posiadanej przez Zamawiającego macierzy IBM FlashSystem 5000 o dodatkową półkę.**

1. Rozbudowa posiadanej macierzy IBM FlashSystem 5000 o dodatkową półkę wyposażoną w minimum min 10 dysków o pojemności 1.92TB SSD SAS każdy.
2. Macierz musi zostać zainstalowana i skonfigurowana w następujący sposób:
3. Montaż w szafie rack 42U;
4. Podłączenie do listew zasilających PDU;
5. Konfiguracja konsoli zarządzającej, konfiguracja RAID macierzy, wirtualnych dysków, hostów i grup hostów;
6. Wykonanie podłączenia sieciowego macierzy i serwerów zgodnie ze wskazówkami Zamawiającego;
7. Instalacja i konfiguracja zasobów macierzy zgodnie ze wskazówkami Zamawiającego.
8. **Okres gwarancji 36 m-cy** 9x5 NBD.

**Zadanie nr 7 - Rozszerzenie obecnie posiadanej usługi HEZO dla urządzeń Fortinet Zamawiającego.**

1. Ogólne
2. okno wsparcia 24x7;
3. czas reakcji – 1h;
4. czas dostawy sprzętu – 8h;
5. język wsparcia – polski;
6. obsługiwanie zgłoszeń telefonicznych oraz zgłoszonych przez dedykowany portal;
7. pomoc w rozwiązywaniu problemów;
8. zdalne wdrożenie/rekonfiguracja urządzeń;
9. pomoc techniczna/doradztwo w zakresie konfiguracji;
10. konsultacje architekta bezpieczeństwa;
11. okresowe przeglądy konfiguracji;
12. okresowe przeglądy logów;
13. okresowe wsparcie przy aktualizacji oprogramowania
14. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.
15. Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
16. Dedykowana strona internetowa, mail oraz telefon w języku polskim – wsparcie 24x7.
17. **Rozszerzenie obecnie posiadanej usługi na okres 36 m-cy.**

**Zadanie nr 8 - Dostarczenie usługi polegającej na oddaniu do dyspozycji Zamawiającego zasobów informatycznych, powierzchni dyskowej w postaci chmury IaaS udostępnionej za pomocą protokołu S3.**

1. **Wymagania prawne i normatywy warunkujące przetwarzanie danych**
2. Ustawa o Ochronie Danych Osobowych z 10 maja 2018 (tj. Dz. U. z 2019 r., poz. 1781) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (Regulacji Ochrony Danych Osobowych);
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
4. Posiadanie Certyfikatu PL-EN ISO:27001;
5. Posiadanie Certyfikatu PL-EN ISO:27017;
6. Posiadanie Certyfikatu PL-EN ISO:22301;
7. Posiadanie Certyfikatu TIER III Uptime Institute (lub zgodność z wytycznymi dla TIER III Uptime Institute)
8. **Wymagania dotyczące bezpieczeństwa fizycznego**
9. Data Center zlokalizowane jest co najmniej w wydzielonej części budynku, chronionej przez system alarmowy i system telewizji przemysłowej budynkowej (nadzorowany);
10. Dostęp do pomieszczeń tylko dla upoważnionych osób, rejestracja wejść/wyjść przez system kontroli dostępu z jego rejestracją, w oparciu o co najmniej karty magnetyczne lub kody PIN;
11. Wydzielone fizycznie strefy Data Center zamykane drzwiami o odporności ogniowej 60 minut, wyposażone w mechanizmy samozamykające.
12. **Wymagania dotyczące bezpieczeństwa energetycznego**
13. Zasilanie energetyczne z dwóch niezależnych źródeł oraz dodatkowo awaryjne zasilanie z agregatów prądotwórczych;
14. System samoczynnego załączenia rezerwy, monitorujący parametry zasilania, przełączający na właściwe w przypadku awarii;
15. Ciągłość działania urządzeń IT zabezpieczona przez zestawy UPS-ów, pracujących w układzie n+1 lub 2n;
16. Dedykowane rozdzielnie energetyczne dla każdego z torów zasilania.
17. **Wymagania dotyczące klimatyzacji i systemów przeciwpożarowych**
18. System przeciwpożarowy monitorowany przez Państwową Straż Pożarną;
19. Stałe urządzenia gaśnicze gaszące gazem obojętnym, oddzielne dla każdej serwerowni lub równoważne rozwiązania;
20. Ściany i drzwi Data Center gwarantujące co najmniej 60 minutową odporność ogniową;
21. Mikroklimat w zakresie wilgotności i temperatury pomieszczeń kontrolowany za pomocą zdublowanych klimatyzatorów precyzyjnych i instalacji wentylacyjnej;
22. Wdrożony system detekcji dymu.
23. **Wymagania dotyczące bezpieczeństwa systemowego**
24. Dwa zasilacze we wszystkich krytycznych serwerach;
25. Podłączenie do dwóch niezależnych obwodów zasilających;
26. Wpięcie do sieci LAN za pomocą co najmniej dwóch kart sieciowych we wszystkich krytycznych serwerach;
27. Zdublowanie wszystkich połączeń światłowodowych.
28. **Wymagania dotyczące fizycznych środków ochrony danych**
29. Dostęp do pomieszczeń lub wydzielonych ich części, w których będzie świadczona usługa będzie zagwarantowany wyłącznie dla osób upoważnionych (za pomocą systemu kontroli), oraz nadzorowany dla celów dowodowych (np. monitoring) z możliwością udostępnienia Zamawiającemu;
30. Dostęp wydzielonych części infrastruktury Data Center, w których przetwarzane będą dane Zamawiającego, muszą mieć osoby upoważnione (posiadające imienne upoważnienia);
31. Dostęp logiczny do systemów, w których przetwarzane są dane Zamawiającego, będą miały wyłącznie osoby upoważnione (posiadające imienne upoważnienia);
32. Miejsce przetwarzania danych Zamawiającego powinno być w sposób należyty zabezpieczone przed awariami i zjawiskami naturalnymi (jak zalania, pożary, itd.).
33. **Wymagania teleinformatyczne**
34. Całość środowiska sprzętowo-systemowego dostarczanego przez Wykonawcę zostanie zaprojektowana i będzie utrzymywana bez pojedynczego punktu awarii;
35. Zabezpieczenie połączenia pomiędzy Data Center a infrastrukturą Zamawiającego zostanie zrealizowane w technologii Secure Sockets Layer;
36. Wykonawca zapewni łącze do sieci Internet o przepustowości minimum 1 Gbps bez limitu transferu.
37. **Wymagania parametrów usługi**
38. Dostarczone środowisko będzie umożliwiało zapisanie 10TB danych.
39. **Okres trwania usługi 24 m-ce.**

**Zadanie nr 9 - Usługa polegająca na wsparciu eksperckim w zakresie cyberbezpieczeństwa, wdrożeniu systemu zarządzania bezpieczeństwem informacji, szkolenia osób odpowiedzialnych za świadczenie usługi kluczowej, audyt.**

**I. Zakup usługi polegającej na wsparciu eksperckim w zakresie cyberbezpieczeństwa**

1. **Usługa polega na:**
2. zakupie wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do 31.12.2022 r. w zakresie wdrożenia przez Wykonawcę na rzecz Zamawiającego wymagań Ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U.2020.1369 t.j. z dnia 2020.08.11) w zakresie:
3. Analizy przedwdrożeniowej;
4. Analizy ryzyka (Art. 8. Ustawy o Krajowym Systemie Cyberbezpieczeństwa)
5. Opracowania i wdrożenie dokumentacji (Art. 10. Ustawy o Krajowym Systemie Cyberbezpieczeństwa)
6. dodatkowo, na podstawie „ZARZĄDZENIE NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA z dnia 20 maja 2022 r. w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców” Zamawiający wymaga przeprowadzenia końcowego audytu cyberbezpieczeństwa w ramach ww. zarządzenia zakończonego raportem. Przeprowadzony audyt wykaże podniesienie poziomu cyberbezpieczeństwa w odniesieniu do stanu początkowego wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.
7. **Wymagania dla członków zespołu audytowego:**

Audyt może być przeprowadzony przez:

1. jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U.2022.5 t.j. z dnia 2022.01.03), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2. co najmniej dwóch audytorów posiadających:
3. certyfikaty określone w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu lub
4. co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
5. co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
6. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
7. Certified Internal Auditor (CIA);
8. Certified Information System Auditor (CISA);
9. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
10. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
11. Certified Information Security Manager (CISM);
12. Certified in Risk and Information Systems Control (CRISC);
13. Certified in the Governance of Enterprise IT (CGEIT);
14. Certified Information Systems Security Professional (CISSP);
15. Systems Security Certified Practitioner (SSCP);
16. Certified Reliability Professional;
17. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.
18. **Analiza przedwdrożeniowa:**
19. identyfikacja i opis usługi kluczowej identyfikacja i opis systemów informacyjnych służących do świadczenia usługi kluczowej;
20. identyfikacja i opis systemów oraz narzędzi wspierających dla systemów informacyjnych służących do świadczenia usługi kluczowej;
21. administrowanie usługą kluczową oraz systemem informacyjnym;
22. organizacja wewnętrznej struktury cyberbezpieczeństwa;
23. wyznaczenie osoby (zespołu) odpowiedzialnej za utrzymanie kontaktów   
    z podmiotami Krajowego Systemu Cyberbezpieczeństwa;
24. szacowanie ryzyka dla systemu informacyjnego usługi kluczowej;
25. szacowanie ryzyka dla obiektu, w którym zlokalizowane są systemy informacyjne usługi kluczowej;
26. zarządzanie bezpieczeństwem informacji (ISO 27001) – organizacja systemu;
27. zarządzanie bezpieczeństwem informacji (ISO 27001) – zabezpieczenia (**Załącznik A**);
28. zarządzanie ciągłością działania (ISO 22301);
29. zbieranie informacji o zagrożeniach dla systemów informacyjnych i ich podatnościach;
30. monitorowania systemu informacyjnego;
31. zabezpieczenie dokumentacji dotyczącej cyberbezpieczeństwa;
32. sposób zarządzania incydentami;
33. zdolność do:
34. analizy kodu złośliwego;
35. badania odporności systemu informacyjnego;
36. zabezpieczenia śladów kryminalistycznych;
37. modele oraz środki łączności wewnętrznej i zewnętrznej
38. Zgodnie z najlepszymi praktykami audytorskimi, proces zdobywania informacji polega na niezależnym i reprezentatywnym doborze próbek podlagających analizie i ocenie, tj. nie musi być realizowany we wszystkich komórkach organizacyjnych czy lokalizacjach.
39. Metodyka zbierania dowodów audytowych:
40. analiza dokumentacji;
41. obserwacja procesu;
42. wywiady
43. **Analiza wpływu i szacowanie ryzyka:**
44. Celem tego etapu jest zidentyfikowanie systemów informacyjnych niezbędnych   
    do niezakłóconego świadczenia usługi kluczowej oraz uzyskanie miarodajnej wiedzy o charakterze i poziomie ryzyka dla jej bezpieczeństwa oraz infrastruktury, z wykorzystaniem której jest ona świadczona.
45. opisanie usługi kluczowej oraz jej kontekstu i uwarunkowań;
46. przeprowadzenie analizy wpływu systemów informacyjnych na niezakłócone świadczenie usługi kluczowej;
47. określenie metodologii analizy ryzyka;
48. identyfikacja podstawowych aktywów świadczenia usługi kluczowej;
49. identyfikacja aktywów wspierających świadczenie usługi kluczowej;
50. identyfikacja i ocena prawdopodobieństwa zagrożeń dla świadczenia usługi kluczowej;
51. identyfikacja i ocena zabezpieczeń systemów informacyjnych służących   
    do świadczenia usługi kluczowej oraz infrastruktury, z wykorzystaniem której jest ona świadczona;
52. szacowanie ryzyka dla systemów informacyjnych służących do świadczenia usługi kluczowej oraz infrastruktury, z wykorzystaniem której jest ona świadczona;
53. planowanie i priorytetyzacja działań na wynikach szacowania ryzyka:
54. unikanie (likwidacja ryzyka);
55. transfer (częściowe lub całkowite przeniesienie ryzyka na inny podmiot);
56. zarządzanie ryzykiem (podjęcie działań zaradczych, które doprowadzić mają do ograniczenia ryzyka do akceptowalnego poziomu);
57. akceptacja (tolerowanie ryzyka)
58. identyfikacja krytycznych obszarów systemu informacyjnego służącego   
    do świadczenia usługi kluczowej oraz infrastruktury, z wykorzystaniem której jest ona świadczona
59. Zakres usługi:
60. identyfikacja systemów informacyjnych niezbędnych do niezakłóconego świadczenia usługi kluczowej;
61. szacowanie ryzyka;
62. analiza oraz ocena procesu i wyników szacowania ryzyka;
63. analiza planów postępowania z ryzykiem nieakceptowalnym.
64. Produkty:
65. opis usługi kluczowej oraz jej kontekstu i uwarunkowań;
66. identyfikację i opis systemów informacyjnych wspierających świadczenia usługi kluczowej;
67. metodologia analizy wpływu biznesowego – identyfikacji systemów informacyjnych niezbędnych do niezakłóconego świadczenia usługi kluczowej;
68. opis systemów informacyjnych niezbędnych do niezakłóconego świadczenia usługi kluczowej;
69. metodologia szacowania ryzyka wystąpienia incydentu dla systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej;
70. rejestr aktywów podstawowych i wspierających dla systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej;
71. rejestr zagrożeń dla systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej wraz z oceną prawdopodobieństwa ich wystąpienia;
72. raport z szacowania ryzyka wraz z opisem stwierdzonych ryzyk i ich kategoryzacją
73. **Dokumentacja systemu zarządzania bezpieczeństwem:**
74. Celem tego etapu jest wypracowanie i wdrożenie wymaganej dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej oraz ochrony infrastruktury, z wykorzystaniem której jest ona świadczona.
75. Przebieg opracowania dokumentacji obejmuje działania:
76. standaryzacja dokumentacji dla całej organizacji;
77. aktualizacja istniejących dokumentów;
78. opracowanie nowych dokumentów;
79. opracowanie zasad nadzoru na dokumentacją
80. Zakres usługi:
81. opracowanie wykazu obowiązkowej dokumentacji;
82. analiza i ocena zaktualizowanej / nowej dokumentacji
83. Potwierdzeniem wykonania dokumentacji SZBI będzie podpisany z wynikiem pozytywnym przez Strony, Protokół odbioru dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji. Zaakceptowana dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji zostanie przygotowana w języku polskim i przekazana Zamawiającemu najpóźniej w dniu jej odbioru w formie:
84. papierowej, w 2 egzemplarzach (format A4, średnia liczba znaków na stronie – 1.900),   
    z zastrzeżeniem, że zostanie wydrukowana dwustronnie,
85. oraz w formie elektronicznej na adres poczty elektronicznej Zamawiającego wskazany   
    w umowie, w formacie plików do edycji i PDF.
86. Dokumenty SZBI wytworzone i aktualizowane będą zawierać wyłącznie autorskie treści Wykonawcy, przygotowane na potrzeby realizacji usługi. Dokumenty dostarczone przez Wykonawcę stają się własnością Zamawiającego z chwilą ich przyjęcia. Zamawiający jest uprawniony do nieograniczonego w czasie i zakresie korzystania z Dokumentacji w celach, dla której została przygotowana przez Wykonawcę w ramach ustalonego wynagrodzenia. Wykonawca przenosi na Zamawiającego autorskie prawo majątkowe.

II. Wdrożenie systemu zarządzania bezpieczeństwem informacji, szkolenia osób odpowiedzialnych za świadczenie usługi kluczowej

1. Przedmiotem usługi będzie:
2. Realizacja procesu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji do wymogów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
3. Przeprowadzenie szkolenia dla pracowników;
4. Przeprowadzenie szkolenia dla działu IT;
5. Przeprowadzenie szkolenia kadry kierowniczej dla grupy **45 osób.**
6. W ramach wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji Wykonawca wspólnie ze wskazanymi przez Zamawiającego pracownikami odpowiedzialnymi za wykonywanie zadań wynikających z SZBI, przeprowadzi czynności opisane w procedurach w SZBI, przynajmniej raz dla każdej procedury. Realizacja procedury powinna być poprzedzona instruktażem stanowiskowym. Wspólna realizacja procedur ma na celu upewnienie Zamawiającego o możliwości realizacji zaprojektowanego SZBI, a tym samym jego wdrożenie. Jeżeli w toku wykonania procedur okaże się, że nie funkcjonuje ona poprawnie, to Wykonawca zaproponuje zmiany do SZBI.
7. Wykonawca przeprowadzi szkolenie dla kadry kierowniczej Zamawiającego, w ramach którego omówi istotę funkcjonowania najważniejszych procesów SZBI wraz ze ścieżką przejścia przez najważniejsze procesy.
8. Wykonawca przeprowadzi szkolenia techniczne dla działu IT (2 uczestników), w trybie zdalnym lub stacjonarnym, trwające minimum 10 dni (ilość godzin minimum 70) lub we współpracy z innym podmiotem w następującym zakresie:
9. Wprowadzenie do bezpieczeństwa systemów Microsoft/Linux:
10. definicje zagrożeń;
11. definicje ataków;
12. Planowanie i konfigurowanie strategii autoryzacji i uwierzytelniania:
13. komponenty modelu uwierzytelniania;
14. planowanie i wdrażanie strategii uwierzytelniania;
15. konta użytkowników, komputerów i grup;
16. Zabezpieczanie serwerów Windows Server:
17. kontrolery domen;
18. szablony zabezpieczeń, GPO;
19. Microsoft Security Compliance Toolkit;
20. audyt zdarzeń;
21. archiwizacja i odzyskiwanie;
22. EFS;
23. BitLocker;
24. serwery plików i wydruku
25. Instalacja, konfigurowanie i zarządzanie urzędem certyfikacji (Certification Authority):
26. przegląd PKI;
27. wprowadzenie do urzędów certyfikatów;
28. instalacja CA
29. zarządzanie urzędem certyfikatów;
30. Konfiguracja, dostarczanie i zarządzanie certyfikatami:
31. przegląd certyfikatów;
32. zatwierdzanie certyfikatów;
33. szablony certyfikatów;
34. wdrażanie archiwizacji kluczy
35. Monitorowanie systemu linux pod kątem bezpieczeństwa:
36. wyszukiwanie rootkitów, trojanów itp.;
37. skanowanie systemu w celu wykrycia podatności;
38. konfiguracja metod uwierzytelniania i autoryzacji;
39. wdrożenie centralnego systemu uwierzytelniania;
40. konfiguracja firewall;
41. SELinux;
42. zabezpieczanie logów systemowych;
43. konfiguracja serwisów logujących;
44. wdrożenie centralnego logowania zdarzeń;
45. Auditd;
46. kontrola pamięci typu USB;
47. bezpieczeństwo rozruchu systemu;
48. szyfrowanie dysków;
49. skanowanie systemu pod kątem podatności;
50. Sniffing - metody obrony;
51. Wykonawca przeprowadzi szkolenie stacjonarne, po audytowe skierowane do pracowników Zamawiającego obejmujące:
52. omówienie podstawowych zasad bezpieczeństwa informacji i wypełniania procedur dotyczących pracowników działu IT wynikających z SZBI;
53. zagrożenia związane z przetwarzaniem informacji;
54. odpowiedzialność za naruszenie zasad Polityki Bezpieczeństwa;
55. zasady zgłaszania i procedury reagowania na incydenty;
56. zasady bezpiecznej realizacji usług na stanowiskach pracy;
57. zagrożenia w sieci (w tym phishing, ransomware, malware, socjotechnika, atak telefoniczny, spoofing, atak odwrócony - zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa) oraz przykłady;
58. bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja;
59. bezpieczne hasła, managery haseł, autoryzacja dwuetapowa, klucze sprzętowe;
60. metody obrony oraz przeciwdziałania (w tym: przed wyłudzeniem danych osobowych za pomocą metod socjotechnicznych, oprogramowaniem mogącym zablokować dostęp do urządzeń firmowych, szkodliwymi programami mogącymi pozyskać dane firmowe lub osobiste;
61. wskazanie zasad cyberhigieny.
62. Wykonawca przygotuje materiały szkoleniowe w wersji papierowej i na nośnikach informatycznych.
63. Wykonawca wykona powdrożeniowy przegląd SZBI, na zakończenie, którego uprawniony audytor wiodący ISO 27001 wystawi pisemną opinię spełnienia wymogów normy ISO 27001 oraz wykaże odstępstwa od normy ISO 27001, jeżeli takowe powstaną na etapie wdrożenia.

**Załącznik A do Zadania Nr 9**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa zabezpieczenia** | **Numer w zał. A normy ISO/IEC 27001** | **Opis zabezpieczenia i zalecenia** |
| **01** | **Polityka bezpieczeństwa informacji** | 5.1.1  5.1.2 | Należy uzgodnić politykę bezpieczeństwa informacji, a następnie ją opublikować i podać do wiadomości wszystkim pracownikom i odpowiednim osobom trzecim. Polityka powinna być poddawana przeglądom i weryfikowana  w zaplanowanych odstępach czasu oraz w przypadku zaistnienia istotnych zmian, aby zapewnić jej adekwatność i skuteczność.  *Sugerowana częstotliwość przeglądu: raz w roku* |
| **02** | **Organizacja bezpieczeństwa informacji** | 6.1.1  6.1.2 | Należy zdefiniować, przypisać i udokumentować role  i zakres odpowiedzialności pracowników, kontrahentów i innych stron w zakresie bezpieczeństwa. Obowiązki  i zakresy odpowiedzialności nie mogą się pokrywać, aby zminimalizować straty, jakie mogą zostać spowodowane niewłaściwym działaniem. |
| **03** | **Uświadamianie, kształcenie**  **i szkolenia z zakresu bezpieczeństwa informacji** | 7.2.2 | Należy regularnie szkolić wszystkich pracowników, kontra- hentów i odpowiednie osoby trzecie oraz uświadamiać ich o zagrożeniach związanych z bezpieczeństwem informacji. Szkolenia powinny także obejmować politykę bezpieczeń- stwa informacji i procedury wdrożone przez organizację.  *Sugerowana częstotliwość szkoleń: raz w roku* |
| **04** | **Wykaz aktywów** | 8.1.1  8.1.2  8.1.3  8.1.4 | Należy sporządzić i prowadzić scentralizowany wykaz ewi- dencji aktywów oraz go aktualizować. Należy zidentyfiko- wać, udokumentować, zatwierdzić i wprowadzić własność i odpowiedzialność za wszystkie aktywa. Ponadto, należy sporządzić procedurę zarządzania wszystkimi aktywami przypisanymi pracownikom lub osobom trzecim, a następ- nie zapewnić identyfikowalność tychże aktywów przez cały okres ich użytkowania.  *Sugerowana częstotliwość przeglądu: raz w miesiącu* |
| **05** | **Klasyfikacja, oznaczanie i przetwarzanie informacji** | 8.2.1  8.2.2  8.2.3 | Informacje należy klasyfikować, oznaczać i przetwarzać zgodnie z ich bezpośrednią wartością dla organizacji i obo- wiązującymi przepisami. Wszyscy właściciele informacji w organizacji powinni sporządzić i wdrożyć politykę oznacza- nia i przetwarzania informacji.  *Sugerowane poziomy klasyfikacji informacji: publiczna, wewnętrzna, poufna* |
| **06** | **Identyfikacja użytkowników** | 9.2.1  9.2.2 | Każdemu użytkownikowi systemów i usług informatycz- nych powinien być przypisany unikalny identyfikator zgodnie z oficjalną procedurą rejestrowania i wyre- jestrowywania, która pozwala przyznawać i odbierać użytkownikom dostęp. |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa zabezpieczenia** | **Numer w zał. A normy ISO/IEC 27001** | **Opis zabezpieczenia i zalecenia** |
| **07** | **Autoryzacja użytkowników** | 9.2.3  9.2.5  9.2.6 | Przypisanie użytkownikom praw uprzywilejowanego dostępu do systemów i usług informatycznych należy monitorować i regularnie weryfikować, podobnie jak korzystanie  z tych praw przez użytkowników. Użytkownicy powinni dysponować tylko minimalnymi prawami dostępu pozwalającymi im na wypełnianie swoich obowiązków. Każda zmiana w prawach dostępu powinna przebiegać zgodnie z procedurą, którą zatwierdza właściciel informacji. |
| **08** | **Uwierzytelnianie użytkowników** | 9.2.4  9.3.1  9.4.1  9.4.2  9.4.3 | Użytkownikom systemów i usług informacyjnych należy poufnie przypisać dane logowania, którymi będą mogli się uwierzytelnić. Zarówno same dane logowania, jak  i sprawdzające je systemy informatyczne, powinny być odpowiednio zabezpieczone w celu minimalizacji ryzyka odgadnięcia przez osoby nieupoważnione.  *Sugerowana siła danych logowania: 8 znaków nietworzących wyrazu ze słownika* |
| **09** | **Umiejscowienie aktywów** | 11.2.1  11.2.2  11.2.3  11.2.6 | Wszystkie aktywa zawierające dane oraz pomocnicze systemy informatyczne powinny znajdować się w miejscu zabezpieczonym przed przypadkowymi uszkodzeniami  i zagrożeniami środowiskowymi oraz być podłączone do odpowiednich urządzeń peryferyjnych. Dotyczy to akty- wów znajdujących się zarówno wewnątrz, jak i na zewnątrz siedziby organizacji. |
| **10** | **Ochrona przed złośliwym oprogramowaniem** | 12.2.1 | Wszystkie aktywa narażone na zainfekowanie złośliwym oprogramowaniem należy zabezpieczyć instalując  i na bieżąco aktualizując oprogramowanie chroniące. |
| **11** | **Procedury bezpieczeństwa informacji** | 12.1.1 | Należy wdrożyć, udokumentować i utrzymywać procedury dotyczące bezpieczeństwa informacji oraz udostępniać je wszystkim użytkownikom. |
| **12** | **Aktualizacje usuwające podatności w oprogramowaniu** | 12.5.1  12.6.1 | Aktualizacje usuwające podatności, udostępniane przez dostawców oprogramowania, powinny być na bieżąco sprawdzane i instalowane na wszystkich urządzeniach.  *Sugerowana częstotliwość instalowania aktualizacji: raz w miesiącu* |
| **13** | **Bezpieczeństwo sieci** | 13.1.1  13.1.2 | Sieci wykorzystujące ICT należy zaprojektować w taki sposób, aby zminimalizować ryzyko podsłuchiwania ruchu sieciowego i wprowadzania w nim niepożądanych zmian. Należy także ograniczyć komunikację pomiędzy zautoryzo- wanymi użytkownikami do niezbędnego minimum i bloko- wać resztę komunikacji. |
| **14** | **Bezpieczeństwo w umowach**  **z dostawcami** | 15.1.1  15.1.2  15.1.3 | Wszyscy dostawcy, z którymi organizacja wymienia infor- macje, powinni znać polityki bezpieczeństwa obowiązujące w organizacji, a umowy z nimi powinny nakazywać im przestrzegania tychże polityk, co pozwoli na przeprowadza- nie weryfikacji. Te same zalecenia dotyczą podwykonawców pracujących z dostawcami. |

|  |  |  |  |
| --- | --- | --- | --- |
| **15** | **Analiza incydentów i reakcja na nie** | 16.1.2  16.1.3  16.1.4  16.1.5 | Wszyscy użytkownicy systemów i usług informatycznych po- winni zgłaszać wszelkie zaobserwowane lub podejrzewane słabe punkty w zabezpieczeniach w celu analizy. Wyniki ana- lizy pozwolą zastosować konkretne procedury reagowania na incydenty przy zachowaniu pełnego wglądu w sytuację  w trakcie jej rozwoju. |
| **16** | **Identyfikacja wymagań prawnych i umownych** | 18.1.1  18.1.4 | Wszystkie mające zastosowanie wymagania dotyczą- ce bezpieczeństwa informacji wynikające z krajowych, międzynarodowych i sektorowych przepisów należy na  bieżąco monitorować, podobnie jak wymagania wynikają- ce z umów zawartych z osobami trzecimi. Należy zwrócić szczególną uwagę na ochronę danych osobowych. |

* 1. Zabezpieczenia dodatkowe

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa zabezpieczenia** | **Numer w zał. A normy ISO/IEC 27001** | **Opis zabezpieczenia i zalecenia** |
| **01** | **Zarządzanie kontaktami zewnętrznymi i komunikacją** | 6.1.3  6.1.4 | Organizacja powinna nawiązać i utrzymywać stosowne kontakty z właściwymi organami władzy, aby umożliwić szybką reakcję na powszechne zagrożenia, oraz z gru- pami zainteresowanych specjalistów, forami i stowarzy- szeniami z obszaru bezpieczeństwa, przede wszystkim w celu uzyskania rzetelnych informacji o zagrożeniach  i zabezpieczeniach. |
| **02** | **Telepraca** | 6.2.2 | Należy wdrożyć politykę oraz wspierające ją zabezpie- czenia w celu ochrony informacji pobieranych, przetwa- rzanych i przechowywanych w miejscu wykonywania telepracy. Narzędzia do telepracy należy opracowywać z uwzględnieniem dodatkowych zabezpieczeń, aby zapobiec wyciekowi i nadużywaniu informacji. System  dostępu na odległość należy zabezpieczyć przed osobami nieupoważnionymi. |
| **03** | **Zarządzanie urządzeniami mobilnymi** | 6.2.1 | Należy odpowiednio skonfigurować zabezpieczenia  w urządzeniach mobilnych wykorzystywanych do pracy, a także ściśle je monitorować. |
| **04** | **Postępowanie sprawdzające pracowników** | 7.1.1 | Należy sprawdzać przeszłość kryminalną oraz związane z nią informacje wszystkich pracowników i osób trzecich,  którzy mają regularny dostęp do budynku organizacji, zgod- nie z odpowiednimi przepisami prawa i zasadami etyczny- mi. Zakres takiej kontroli powinien być proporcjonalny do wymagań biznesowych. |
| **05** | **Klauzule w umowach pracowników** | 7.1.2  7.2.3  7.3.1  13.2.4 | Wszyscy pracownicy i osoby trzecie powinni podpisać umowę o zachowaniu poufności przed rozpoczęciem korzy- stania z danych organizacji. Umowa powinna też wymagać przestrzegania polityki bezpieczeństwa informacji stosowa- nej przez organizację oraz jasno przedstawiać konsekwen- cje jej nieprzestrzegania, w tym konsekwencje następujące po zmianie stanowiska bądź rozwiązaniu umowy. |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa zabezpieczenia** | **Numer w zał. A normy ISO/IEC 27001** | **Opis zabezpieczenia i zalecenia** |
| **06** | **Zarządzanie nośnikami wymiennymi** | 8.3.1  8.3.3  13.2.1  13.2.2  18.1.3 | Obsługa wszelkich nośników wymiennych powinna być ograniczona konkretnymi zasadami. Nośniki zawierające informacje należy zabezpieczyć przed niepożądanym dostępem, nadużyciem i zniszczeniem w przypadku, gdyby znalazły się poza siedzibą organizacji. |
| **07** | **Usuwanie danych** | 8.3.2  11.2.7 | Należy stosować ścisłe procedury dotyczące bezpiecznego usuwania danych z nośników, które mają być wykorzystane do innych celów, bądź usunięte, w celu uniemożliwienia odzyskania poprzednich danych.  *Sugerowany sposób usuwania danych: pełne nadpisanie* |
| **08** | **Polityka kontroli dostępu** | 9.1.1  9.1.2 | Należy udokumentować, prowadzić i dokonywać przeglądu oficjalnej polityki kontroli dostępu do systemu i sieci organi- zacji zgodnie z wymaganiami dotyczącymi bezpieczeństwa, klasyfikacji informacji i zarządzania nimi oraz poziomów uwierzytelniania pracowników. |
| **09** | **Szyfrowanie** | 10.1.1  10.1.2 | Należy opracować, udokumentować, wprowadzić, zacho- wywać oraz dokonywać okresowych przeglądów i aktuali- zować zabezpieczenia kryptograficzne wykorzystujące silne algorytmy, w celu zapewnienia poufności przechowywa- nych i przekazywanych informacji. Zaleca się stosowanie ścisłych, udokumentowanych procedur dotyczących użyt- kowania, zabezpieczania i przechowywania kluczy krypto- graficznych przez cały okres ich użytkowania.  *Sugerowane algorytmy szyfrujące: AES128+, SHA512+, RSA2048+* |
| **10** | **Bezpieczeństwo fizyczne** | 11.1.1  11.1.2  11.1.3.  11.1.6 | Należy zdefiniować bariery fizyczne i strefy bezpieczeń- stwa w celu zminimalizowania niepożądanego dostępu do budynku i systemów informatycznych organizacji oraz wyposażyć te bariery w system kontroli dostępu. Należy ograniczyć i odpowiednio zabezpieczyć punkty dostępu, w tym punkty ściągania i wysyłania danych. |
| **11** | **Ochrona przed zagrożeniami zewnętrznymi**  **i środowiskowymi** | 11.1.4 | Należy opracować i stosować w budynkach i znajdujących się w nich systemach informatycznych fizyczne zabez- pieczenia przed katastrofami naturalnymi bądź innymi klęskami żywiołowymi czy też katastrofami spowodowa- nymi przez człowieka.  *Sugerowane zagrożenia, które należy wziąć pod uwagę: pożar, wilgoć, trzęsienie ziemi* |
| **12** | **Konserwacja sprzętu** | 11.2.4 | Sprzęt należy konserwować zgodnie z Planem Bezpie- czeństwa Informacji obowiązującym w organizacji. Należy monitorować dostęp do systemów informatycznych uzyskany w celach konserwacji. |

|  |  |  |  |
| --- | --- | --- | --- |
| **13** | **Stanowiska pracy**  **i sprzęt bez nadzoru** | 11.2.8  11.2.9 | Przed pozostawieniem stanowiska pracy bez nadzoru, wszel- kie urządzenia należy zawsze zabezpieczyć przed niepożą- danym dostępem fizycznym i kradzieżą. Urządzenia należy zablokować po każdej sesji pracy oraz ustawić automatyczne wyłączanie po odpowiednim okresie nieaktywności. Na stanowiskach pracy nie należy zostawiać żadnych nośników danych bez nadzoru.  *Sugerowany czas do automatycznego zamknięcia sesji lub włączenia wygaszacza ekranu: 15 minut* |
| **14** | **Zarządzanie zmianami** | 12.1.2  12.6.2  14.2.2  14.2.4 | Wszelkie zmiany w procesach i systemach organizacyjnych, biznesowych i informatycznych, które mogą wpłynąć na bezpieczeństwo informacji, należy rejestrować, zatwierdzać i sprawdzać. Zmiany w systemie i oprogramowaniu powinni wprowadzać wyłącznie upoważnieni pracownicy. |
| **15** | **Rozdział środowisk do opracowywania i testowania** | 12.1.4  14.3.1 | Należy w miarę możliwości rozdzielić infrastrukturę prze- znaczoną do opracowywania i testowania oraz infrastruk- turę operacyjną w celu zminimalizowania ryzyka nieupo- ważnionego dostępu do systemu operacyjnego. Ponadto, dane wykorzystywane do opracowywania i testowania powinny różnić się od danych wykorzystywanych do produkcji (tj. powinny być anonimowe lub niezwiązane  z prawdziwymi osobami i zdarzeniami).  *Sugerowany sposób rozdziału: odrębne systemy i sieci* |
| **16** | **Zapasowe kopie informacji** | 12.3.1 | Należy tworzyć i regularnie sprawdzać kopie zapasowe in- formacji i oprogramowania zgodnie z opracowaną polityką kopii zapasowych.  *Sugerowana częstotliwość tworzenia kopii zapasowych: raz dziennie lub raz w tygodniu* |
| **17** | **Rejestracja**  **i przechowywanie zdarzeń** | 12.4.1  12.4.2  12.4.3 | Należy rejestrować większość działań związanych z bez- pieczeństwem, a rejestry należy zabezpieczać i chronić przed dostępem i zmianami oraz poddawać regularne- mu przeglądowi. Wszelkie działania wykonywane przez administratorów i operatorów systemów powinny być rejestrowane jako udane bądź nieudane próby logowania i wylogowania.  *Sugerowany okres przechowywania rejestrów: sześć miesięcy lub więcej* |
| **18** | **Synchronizacja zegarów** | 12.4.4 | Zegary systemowe we wszystkich działach organizacji lub domeny bezpieczeństwa należy na bieżąco synchronizo- wać z jednym wzorcowym i rzetelnym źródłem czasu. |
| **19** | **Rozdzielenie sieci** | 13.1.3 | Usługi i systemy informatyczne oraz ich użytkowników należy rozdzielić w obrębie różnych obszarów sieci, przy czym we wszystkich obszarach powinny obowiązywać jednakowe wymagania dotyczące zabezpieczeń. Rozdziału należy dokonać za pomocą zapór ogniowych (ang. firewalls) lub podobnych rozwiązań. |
| **20** | **Bezpieczeństwo wiadomości**  **i komunikacji elektronicznej** | 13.2.3 | Należy zapewnić poufność informacji przekazywanych za pomocą komunikatorów i podobnych systemów oraz wykrywać ataki dokonywane tą drogą. |

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Nazwa zabezpieczenia** | **Numer w zał. A normy ISO/IEC 27001** | **Opis zabezpieczenia i zalecenia** |
| **21** | **Uwzględnianie bezpieczeństwa na etapie projektowania rozwiązań** | 6.1.4  14.1.1  14.2.5 | Bezpieczeństwo informacji powinno być nieodłączną częścią systemów informatycznych przez cały okres użyt- kowania tychże systemów, w tym podczas wczesnej fazy projektowania. Wszelkie projekty podejmowane w orga- nizacji powinny brać pod uwagę kwestie bezpieczeństwa informacji od jak najwcześniejszego etapu. |
| **22** | **Bezpieczeństwo usług aplikacyjnych** | 14.1.2  14.1.3 | Systemy informatyczne wykorzystywane do świadczenia usług powinny być chronione przed typowymi atakami za pomocą bezpiecznej, wzmocnionej konfiguracji. Powin- ny być także opracowywane w taki sposób, by mogły korzystać z dodatkowych zabezpieczeń i być na bieżąco monitorowane i chronione za pomocą dedykowanych środków bezpieczeństwa, proporcjonalnie do ich naraże- nia na ataki.  *Sugerowane środki bezpieczeństwa: zapory ogniowe i IDS/IPS* |
| **23** | **Bezpieczny cykl opracowywania projektów** | 14.2.1  14.2.6  14.2.7 | Organizacja powinna ustanowić wytyczne dotyczące bezpiecznego cyklu opracowywania aplikacji, które można także będzie zastosować do projektów zewnętrznych wykonywanych na zlecenie w celu zminimalizowania podatności w aplikacjach. |
| **24** | **Testowanie bezpieczeństwa** | 14.2.3  14.2.8  14.2.9  18.2.3 | Należy ustanowić kryteria dotyczące bezpieczeństwa i za- twierdzania nowych systemów informatycznych oraz no- wych aktualizacji i wersji oprogramowania. Ponadto każdy system należy odpowiednio testować w fazie opracowy- wania, przed zaakceptowaniem, a następnie w regularnych odstępach czasu. Wykryte podatności należy usunąć przed następnym testem.  *Sugerowana częstotliwość testowania: testy wewnętrzne raz na sześć miesięcy, testy zewnętrzne raz na kwartał* |
| **25** | **Monitorowanie bezpieczeństwa usług świadczonych przez dostawców** | 15.2.1  15.2.2 | Należy regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych, w tym realne wypełnia- nie przez dostawców zapisów umownych. |
| **26** | **Polityka zarządzania incydentami** | 16.1.1 | Incydenty związane z bezpieczeństwem informacji należy kontrolować, rejestrować i przetwarzać oraz reagować na nie zgodnie z konkretnymi odpowiedzialnościami wpro- wadzonymi i zatwierdzonymi przez kierownictwo. Należy również wprowadzić odpowiednie procedury komunikacji i eskalacji. |
| **27** | **Wyciąganie wniosków z incydentów** | 16.1.6 | Wiedzę zdobytą podczas analizy i rozwiązywania incy- dentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wy- stąpienia lub skutku przyszłych incydentów. Może okazać się konieczne dostosowanie procedur reakcji na incydenty do nowych warunków. |

|  |  |  |  |
| --- | --- | --- | --- |
| **28** | **Zarządzanie redundancją** | 17.2.1 | Obiekty przetwarzające informacje należy wyposażyć w re- dundantne komponenty w taki sposób, by mogły spełnić wymagania dotyczące dostępności nawet podczas awarii. |
| **29** | **Ochrona własności intelektualnej** | 18.1.2 | Należy wdrożyć procedury zapewniające zgodność  z wymaganiami prawnymi, regulacyjnymi i umownymi w zakresie wykorzystania materiałów objętych prawem  własności intelektualnej i użytkowaniem prawnie zastrze- żonego oprogramowania. |
| **30** | **Audyty i oceny bezpieczeństwa informacji** | 18.2.1  18.2.2 | Niezależni audytorzy powinni regularnie dokonywać prze- glądu systemów bezpieczeństwa informacji. Kierownictwo powinno zapewnić prawidłowe wdrażanie wszystkich procedur bezpieczeństwa w ramach swojego zakresu od- powiedzialności w celu uzyskania zgodności z politykami  i normami bezpieczeństwa. Należy regularnie dokonywać przeglądu systemów informatycznych, aby zapewnić cią- głą zgodność z normami wdrażania bezpieczeństwa. |