# Plan działania
# w zakresie cyberbezpieczeństwa
# w ochronie zdrowia

Rekomendacje Centrum E-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa wersja 1.2



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

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

NIP: 5251575309
REGON: 001377706

# I. Spis treści





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

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

NIP: 5251575309
REGON: 001377706

Wykaz ilustracji





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

# II. Cyberbezpieczeństwo sektora ochrony zdrowia - wstęp

System cyberbezpieczeństwa w każdym sektorze opiera się o zestaw regulacji prawnych adresujących zadania do poszczególnych organów. W oparciu o ustawę o Krajowym Systemie Cyberbezpieczeństwa wyróżnić należy:

- Organ Właściwy do spraw cyberbezpieczeństwa – w przypadku Ochrony Zdrowia jest to Minister Zdrowia

- Sektorowy Zespół Cyberbezpieczeństwa -CSIRT – w każdym sektorze Organ Właściwy do spraw Cyberbezpieczeństwa może powołać sektorowy zespół do spraw cyberbezpieczeństwa – w tym wypadku CSIRT sektor ochrony zdrowia

- Podmioty Wykonujące Działalność Leczniczą – wszystkie podmioty sektora ochrony zdrowia zajmujące się leczeniem. Podmioty te zgodnie z Rozporządzeniem o Krajowych Ramach Interoperacyjności oraz z ustawą o Krajowym Systemie Cyberbezpieczeństwa wykonują działania w celu zapewnienia bezpieczeństwa danych medycznych oraz informują właściwy CSIRT i incydentach.

Wszystkie podmioty sektora ochrony zdrowia muszą wypełniać obowiązki w zakresie cyberbezpieczeństwa wynikające z dwóch podstawowych aktów prawnych - Rozporządzenia KRI oraz Ustawy KSC.

Zgodnie z rozporządzeniem o Krajowych Ramach Interoperacyjności każdy podmiot realizujący zadania publiczne musi dostosować swój system teleinformatyczny do wymagań zawartych w normie ISO/IEC 27001. W tym celu należy m. innymi wdrożyć System Zarządzania Bezpieczeństwem Informacji oraz wykonywać raz do roku audyt potwierdzający zgodność jednostki z wymaganiami KRI.

Podstawowe kroki do wdrożenia KRI:

1. Opracowanie i wdrożenie dokumentacji systemu zarządzania bezpieczeństwem informacji
2. Opracowanie i wdrożenie schematu zarządzania i nadzoru nad incydentami
3. Prowadzenie regularnych szkoleń w zakresie bezpieczeństwa informacji
4. Coroczne wykonywanie audytów wewnętrznych systemu zarządzania bezpieczeństwem informacji na zgodność z rozporządzeniem KRI
5. Wykonanie działań korygujących i zapobiegawczych – wykonanie zaleceń po audytowych

Podstawowe kroki do wdrożenia KSC (Operatorzy Usług Kluczowych)

Pełne obowiązki operatorów usług kluczowych są określone w ustawie o KSC i każdy operator powinien się z nimi zapoznać, aby móc zapewnić zgodność z ustawą.

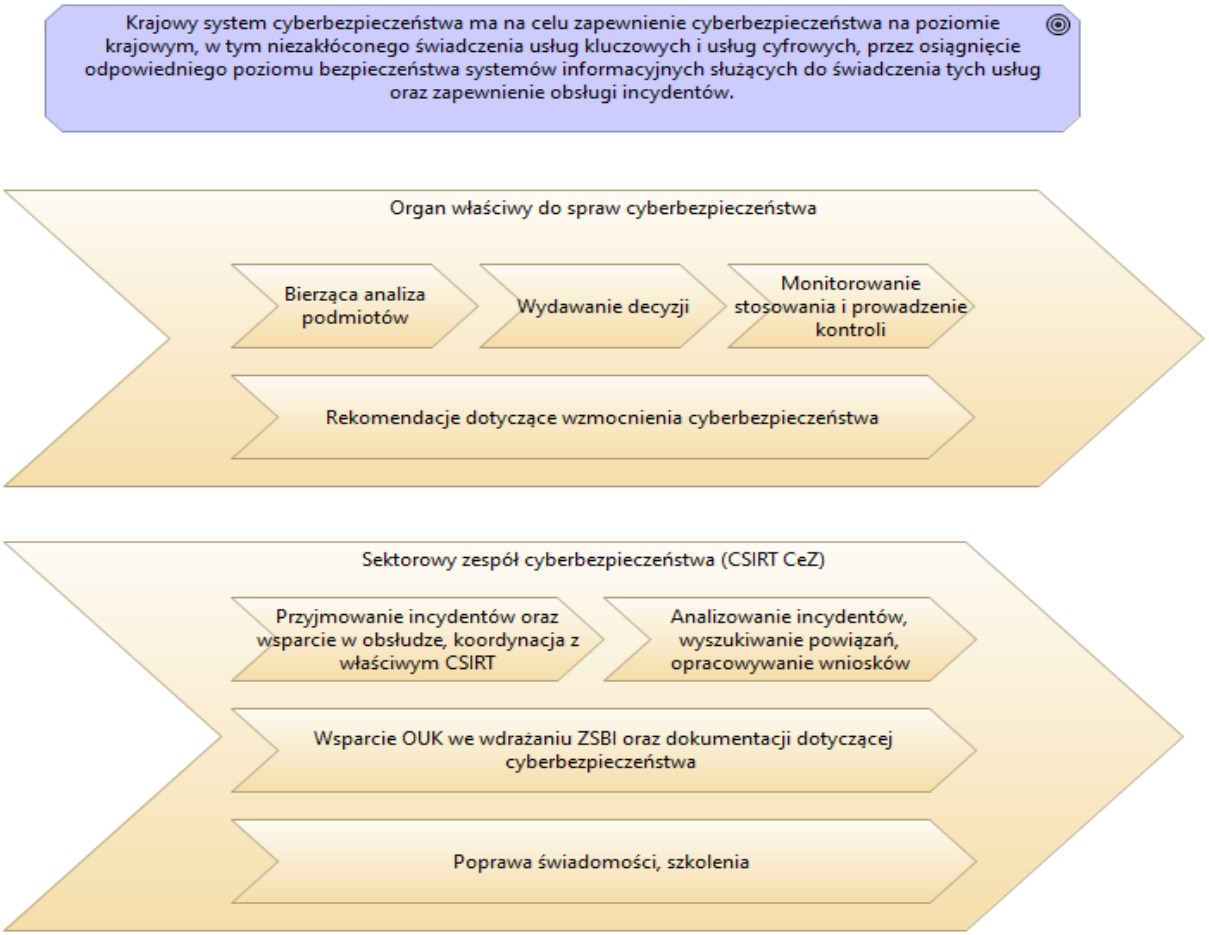


Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Do najważniejszych grup obowiązków należą:

1. zarządzanie ryzykiem (w tym szacowanie ryzyka);
2. wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe; bezpieczeństwo i ciągłość dostaw; wdrażanie, dokumentowanie i utrzymywanie planów działania);
3. zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty;
4. obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT; wyznaczenie osoby kontaktowej na potrzeby KSC.

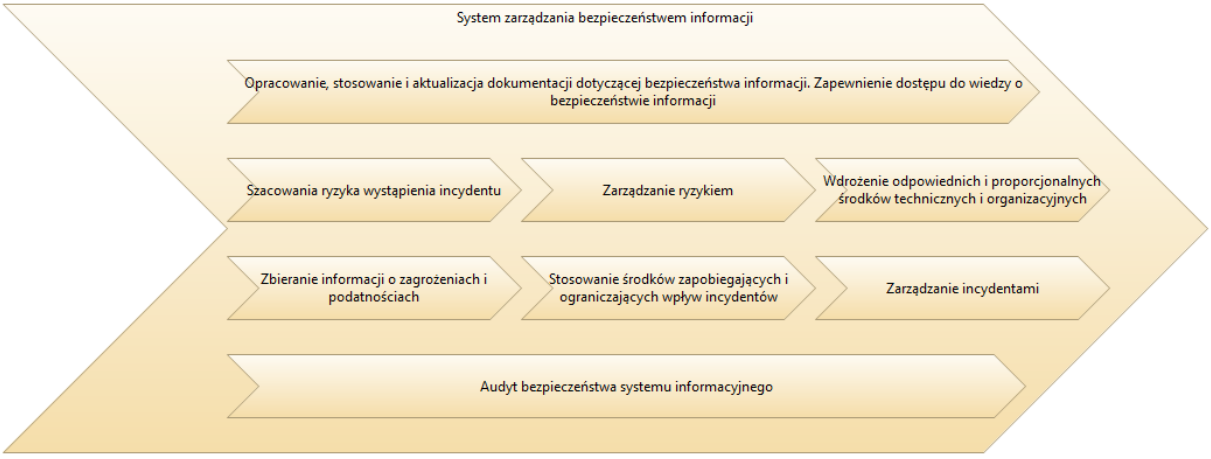
Prezentacja graficzna poszczególnych łańcuchów zadań (wartości):




*Rysunek 1 Łańcuch wartości dla organu właściwego z KSC i CSIRT*



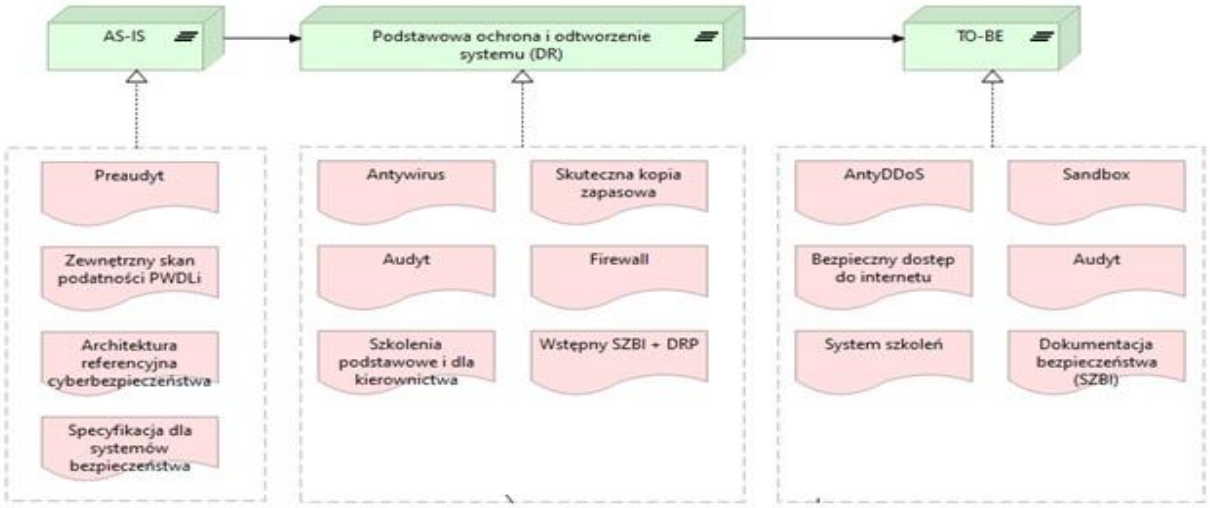
Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706




*Rysunek 2 Łańcuch wartości dla PWDL*

Rekomendowany w CEZ plan działania celem wdrożenia zaleceń KRI/KSC:

1. Ustalenie stanu obecnego – preaudyt/ankieta poziomu dojrzałości; skan podatności; ustalenie potrzeb; specyfikacja funkcjonalna i techniczna systemu bezpieczeństwa
2. Implementacja podstawowej architektury bezpieczeństwa – SZBI; skuteczna polityka kopii bezpieczeństwa; ochrona brzegu sieci; antywirus; szkolenia w zakresie cyberbezpieczeństwa; audyt
3. Rozbudowa systemu podstawowego do systemu docelowego jako proces – dokumentacja SZBI aktualizowana okresowo; ochrona poczty elektronicznej; ochrona łącz dostępowych; szkolenia jako proces w organizacji




*Rysunek 3 Plan implementacji w PWDL*



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

System Zarządzania Bezpieczeństwem Informacji (SZBI) - z ang. ISMS (Information Security Management System) - część całościowego systemu zarządzania oparta na podejściu wynikającym z oceny ryzyka, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. System zarządzania obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa).

Na dokumentację składają się następujące dokumenty:

- ZSZ.ISO.PBI-Polityka_Zintegrowanego_Systemu_Zarzadzania
- ZSZ.ISO.PBI-Ksiega_Zintegrowanego_Systemu_Zarzadzania
- ZSZ.ISO.SOA-Deklaracja_Stosowania
- ZSZ.ISO.PR.7.5.3-Nadzor_nad_Udokumentowanymi_Informacjami
- ZSZ.ISO.PR.9.2-Audyt_Wewnetrzny_ZSZ
- ZSZ.ISO.PR.9.3-Przeglad_Zarzadzania
- ZSZ.ISO.PR.A.12.6.1-Zarzadzanie_Podatnosciami
- ZSZ.ISO.PR.A.16-Z2-Instrukcja_Zabezpieczania _Materiału_Dowodowego
- ZSZ.ISO.PR.A.16-Z1-Rejestr_Zdarzen_i_Incydentow_
- ZSZ.ISO.PR.A.16-Zarzadzanie_Incydentami_Bezpieczenstwa
- ZSZ.ISO.PR.A.8.3-Zarzadzanie_Nosnikami_Informacji
- ZSZ.ISO.PR.A.7-Zarzadzanie_Bezpieczenstwem_Zasobow_Ludzkich
- ZSZ.ISO.P.01-Polityka_Dostepu_do_Srodowiska_Teleinformatycznego
- ZSZ.ISO.P.A.15-Polityka_Bezpieczenstwa_Informacji_dla_Wykonawców
- ZSZ.ISO.PR.10.1-Dzialania_Korygujace
- ZSZ.ISO.P.A.14-Polityka_Pozyskiwania_Rozwoju_i_Utrzymania_Systemow
- ZSZ.ISO.PR.9.1-Monitorowanie_Skutecznosci_Zintegrowanego Systemu Zarządzania
- ZSZ.ISO.PR.A.18.2.2-Zarzadzanie_Wyjatkami_Bezpieczenstwa_Informacji
- ZSZ.ISO.SL-01-Slownik_Definicji_i_Skrotow
- ZSZ.ISO.PR.A.8.2-Zasady_Postepowania_z_Informacjami_- zmiany
- Polityka-i-metodyka-zarzadzania-ryzykiem
- Polityka nadawania, odbierania, modyfikacji uprawnień



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

# III. Zasady postępowania w przypadku stwierdzenia ataku ransomware

## 3.1 Hybrydowe podejście do bezpieczeństwa

- współpraca wewnętrznych specjalistów z ekspertami z zewnątrz:

> W przypadku ataku typu ransomware dobrą praktyką jest **zaangażowanie zewnętrznych ekspertów**, w celu ustalenia źródła ataku oraz podatności (luk), które zostały wykorzystane. Poleganie jedynie na wewnętrznym IT może prowadzić do błędnych wniosków (jeśli np. ransomware był atakiem wewnętrznym, a także jeśli administratorzy próbują ukryć podatność, którą sami stworzyli, lub w przypadku naruszenia polityki bezpieczeństwa obowiązującej w organizacji). Dobrą praktyką jest wykorzystanie ekspertów zewnętrznych w celu przeprowadzenia 'kontrolowanego' ataku w celu ujawnienia wszelkich podatności zanim nastąpi faktyczny atak ransomware.

- weryfikacja stanu kopii zapasowych:

Celem weryfikacji poprawności wykonywania kopii zapasowych kierownik jednostki/osoba odpowiedzialna za stan kopii powinny okresowo wypełniać poniższą tabelę. Kolejn kolumny zawierają listę systemów, wktórych gromadzone są dane medyczne lub systemów niezbędnych do funkcjonowania infrastruktury informatycznej w jednostce; wersję systemu – zwykle jest to kombinacja liter i cyfr stanowiąca tzw. numer wersji/ ostatniej aktualizacji systemu; informację czy kopię wykonuje się codziennie – w przypadku systemów gromadzących dane medyczne jest szczególnie ważne aby kopie były aktualizowane min. 1 raz/dobę; odmiejscowienie – informacja o tym, czy kopia bezpieczeństwa wykonana jest na nośniku, który następnie został odłączony od sieci LAN jednostki.; weryfikacja odtwarzania – wykonywane codziennie kopie bezpieczeństwa należy okresowo odtwarzać i sprawdzać czy np. nośnik nie uległ zużyciu lub uszkodzeniu. Okresowa weryfikacje możliwości odtwarzania zmniejsza ryzyko, iż w krytycznym momencie może nie dać się odtworzyć kopii zapasowej.

Przedstawiona poniżej tabela to przykład prostej możliwości sprawdzenia czy służby informatyczne w jednostce wykonują prawidłową kopię bezpieczeństwa. Przykładowe wartości wpisane do tabeli to jedynie przykład, pokazujący jakie wartości powinny się w tabeli pojawić.



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

| SYSTEM | WERSJA, AKTUALIZACJA | KOPIA ZAPASOWA | | |
|---|---|---|---|---|
| | | Wykonywana codziennie | Odmiejscowiona | Weryfikacja odtwarzania |
| **HIS** | 1.11.08 | TAK | taśma | 10.12.2022 |
| **LABORATORIUM LIS** | xxxxx | NIE | NIE | xxxx |
| **APTEKA** | xxxxx | xxxx | xxxx | xxxx |
| **PACS** | xxxxx | xxxx | xxxx | xxxx |
| **EDM** | xxxxx | xxxx | xxxx | xxxx |
| **FK, Kadry** | xxxxx | xxxx | xxxx | xxxx |
| **AD, DNS** | xxxxx | xxxx | xxxx | xxxx |
| **wirtualizator** | xxxxx | xxxx | xxxx | xxxx |



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

## 3.2 Opracowanie planu komunikacji i działania

Należy zdefiniować proces, który:

1) **Jednoznacznie potwierdzi, że nastąpił atak** po to, aby dać zgodę administratorom na rozpoczęcie procesu odzyskiwania, co będzie skutkowało ograniczeniem wydajności środowiska lub jego całkowitą niedostępnością.

2) **Oszacuje skalę problemu zaszyfrowania danych**, możliwości ich odtworzenia oraz potencjalny czas przywrócenia działania wszystkich usług, a następnie przekaże te dane do osób odpowiedzialnych za komunikację wewnątrz i na zewnątrz organizacji.

3) **zdefiniuje politykę odtwarzania** - mogą być wykonywane w zdefiniowany wcześniej sposób (wykorzystując skrypty, gdzie zaszyta została kolejność oraz logika odtworzenia). Innym sposobem jest wykorzystanie dedykowanego narzędzia do orkiestracji tak, aby nie było wymagane ręczne tworzenie skryptów. Jeszcze innym podejściem jest umowna polityka „papierowa", gdzie to rolą administratora jest późniejsze jej wykonanie. Krytycznym elementem jest ustalenie zakresu odtwarzania, kolejności, w której systemy są odtwarzane: najpierw krytyczne od strony infrastrukturalnej, dalej krytyczne od strony danych „białych", potem części biznesowej i dopiero pozostałe dane. Równie ważne jest wyraźne określenie tego, co uznaje się za poprawnie odtworzony system – mogą być to testy zarówno zautomatyzowane jak i ręczne.

**Bezpośrednio po ataku warto podjąć kroki podane poniżej jako przykładowa lista:**

a. Poinformuj dyrektora jednostki, uzgodnij zgłoszenie do właściwego CSIRT
b. NIE WYŁĄCZAJ SERWERÓW, Skontaktuj się z CBZC to specjalizowana jednostka Policji do zadań w zakresie cyberprzestępczości. Informacje o najbliższej jednostce CBZC znajdziesz we właściwym Urzędzie Wojewódzkim.
c. Wykonaj kopię zaszyfrowanych danych na zasób, który następnie odseparujesz
d. Przygotuj do odtworzenia kopie zapasowe danych – zweryfikuj datę ich wykonania
e. Odłącz stacje robocze jako potencjalnie zainfekowane
f. Zweryfikuj konfigurację i wersję urządzeń brzegowych
g. Zweryfikuj kontakty/umowy z dostawcami systemów HIS,LAB i innych
h. Zorganizuj zespół zarządzania zdarzeniem : Dyrektor, pełnomocnik ds. bezpieczeństwa, inspektor ochrony danych osobowych, kierownik informatyki
i. Ustal priorytety, rozdziel zadania: zgłoszenie do UOD, reinstalacja infrastruktury, organizacja pracy jednostki do momentu przywrócenia sprawnej infrastruktury i systemów
j. Ustal ramy czasowe zadań :
    1. Reinstalacja usług podstawowych w LAN: AD, DNS, DHCP lub inne środowiska.
    2. Skanowanie AV stacji roboczych
    3. Uruchomienie usług zdalnego dostępu (jeśli są potrzebna)
    4. Instalacja serwerów aplikacyjnych i baz danych (odtwarzanie z kopii zapasowych)
k. Weryfikuj status prac 3 razy w ciągu doby



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

# IV. Rekomendacje w zakresie architektury cyberbezpieczeństwa (podstawowej i docelowej)

## 1. Architektura podstawowa

Tworząc podstawy bezpieczeństwa infrastruktury informatycznej należy skoncentrować wysiłki na obszarach objętych największym ryzykiem wycieku danych i ataku z zewnątrz na infrastrukturę wewnątrz jednostki. Niniejsza rekomendacja skupia się na typowych zagadnieniach cyberbezpieczeństwa, nie rozwijając wątku zasilania gwarantowanego oraz zagadnień związanych z ciągłością działania i dokumentacji procesów oceny ryzyka i polityk w tym zakresie. Obowiązki wynikające z Rozporządzenia o Krajowych Ramach Interoperacyjności należy spełniać od 2012 roku a normy i standardy w tym zakresie opisano na serwisie GOV.PL. Wszelkie informacje można odszukać w tym miejscu:
https://www.gov.pl/web/ia/standardy-krajowych-ram-interoperacyjnosci-kri

Poniższe rekomendacje opierają się o następujące priorytety:

PRIORYTET PIERWSZY

**Konieczność ochrony danych medycznych** w przypadku skutecznego ataku Ransomware. Nie ma możliwości zapewnienia 100% ochrony przed atakami. Dlatego największy nacisk należy położyć na działania zapewniające zachowanie jak najbardziej aktualnych danych w kopiach zapasowych. Kopie zapasowe w celu zapewnienia ich prawidłowego odczytania (odtworzenia danych) muszą być wykonywane regularnie, zgodnie z przestrzeganą polityką tworzenia kopii, muszą być regularnie weryfikowane w celu sprawdzenia ich możliwości odczytania, muszą być odmiejscowione dla uzyskania pewności, iż w momencie ataku kopie nie będą narażone na skasowanie.

PRIORYTET DRUGI

**Ochrona poczty elektronicznej** jako usługi własnej lub dzierżawionej. Atak typu ransomware opiera się o wykorzystanie podatności serwerów pocztowych lub o metodę polegającą na przesłaniu infekującego załącznika w poczcie elektronicznej. Konieczne jest zatem aktywne weryfikowanie treści załączników oraz linków zawartych w poczcie a także ochrona dostępu do skrzynek poprzez wprowadzenie dodatkowych faktorów uwierzytelniania.

PRIORYTET TRZECI

**Ochrona brzegu sieci.** Braki finansowe i niedostatek kadr wielokrotnie powodują brak aktualizacji, podatności w urządzeniach brzegowych. Konieczne jest uaktualnienie bądź zakup nowych urządzeń typu firewall. Urządzenia tego typu stanowią pierwszą i główną zaporę zasobów przed rekonesansem i atakiem cyberprzestępców. Podatności i niedostatki konfiguracyjne tych urządzeń powinny być likwidowane celem ochrony zasobów danych.

PRIORYTET CZWARTY

**Ochrona stacji roboczych.** Atak typu ransomware polega na stopniowej infekcji wszystkich dostępnych stacji roboczych. Możliwość wykrycia i zablokowania aktywności polegającej na szyfrowaniu stacji roboczych powinna stanowić swoistą



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

„drugą linię obrony” w przypadku zainfekowania sieci LAN. Segmentacja sieci lokalnych oraz stałe monitorowanie stacji roboczych będzie czynnikiem podnoszącym odporność zasobów na atak. Segmentacja sieci dodatkowo wspiera proces „oddzielenia” systemów kopii zapasowych od reszty systemów produkcyjnych (część priorytetu pierwszego).

### 2. Podstawowe działania w celu realizacji priorytetów

W ramach podstawowych struktur systemu cyberbezpieczeństwa rekomendowane są działania w zakresie:

a) Audytu bezpieczeństwa w oparciu o rozporządzenie KRI (w przypadku otrzymania decyzji OUK audyt musi obejmować obowiązki wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa – informacje w tym miejscu https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- )
b) Instalacji urządzeń typu FIREWALL
c) Skutecznej ochrony antywirusowej
d) Skutecznej kopii zapasowej
e) Bezpiecznej poczty elektronicznej
f) Przygotowania dokumentacji Zintegrowanego Systemu Zarządzania Bezpieczeństwem w jednostce
g) Przygotowaniu i przeprowadzeniu cyklicznych szkoleń całej załogi w zakresie bezpieczeństwa

## V. Rekomendacje w zakresie funkcjonalności komponentów bezpieczeństwa

Poniżej przedstawiono opisy funkcjonalne urządzeń lub usług. Opisy te mogą stanowić pomoc w sporządzeniu dokumentacji opisującej wymagania dotyczące sprzętu lub usług zamawianych celem wypełnienia przedstawionych wyżej priorytetów. Zawarty poniżej opis wymagań audytowych to opis wymagań jakie powinna spełnić infrastruktura, konfiguracja i dokumentacja systemu cyberbezpieczeństwa po zakończeniu całego działania celem uzyskania dofinansowania.

### 1. Audyt bezpieczeństwa - rekomendacja

Przygotowując architekturę bezpieczeństwa należy wykonać kilka czynności audytowych:
- Audyt infrastruktury - audyt i analiza stanu infrastruktury oraz usług sieciowych świadczonych przez tę infrastrukturę. Czynności audytowe:



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

a) Inwentaryzacja zasobów sprzętowych sieci oraz analiza obecnego stanu sieci pod względem fizycznym i logicznym.
b) Audyt wydajności sieci w kontekście parametrów sieciowych
oraz działających w niej aplikacji.
c) Audyt architektury sieciowej (fizycznej i logicznej).

Wynikiem takiego audytu powinny być zalecenia w zakresie optymalizacji i konfiguracji infrastruktury

- Właściwy audyt bezpieczeństwa oraz analiza zgodności ze standardami. Wynikiem audytu powinny być zalecenia w zakresie cyberbezpieczeństwa i ciągłości działania.

Zakres minimum audytu w zakresie wykonania podstawowego systemu cyberbezpieczeństwa wygląda następująco:

| Nazwa obszaru | Opis |
|---|---|
| Skuteczność działania infrastruktury | – Urządzenia i konfiguracja w zakresie ochrony poczty<br>– Urządzenia i konfiguracja w zakresie ochrony sieci<br>– Urządzenia i konfiguracja w zakresie systemów serwerowych<br>– Urządzenia i konfiguracja w zakresie stacji roboczych<br>– Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa |
| Procesy zarządzania bezpieczeństwem informacji | – Nośniki wymienne – udokumentowany sposób podstępowania<br>– Zarządzanie tożsamością / dostęp do systemów w zakresie:<br>○ Przydzielanie dostępu<br>○ Odbieranie dostępu<br>– Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję OUK (Dz.U. 2019 poz. 2479) |
| Monitorowanie i reagowanie na incydenty bezpieczeństwa | – Procedury zarządzania incydentami<br>– Raportowanie poziomów pokrycia scenariuszami znanych incydentów<br>– Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa<br>– Monitorowanie i wykrycie incydentów bezpieczeństwa<br>– Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów |
| Zarządzanie ciągłością działania | – Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa<br>– Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa<br>– Procedury wykonywania i przechowywania kopii zapasowych<br>– Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP)<br>– Procedury utrzymaniowe |
| Utrzymanie systemów informacyjnych | – Harmonogramy skanowania podatności<br>– Aktualny status realizacji postępowania z podatnościami<br>– Procedury związane ze z identyfikowaniem (wykryciem) podatności<br>– Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami |
| Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług | – Polityka bezpieczeństwa w relacjach z dostawcami<br>– Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa<br>– Dostęp zdalny<br>– Metody uwierzytelnienia |



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

## 2. Firewall - zapora sieciowa z wbudowanym IPS oraz systemem antywirusowy

Ochronę sieci należy zaprojektować w oparciu o potrzeby jednostki biorąc pod uwagę takie parametry jak:

- oczekiwana dotyczących przepustowość brzegu sieci

- liczba osób pracujących zdalnie z wykorzystaniem VPN

,- liczba zestawionych tuneli IPSec.

- liczba usług wystawianych na zewnątrz organizacji

- liczba jednoczesnych sesji

Uwaga: parametry zaznaczone szarym tłem należy dobrać do potrzeb jednostki.

Rekomendowane są następujące funkcjonalności urządzeń (oprogramowania) tego typu (w miarę posiadanych środków należy dążyć do układów w klastrze):

a) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active i Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
c) Monitoring stanu realizowanych połączeń VPN.
d) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
e) System realizujący funkcję Firewall musi dysponować interfejsami (liczbę i parametry maksymalne należy dostosować do potrzeb):
    (1) Gigabit Ethernet RJ-45.
    (2) SFP 1 Gbps.
    (3) SFP+ 10 Gbps (opcje zależne od potrzeb).
f) System Firewall musi posiadać wbudowany port konsolowy oraz gniazdo USB oraz instalacji oprogramowania z klucza USB.
g) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
h) System realizujący funkcję Firewall powinien być podłączony do systemu zbierania logów z odpowiednią przestrzenią dyskową, która umożliwi przetrzymywanie logów i ruchu sieciowego co najmniej 3 miesiące wstecz (ruch sieciowy) oraz 12 miesięcy wstecz (logi systemu).
i) W zakresie Firewall 'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę (opcje zależne od potrzeb).
j) Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B (opcje zależne od potrzeb).
k) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 10 Gbps (opcje zależne od potrzeb).
l) Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps (opcje zależne od potrzeb).



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

m) Wydajność skanowania ruchu w celu ochrony przed atakami z zewnątrz i wewnątrz (ochrona IPS) minimum 5 Gbps (opcje zależne od potrzeb).
n) Wydajność skanowania z włączonymi funkcjami: IPS, Application Control, Antywirus, Web Filter minimum 3 Gbps (opcje zależne od potrzeb).
o) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu https minimum 4 Gbps (opcje zależne od potrzeb).
p) W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:
    (1) Ochrona IPS,
    (2) Ochrona antywirusowa/malware co najmniej dla protokołów SMTP, SMTPS, POP3, IMAP, IMAPS, HTTP, HTTPS, FTP.
    (3) Kontrola Aplikacji,
    (4) Kontrola stron WWW,
    (5) Kontrola zawartości poczty (ochrona przed spamem),
    (6) Ochrona przed sieciami botnet,
    (7) Kontrola zapytań DNS,
    (8) Deszyfracja SSL (Inspekcja ruchu szyfrowanego),
    (9) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    (10) Zarządzanie pasmem (QoS, Traffic shaping).
q) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
r) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
s) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
t) Analiza ruchu szyfrowanego protokołem SSH.
u) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
v) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń i rejestrowanie zdarzeń.
w) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    (1) Translację jeden do jeden oraz jeden do wielu.
    (2) Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.
x) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
y) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
z) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    (1) Wsparcie dla IKE v1 oraz v2.
    (2) Obsługa szyfrowania protokołem minimum AES z kluczem 128 i 256 bitów
    (3) Obsługa protokołu Diffie-Hellman minimum grup 19 i 20.
    (4) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    (5) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    (6) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    (7) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    (8) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
aa) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:


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

(1) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki.
(2) Pracę w trybie tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
(3) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

bb) W zakresie routingu rozwiązanie powinno zapewniać minimum obsługę:
(1) Routingu statycznego.
(2) Policy Based Routingu.
(3) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

cc) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

dd) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

ee) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

ff) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

gg) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

hh) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

ii) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, rar.

jj) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.

kk) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz DOC i pokrewnych

ll) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

mm) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

nn) Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

oo) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

pp) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

qq) Mechanizmy ochrony dla aplikacji Webowych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

rr) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

ss) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

tt) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

uu) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

vv) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

ww) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

xx) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.



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

yy) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

zz) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.

aaa) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

bbb) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url system nie będzie dokonywał deszyfracji SSL w komunikacji.

ccc) System Firewall musi umożliwiać weryfikację tożsamości użytkowników minimum za pomocą:

(1) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
(2) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
(3) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
(4) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

ddd) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem usług katalogowych oraz zastosowanie innych mechanizmów: RADIUS lub API.

eee) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

fff) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

ggg) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.

hhh) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

iii) Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

jjj) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

kkk) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

lll) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

mmm) Musi istnieć możliwość logowania do serwera SYSLOG.

nnn) W komplecie z urządzeniem muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

(1) Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres nie krótszy niż 12 miesięcy.



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

**3. Chmurowy system ochrony LAN/WAN**

A. Charakterystyka systemu:

- System jest rozwiązaniem chmurowym
- Rozwiązanie jest niezależne od stosowanych portów i protokołów
- Rozwiązanie daje możliwość wdrożenia zarówno w sieciach ze stałym jak i ze zmiennym adresem publicznym IP
- Rozwiązanie działa na rekordach DNS typu: A, AAAA, ANY, CNAME, PTR, SRV i TXT
- Rozwiązanie umożliwia stosowanie lokalnych serwerów DNS
- Klasyfikacja zagrożeń opiera się o mechanizmy uczenia maszynowego wykorzystujące globalnie zbierane informacje o domenach, adresach IP oraz systemach autonomicznych BGP (ASN)
- Rozwiązanie umożliwia zainstalowanie sieciowego forwardera zapytań DNS pozwalającego na szyfrowane przesyłanie zapytań oraz odpowiedzi DNS od klienta do chmury a także z chmury do klienta
- Instalacja forwardera DNS nie wymaga instalacji sprzętu fizycznego
- Funkcjonalność forwardera DNS nie jest dodatkowo licencjonowana w stosunku do bazowej funkcjonalności systemu tj. blokowania zapytań DNS do domen sklasyfikowanych jako niebezpieczne
- System umożliwia integrację systemu z Usług Katalogowych (AD) do granularyzacji polityk per grupa użytkowników oraz pełnej widoczności w generowane przez użytkowników zapytania DNS
- Rozwiązanie może obejmować swoją ochroną zarówno urządzenia pracujące wewnątrz sieci klienta, jak również komputery przenośne z systemami Windows i MacOS będące poza siecią firmową
- Funkcjonalność ochrony komputerów przenośnych znajdujących się poza siecią firmową (zaufaną) nie jest dodatkowo licencjonowana w stosunku do bazowej funkcjonalności systemu tj. blokowania zapytań DNS do domen sklasyfikowanych jako niebezpieczne
- Funkcjonalność ochrony komputerów przenośnych znajdujących się poza siecią firmową (zaufaną) może być zrealizowana poprzez:
  - instalację dedykowanego oprogramowania (agenta typu standalone) na stacji końcowe

B. Mechanizmy bezpieczeństwa

- System umożliwia blokowanie zapytań DNS skorelowanych z domenami o niebezpiecznej treści, w tym:
  - zapytań DNS skorelowanych z domenami wykorzystywanymi do propagacji złośliwego oprogramowania
  - zapytań DNS skorelowanych z domenami wykorzystującymi mechanizm typu Phishing
  - domen wykorzystywanych do nawiązywania połączeń typu Command and Control
  - zapytań DNS do domen powiązanych z aktywnościami typu Botnet
  - zapytań DNS do nowo powstałych domen tzw. „newly seen domains”
  - zapytań DNS do domen powiązanych z wydobywaniem walut wirtualnych tzw. Cryptomining
- Funkcjonalność blokowania zapytań DNS realizowana jest bez konieczności instalacji sprzętu fizycznego



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

- System umożliwia blokowanie zapytań DNS bazując na informacjach dostarczonych ze źródeł zewnętrznych w tym m.in.:
  - Splunk
  - Anomalii
- System umożliwia blokowanie zapytań DNS bazując na dedykowanych listach domen z wykorzystaniem mechanizmu API
- System umożliwia tworzenie listy domen dopuszczanych i listy domen zabronionych przez administratora systemu
- System umożliwia dodawanie polityk związanych z filtracją treści odwiedzanych przez użytkowników domen
- System umożliwia blokowanie zapytań C2 (bezpośrednio do IP) które omijają kanał DNS
- System zapewnia możliwość integracji z systemem XDR tego samego producenta. Integracja nie wymaga dodatkowych licencji i jest zawarta w cenie rozwiązania Chmurowego Systemu Ochrony LAN/WAN.
- System umożliwia głęboką analizę ruchu z wykorzystaniem silnika IPS
- System umożliwią inspekcję online ruchu webowego oraz aplikacji cloud'owych wykorzystującą silnik DLP
- System umożliwia dekrypcję oraz inspekcję ruchu SSL (HTTPS)
- System umożliwia analizę próbek złośliwego oprogramowania (bez limitu próbek na dzień) w systemie sandbox tego samego producenta co Chmurowy System ochrony LAN/WAN
- System zawiera funkcjonalność komponentu chmurowego proxy
- System funkcjonalność komponentu chmurowego firewalla L3/L4

C. Funkcjonalność Cloud Access Security Broker (CASB)
   - System pozwala na wykrywanie oraz blokowanie tzw. Shadow IT (bazując na domenach)

D. Funkcjonalność bezpiecznej bramy internetowej
   - System umożliwia filtrowanie ruchu internetowego (web) w oparciu o domenę lub kategorię domen
   - Z wykorzystaniem funkcjonalności selektywnego proxy system umożliwia:
     - dekrypcję i inspekcję ruchu SSL (HTTPS)
     - blokowanie URL bazując na dedykowanym ośrodku badawczym producenta (tzw. Security Intelligence) oraz źródłach zewnętrznych
     - blokowanie plików bazując na silniku antywirusowym oraz informacjach pochodzących z rozwiązania do ochrony stacji końcowych (natywna integracja) tego samego producenta co Chmurowy System Ochrony LAN/WAN

E. Mechanizmy przesyłania ruchu
   - System umożliwia przekazywanie zewnętrznych zapytań DNS do analizy w celu ochrony urządzeń znajdujących się wewnątrz sieci lokalnej z wykorzystaniem natywnej integracji z urządzeniami sieciowymi oraz UTM tego samego producenta

F. Informacje o użytkownikach



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

- System umożliwia tworzenie polityk oraz przeglądanie raportów w oparciu o:
  - publiczny adres IP
  - podsieć prywatną
  - urządzenie sieciowe (włączając VLAN oraz SSID dla integracji opisanych w pkt. 4)
  - przynależność do grupy Usług Katalogowych (włączając konkretnych użytkowników)

G. Zarządzanie

- System zawiera panel do zarządzania politykami, przeglądania i analizy logów w formie graficznej, dostępny jako portal webowy znajdujący się w chmurze. Witryna jest kompatybilna z przeglądarkami (w dwóch ostatnich wersjach/aktualizacjach) na stacjach Windows, OS X oraz Linux (zgodnie z ich dostępnością):
  - Edge
  - Safari
  - FireFox
  - Chrome
- System umożliwia stworzenie dedykowanej i spersonalizowanej strony blokowania która jest wyświetlana użytkownikom w momencie zablokowania dostępu do domeny:
  - możliwe jest wprowadzenie komunikatu w języku polskim
  - możliwe jest wprowadzenie grafiki tj. logo organizacji
- System umożliwia tworzenie, odczytywanie, aktualizacje i usuwanie obiektów konfiguracyjnych z wykorzystaniem API zgodnym z pryncypiami RESTful

H. Raportowanie oraz logi

- System umożliwia przeglądanie informacji i logów w czasie rzeczywistym
- System umożliwia utworzenie raportu dającego wgląd w usługi chmurowe wykorzystywane przez użytkowników wraz ze statystykami wykorzystania konkretnych serwisów
- System umożliwia utworzenie raportu pokazującego ilość konkretnych zapytań DNS, które zostały zablokowane wraz z ich kategorią – Malware, C&C, Phishing
- System umożliwia wgląd w ilość zapytań DNS generowanych przez użytkowników sieci do konkretnej domeny
- System umożliwia filtrowanie logów pod kątem:
  - dnia i godziny
  - adresu lokalnego użytkownika
  - nazwy użytkownika z AD
  - konkretnej domeny
  - kategorii bezpieczeństwa pod którą domena została skategoryzowana
- Rozwiązanie daje możliwość obrazowania ilości zapytań DNS w funkcji czasu w formie grafów
- Rozwiązanie umożliwia automatyczne generowanie określonych przez administratora raportów przy użyciu kalendarza
- Administrator ma możliwość pobrania raportu aktywności w rozszerzeniu .csv
- Panel administratora daje możliwość przeglądania wszystkich zapytań pochodzących z sieci i urządzeń pracowników zdalnych przez okres 30 dni
- System daje możliwość wyeksportowania logów z dashboardu znajdującego się w chmurze



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

- System umożliwia interakcję z komponentami zewnętrznymi oraz integrację za pośrednictwem REST API

I. Skalowalność i możliwości rozbudowy
   - System umożliwia zwiększenie ilości użytkowników i urządzeń objętych ochroną wraz ze wzrostem potrzeb organizacji w przyszłości poprzez dokupienie dodatkowych licencji
   - System umożliwia rozszerzenie funkcjonalności bezpieczeństwa o komponent interaktywnej analizy zagrożeń pozwalający na obserwację globalnych trendów zapytań DNS oraz szczegółową analizę i obserwację powiązań pomiędzy domenami, adresami IP i plikami w celu szybkiej analizy zagrożeń

J. System umożliwia interaktywną analizę zagrożeń pozwalając na obserwację globalnych trendów zapytań DNS oraz szczegółową analizę i obserwację powiązań pomiędzy domenami, adresami IP i plikami w celu szybkiej analizy zagrożeń i w ramach powyższego zapewnia:
   - Dostęp do internetowego interfejsu użytkownika dla 5 użytkowników
   - Interfejs API pozwalający na zasilenie systemów zewnętrznych informacjami o domenach, adresach IP i URL
   - Dostęp do danych z rekordów WHOIS
   - Informacje o geograficznym rozkładzie zapytań DNS do analizowanej domeny
   - Informacje o liczbie zapytań DNS w skali czasu dla analizowanej domeny
   - Informacje o subdomenach dla analizowanej domeny macierzystej
   - Informacje o domenach współwystępujących tj. domenach odwiedzanych przed lub po odwiedzeniu domeny macierzystej (w celu rozpoznania infrastruktury atakującego)
   - Możliwość przeszukiwania informacji o domenach za pomocą wyrażeń regularnych
   - Informacje o próbkach złośliwego oprogramowania powiązanych z analizowaną domeną a w tym:
     - SHA256 pliku
     - SHA1 pliku
     - MD5 pliku
     - wskaźniki behawioralne pliku opisujące szczegółowo listę złośliwych aktywności powiązanych z plikiem

K. Dostępność i prywatność danych
   - Dostawca usługi posiada infrastrukturę rozproszoną składającą się Centrów (CPD) Przetwarzania Danych w Ameryce Północnej, Ameryce Południowej, Afryce, Azji, Australii i Europie zapewniając tym samym wysoką i bezprzerwową dostępność usługi
   - Dostawca usługi posiada infrastrukturę rozproszoną składającą się Centrów Przetwarzania Danych przynajmniej w dziesięciu krajach w Europie zapewniając tym samym wysoką i bezprzerwową dostępność usługi
   - Dostawca usługi posiada infrastrukturę (CPD) na terenie Polski



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

# 4. System kopii bezpieczeństwa

Powszechnie wiadomo, że kopie bezpieczeństwa wykonywane są na wypadek awarii systemu zawierającego dane. Dane są różne i należy do nich podchodzić indywidualnie. Czynniki, które należy brać pod uwagę, to między innymi: dostępny budżet, krytyczność aplikacji, wymagania biznesowe, co do długości przechowywania danych (właściciel aplikacji może mieć ważny głos jak długo i jak często wymaga zabezpieczania swoich danych). Niektóre dane mogą wymagać wykonywania backupów z dużą częstotliwością. Wiemy także, że niektóre dane się nie zmieniają (np. obrazy ISO, programy instalacyjne, różnego rodzaju skany) i nie musimy ich wcale backupować. Liczba przechowywanych kopii jest niezwykle ważna z punktu widzenia budżetu potrzebnego na repozytorium danych. Jeżeli repozytorium jest małe to możemy skrócić retencję lub ilość backupowanych danych. Czasami różnego rodzaju wymogi prawne mogą wymuszać przechowywanie danych przez kilka lat. Można wtedy wykonać tzw. „tiering backupów" – oznacza to, że krótkoterminowe backupy przenosimy na lokalne (szybsze i droższe) repozytorium, a backupy długoterminowe na tańsze (tam, gdzie ponosimy mniejszy koszt za każdy GB przechowywanych danych) np. na deduplikator, do chmury lub na taśmy. Podobnie z lokalizacją backupów – te krytyczne, których utrata będzie najbardziej bolesna - zapisujemy w kilku miejscach. Dane mniej ważne czasami wystarczy skopiować do jednego repozytorium. Bardzo ważne jest, aby przynajmniej jedna z kopii zapasowych była przechowywana poza siedzibą przedsiębiorstwa. Nietrudno sobie wyobrazić działanie pożaru lub wody, które niszczą firmowe budynki w tym serwerownie. W takiej sytuacji pomimo posiadania kilku kopii, dodatkowo (co ważne!) wykonanych na kilku różnych nośnikach, może się okazać, że żadna z nich nie nadaje się do użytku. Wówczas możemy sięgnąć po kopię, która przechowywana była w fizycznie innym miejscu.

System kopii bezpieczeństwa powinien zostać zaprojektowany w sposób pozwalający na odtworzenie zasobów jednostki po awarii systemów produkcyjnych lub ataku szyfrującego dane. Dlatego komponenty wchodzące w skład systemu nie powinny brać udziału w produkcyjnym działaniu jednostki. Standardowo są to oddzielne od produkcyjnych urządzenia pracujące w wydzielonej, zabezpieczonej podsieci.

Pojemność i funkcjonalność systemu kopii, liczba i wielkość urządzeń zależą od ilości danych systemów produkcyjnych, czasów odtwarzania RTO i RPO oraz od technologii użytkowanych w systemach produkcyjnych takich jak wirtualizatory, relacyjne bazy danych. Ważnym elementem wpływającym na wielkość systemu kopii bezpieczeństwa jest harmonogram wykonywania kopii bezpieczeństwa oraz rodzaj kopii (codzienne pełne kopie, codzienne kopie przyrostowe, a tygodniowe pełne, etc.). Kolejnym czynnikiem mającym wpływ na pojemność systemu kopii bezpieczeństwa są regulacje formalne dotyczące okresu przechowywania danych. Minimalna pojemność systemu (łącznie urządzenia dyskowe i taśmowe) kopii powinna być **szacunkowo sześciokrotnie większa od wielkości zasobów produkcyjnych objętych systemem, o ile system kopii bezpieczeństwa nie używa mechanizmów deduplikacji danych**.

Parametryzacja systemu kopii bezpieczeństwa powinna być przedmiotem analizy. W analizie należy uwzględnić wymienione wyżej aspekty

W skład rekomendowanego systemu kopii bezpieczeństwa wchodzą:



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

1. Oprogramowanie systemu kopii bezpieczeństwa.
2. Serwer zarządzający wykonywaniem kopii (na przykładowym schemacie nazwanym Cell Manager).
3. Serwer posiadający dostęp do urządzeń przechowujących dane (na przykładowym schemacie Media Agent).
4. Urządzenie dyskowe do przechowywania danych. W zależności od zastosowanego oprogramowania będą to dyski w serwerze, macierz dyskowa, deduplikatory.
5. Biblioteka taśmowa LTO6.

Minimalne funkcjonalności systemu kopii bezpieczeństwa:

1. Harmonogramowanie wykonania kopii.
2. Możliwość wykonywania kopii typu snapshot.
3. Możliwość wykonywania kopii bezpieczeństwa na różne nośniki danych (urządzenia dyskowe, taśmy LTO)
4. System musi posiadać funkcjonalność wykonywania kopii on-line wykorzystywanych w instytucji; baz danych.
5. Zarządzanie przechowywanymi danymi, kopie wykonanych zadań pomiędzy nośnikami, retencja danych.

## 3.1 Scenariusze wdrożeniowe

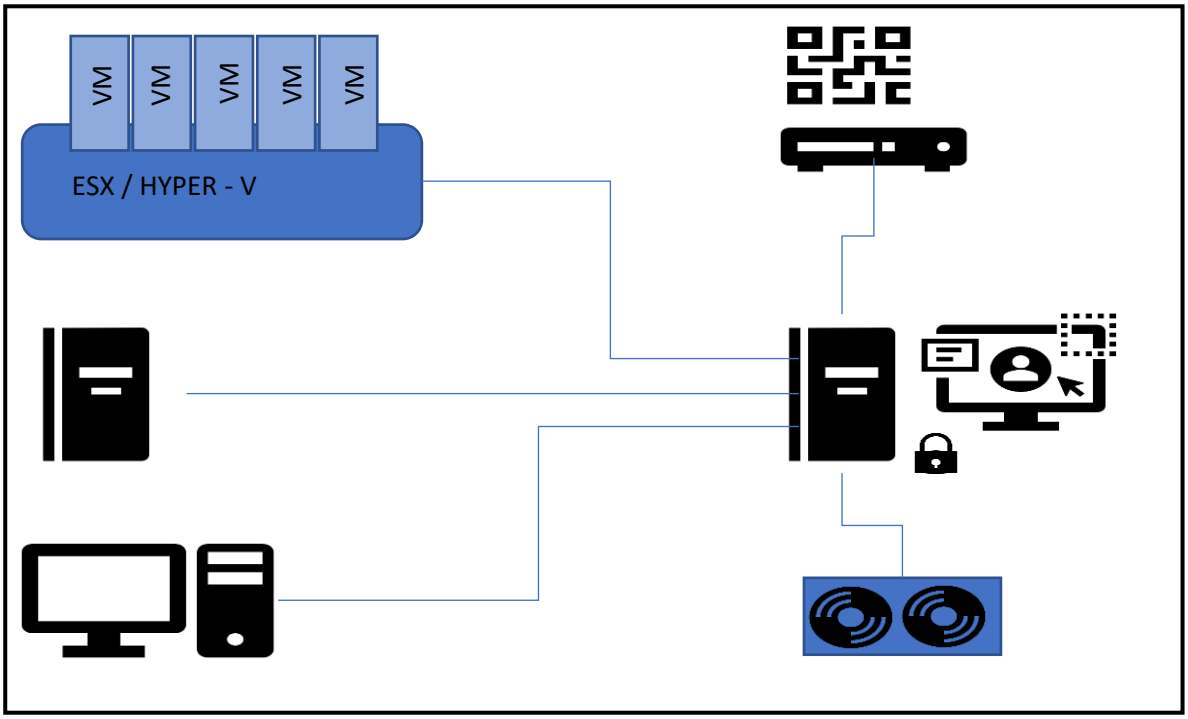
Scenariusze wdrożenia są podzielone na trzy kategorie, w zależności od wielkości lokalizacji i ilości danych które należy zabezpieczyć. Architektury referencyjne dla tych kategorii zapewniają ogólne wytyczne dotyczące tego, jak i gdzie należy wdrażać i podłączać komponenty infrastruktury kopii zapasowych i bloki konstrukcyjne, szacowane rozmiary i im odpowiadająca konfiguracja sprzętowa została przyjęte dla środowisk małych, średnich i dużych. Środowiska te mogą zawierać wirtualizatory oraz maszyny fizyczne (serwery, stacje robocze, laptopy).

### Opis architektury

W każdej zabezpieczanej jednostce zlokalizowane są (jak na poniższym rysunku) co najmniej dwa aktywne komponenty kopii zapasowych. Serwer zarządzający, którego zadaniem będzie koordynacja wszystkich zadań, zdalna instalacja komponentów infrastruktury zabezpieczającej, odbieranie kopii zapasowych ze środowiska produkcyjnego i przekazywanie ich do bezpiecznych repozytoriów dyskowych. Serwer zarządzający koordynuje również przesyłanie zabezpieczonych danych na napędy taśmowe. Druga maszyna – składująca dane na urządzeniach dyskowych/dyskach w serwerze – jest odpowiedzialna za bezpieczne przechowywanie danych. Jej dostępność w sieci jest ograniczona do niezbędnego minimum pozwalającego na wykonywanie i zarządzanie kopiami bezpieczeństwa.. Systemy kopii bezpieczeństwa powinny być odseparowane od systemów produkcyjnych, poprzez stosowanie wewnętrznych firewall-i , VLAN-ów z kontrolą ruchu sieciowego.



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




Serwer zarządzający kopią zapasowej musi mieć możliwość połączenia się z repozytorium dyskowym przez sieć IP – zalecane 1Gbps Serwer składujący dane wyposażony być w interfejsy Ethernet 10 Gb i FC 16Gb  Podobne łącze jest rekomendowane przy odbieraniu zabezpieczanych danych ze środowisk wirtualnych oraz fizycznych. Aby zapobiec manipulowaniu przez oprogramowanie ransomware lub jakiekolwiek inne manipulowanie danymi, kopii zapasowa powinna korzystać z technik blokowania danych na wybrany interwał czasowy lub zapisywać je np. na taśmy magnetyczne ( LTO)  . W celu oszczędności, w małych lokalizacjach komponenty, takie jak serwer backupu, czy serwer monitorowania mogą mieć postać maszyny wirtualnej, na posiadanym wirtualizatorze. Dodatkowa kopia taśmowa powinna być cyklicznie (np. raz na tydzień/miesiąc) umieszczana i przechowywana w bezpiecznej lokalizacji, poza główną serwerownią. Na serwerze zarządzającym można dodatkowo skonfigurować system monitorujący który będzie potrafił wykryć i zaraportować podejrzane aktywności.

System kopii bezpieczeństwa należy zwymiarować zgodnie z potrzebami  organizacji.

## 3.2 Przykładowe scenariusze wdrożenia - mała lokalizacja

### – do 20 maszyn wirtualnych/fizycznych do 3TB danych źródłowych (do 18TB danych w systemie backup)



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

Serwer zarządzający – ogólne wymagania minimalne (opisany szczegółowo dalej jako „serwer zarządzający – mały”):

a. Procesor: 8 rdzeni CPU 2.5 GHz,

b. RAM: 32 GB RAM,

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 2 x Ethernet 1Gb ,

e. Karta zarządzająca/port zarządzania,

Serwer składowania danych i repozytorium dyskowe – wymagania minimalne (opisane szczegółowo dalej jako „repozytorium dyskowe – małe”):

a. Procesor: 8 rdzeni CPU 2.5 GHz

b. RAM: 64 GB RAM,

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 2 x Ethernet 10Gb,

e. Karta rozszerzeń: 2 x FC 16Gb

f. Karta zarządzająca/port zarządzania,

g. System operacyjny zgodny ze środowiskiem urządzenia i systemem kopii bezpieczeństwa

h. Macierz dyskowa do składowania danych z kartami Ethernet i FC

i. Biblioteka taśmowa: 1x LTO8 , liczba slotów: 40 szt.

## 3.3 Przykładowe scenariusze wdrożenia - średnia lokalizacja

## – do 50 maszyn wirtualnych/fizycznych, do 6TB danych źródłowych (do 32TB danych w systemie backup przed deduplikacją)

Serwer zarządzający – ogólne wymagania minimalne (opisany szczegółowo dalej jako „serwer zarządzający – średni”):

a. Procesor: 8 rdzeni CPU 2.5 GHz,

b. RAM: 64 GB RAM,

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 2 x Ethernet 1Gb,



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

e. Karta zarządzająca/port zarządzania,

Serwer składowania danych i repozytorium dyskowe – wymagania minimalne (opisane szczegółowo dalej jako „repozytorium dyskowe – średnie”):

a. Procesor: 8 rdzeni CPU 2.5 GHz

b. RAM: 64 GB RAM,

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 2 x Ethernet 10Gb,

e. Karta rozszerzeń: 2 x FC 16Gb

f. Karta zarządzająca/port zarządzania,

h. Urządzenie dyskowe ze sprzętowym wsparciem dla deduplikacji danych o pojemności netto 32TB (przed deduplikacją)do składowania danych z kartami min 2x Ethernet 10 Gb i FC 16Gb

i. Biblioteka taśmowa: 2 x LTO8 , liczba slotów: 40 szt.

## 3.4 Przykładowe scenariusze wdrożenia – duża lokalizacja

## – powyżej 50 maszyn wirtualnych/fizycznych do 20TB danych źródłowych (do 52TB danych w systemie backup przed deduplikacją)

Serwer zarządzający – ogólne wymagania minimalne (opisany szczegółowo dalej jako „serwer zarządzający – duży”):

a. Dwa procesory: każdy 8 rdzeni CPU 2.5 GHz,

b. RAM: 128 GB RAM,

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 2 x Ethernet 1Gb

e. Karta zarządzająca/port zarządzania,

Serwer składowania danych i repozytorium dyskowe – wymagania minimalne (opisane szczegółowo dalej jako „repozytorium dyskowe – duże”):

a. Procesor: 8 rdzeni CPU 2.5 GHz

b. RAM: 54 GB RAM,



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

c. Dyski: 2 x 480GB SSD na system operacyjny w RAID 1,

d. Karta rozszerzeń: 4 x Ethernet 10Gb,

e. Karta rozszerzeń: 2 x FC 16Gb

f. Karta zarządzająca/port zarządzania,

h. Urządzenie dyskowe ze sprzętowym wsparciem dla deduplikacji danych o pojemności netto 52TB (przed deduplikacją) do składowania danych z kartami min 4 x Ethernet 10 Gb i FC 16Gb

i. Biblioteka taśmowa: 4 x LTO8 , liczba slotów: 40 szt.

## 3.5 Przykładowe przydatne, funkcje oprogramowania kopii zapasowej.

Każdorazowo przy wyborze systemu kopii zapasowej należy uwzględnić produkcyjne oprogramowanie wykorzystywane przez podmiot i do posiadanej infrastruktury dobrać system kopii bezpieczeństwa, uwzględniając wymagania wymienione w punkcie systemy kopii bezpieczeństwa.

Zgodnie z powyższymi założeniami rekomendowane są następujące funkcjonalności środowiska systemu kopii zapasowej:

- Współpraca z infrastrukturą posiadanych przez podmiot systemów wirtualizacji.
- Oprogramowanie powinno posiadać mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek innych funkcjonalności oprogramowania kopii bezpieczeństwa.
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji systemu kopii bezpieczeństwa.
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła, szyfrowanie transmisji.
- Oprogramowanie powinno posiadać możliwość wykorzystywania mechanizmu Change Block Tracking platform wirtualizacyjnych podczas realizacji kopiii.
- Oprogramowanie musi posiadać mechanizm wykonywania kopii bezpieczeństwa ze snapshotów systemów wirtualizacyjnych posiadanych przez podmiot.
- Oprogramowanie musi posiadać agentów baz danych posiadanych przez podmiot do wykonywania online-owych kopii bezpieczeństwa.
- Oprogramowanie musi wspierać kopiowanie backupów na taśmy bezpośrednio z systemów operacyjnych jak również ze składowanych kopii na urządzeniach dyskowych.
- Oprogramowanie musi posiadać mechanizmy ustawiania harmonogramu wykonywania kopii bezpieczeństwa.
- Oprogramowanie musi umożliwiać wykonywanie kopii przyrostowej i pełnej.



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

## 3.7 Ochrona środowiska backupu

### 3.7.1 Automatyzacja procesów backupu i odzyskiwania po awarii

Awaria to zawsze sytuacja stresująca, podczas której łatwo popełnić błąd. Dlatego warto zautomatyzować jak najwięcej procesów backupu oraz odtwarzania. Można tu wykorzystać wszelkiego rodzaju tagi, które będą automatycznie dodawały nowopowstały zasób do polityki backupowej. Aby móc polegać na naszych backupach koniecznym jest cyklicznie je weryfikować w innym niż produkcyjne środowisko– czy w razie awarii możemy na nich polegać i odzyskać dane. Taką weryfikację również można zautomatyzować tak, aby np. każdy weekendowy backup był przetestowany pod kątem odtwarzalności danych. Specjaliści powtarzają jak mantrę, że sam backup to za mało. Dopiero pewność tego, że dane da się szybko i w całości przywrócić jest gwarantem bezpieczeństwa. Dlatego tak ważnym aspektem jest testowanie wykonywanych kopii pod kątem zdolności przywrócenia danych. Zalecane jest utworzenie procedur odtwarzania danych, a proces weryfikacji po wykonanym odtworzenia z kopii bezpieczeństwa powinien mieć odzwierciedlenie w protokołach potwierdzających wykonane zadania.

# 4. Bezpieczna poczta elektroniczna

Rekomendowana jest poczta elektroniczna jako usługa. Na rynku dostępnych jest wielu dostawców usług pocztowych. Należy jednak zwrócić uwagę na dwa podstawowe parametry takiej usługi: MFA – wieloskładnikowe uwierzytelnianie oraz usługi bezpieczeństwa skrzynek pocztowych (antywirus, antymalware). Zaleca się wykorzystanie usług pocztowych w chmurze.

### 4.1 Poczta on-line – specyfikacja parametrów funkcjonalnych

- Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych
- Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata
- Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami
- Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia
- Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

Usługa musi umożliwiać:

a. obsługę poczty elektronicznej,
b. zarządzanie czasem,
c. zarządzania zasobami
d. zarządzanie kontaktami i komunikacją.



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

- Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
  a. Zarządzania użytkownikami poczty,
  b. Wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
  c. Wsparcia integracji własnej usługi katalogowej (Usług Katalogowych) z usługą hostowana poczty.
- Dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy:
  - Posiadanego oprogramowania (dedykowany klient poczty elektronicznej – co najmniej jeden),
  - Przeglądarki (Web Access),
  - Urządzeń mobilnych.
- Wymagane cechy usługi to:
  - Skrzynki pocztowe dla każdego użytkownika o pojemności minimum 40 GB,
  - Standardowy i łatwy sposób obsługi poczty elektronicznej,
  - Obsługa najnowszych funkcji klientów pocztowych w wersjach wprowadzonych na rynek w 2019 roku lub później , w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, FireFox i Safari,
  - Współdziałanie z innymi produktami takimi jak - uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy.
  - Bezpieczny dostęp z każdego miejsca, w którym jest dostępny Internet.
- Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich.

## 4.2 Ochrona poczty elektronicznej – specyfikacja parametrów minimalnych

- Usługa musi umożliwiać definiowanie polityk ochrony przed cyberzagrożeniami wraz ustaleniem odpowiedniego poziomu tych zabezpieczeń.
- Kreować raporty o działaniu tego pakietu w czasie rzeczywistym.
- Raportować wykryte zagrożenia, analizować phishingowe adresy i wiadomości.
- Wykrywać, opisywać i symulować cyberzagrożenia dla usługi wraz z możliwością automatyzacji podstawowych działań.
- Eliminować rozpoznane w monitoringu Dostawcy typy zagrożeń.
- Sprawdzać bezpieczeństwo załączników poczty elektronicznej poprzez otwieranie ich i skanowanie zawartości w chronionych środowiskach wirtualnych.
- Sprawdzać bezpieczeństwo linków zawartych w poczcie elektronicznej poprzez otwieranie ich i skanowanie zawartości w chronionych środowiskach wirtualnych.
- Pozwalać na uruchamianie anti-phishingowych polityk sprawdzających zgodność domeny nadawcy.



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

- Pozwalać na tworzenie list bezpiecznych i niebezpiecznych domen.
- Pozwalać na definiowanie standardowych działań na podejrzanych wiadomościach.

## 4.2 Ochrona poczty elektronicznej - System oparty o wykorzystanie usług chmurowych z funkcją zaawansowanego wykrywania malware oraz dwuskładnikowym zabezpieczeniem dostępu do skrzynek.

System ochrony komunikacji e-mail składa się z następujących elementów:

I. Sensory pracujące jako gateway'e MTA (Mail Transfer Agent) do detekcji zagrożeń w ruchu e-mail zlokalizowane w chmurze do obsługi wymaganej liczby skrzynek pocztowych wraz ze wszystkimi usługami subskrypcyjnymi na okres do 3 lat.

II. System sandbox dostępny w chmurze publicznej pozwalający na analizę dynamiczną min 1000 plików (zależnie od liczby skrzynek pocztowych) dziennie z usługami subskrypcyjnymi na okres 3-lat. Wskazane jest, aby system posiadał konsolę graficzną, do której dostęp może mieć co najmniej 3 administratorów z oddzielnie określonymi uprawnieniami.

III. System zabezpieczenia wieloskładnikowego dostępu do skrzynek pocztowych – minimum dwuskładnikowego)

IV. Opcjonalny, nie specyfikowany - Centralny system dla raportowania i kwarantanny zlokalizowany w chmurze ze wszystkimi usługami subskrypcyjnymi na okres 3 lat.

### 4.3.1. Opis funkcjonalny sensorów ochrony poczty elektronicznej

1. System realizuje między innymi następujące funkcje:
   1.1. ochronę przed szkodliwą treścią (m.in. malware, wirusy, phishing etc.),
   1.2. ochronę przed spamem,
   1.3. filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki).
2. System pracuje jako bramka poczty elektronicznej (jako gateway MTA - Mail Transfer Agent) i jest zlokalizowany w chmurze.
3. System umożliwia kontrolę protokołów SMTP oraz ESMTP, w tym szyfrowane wersje tych protokołów z użyciem TLS.
4. System posiada specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej
5. System zapewnia ochronę dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6.
6. Konfiguracja urządzenia możliwa przez:



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

6.1. Interfejs Web: HTTPS,

6.2. CLI: przez SSH,

7. System umożliwia filtrowanie poczty elektronicznej m.in. na podstawie:

7.1. Reputacji IP,

7.2. Reputacji Domeny,

7.3. Wieku Domeny,

7.4. Wyniku SPF, DKIM oraz DMARC,

7.5. Reputacji plików opartej o SHA,

7.6. Linków zawartych w treści lub temacie wiadomości (filtrowanie URL).

8. System zapewnia wsparcie mechanizmów SPF, DKIM oraz DMARC.

9. System zapewnia wsparcie dla S/MIME, TLS oraz DANE.

10. System wspiera przynajmniej jeden dodatkowy niezależny silnik antywirusowy firmy trzeciej bez konieczności wdrażania dodatkowych urządzeń.

11. System umożliwia analizę linków w treści, temacie oraz załącznikach wiadomości e-mail.

12. System wspiera analizę skróconych URL-i w celu wykrycia do jakiej witryny przekierowują.

13. System umożliwia tworzenie filtrów zawartości by dostosować sposób filtrowania wiadomości e-mail.

14. W ramach polityki system umożliwia definiowanie m.in. następujących akcji:

14.1. dostarczenie wiadomości z wykonaniem dodatkowych akcji:

14.1.1. zmodyfikowanie tematu wiadomości,

14.1.2. usunięcie i/lub dodanie nagłówka X-header,

14.1.3. wysłanie kopii wiadomości pod wskazany adres lub adresy email,

14.1.4. przepisanie (potencjalnie) niebezpiecznego linka oraz przekierowanie połączenia do chmurowego proxy producenta, które może ostrzec użytkownika przed zagrożeniem, bądź zablokować połączenie,

14.2. usunięcie załącznika wiadomości,

14.3. zablokowanie wiadomości,

14.4. przekierowanie wiadomości do wskazanej kolejki (kwarantanny),

14.5. wysłanie powiadomienia.

15. System udostępnia mechanizmy analizy i filtrowania oraz zarządzania treścią wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników.

16. System umożliwia filtrowanie i kontrolę treści w oparciu m.in. o:

16.1. słowa kluczowe,



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

16.2. słowniki,

16.3. wyrażenia regularne,

16.4. typ załączników.

17. Kontrola obejmuje m.in. następujące elementy wiadomości:

17.1. tytuł,

17.2. treść,

17.3. nagłówki,

17.4. adres nadawcy,

17.5. adres odbiorcy.

18. System umożliwia wykrywanie dokumentów używających skrypty (tzw. macro) i filtrowanie wiadomości na tej podstawie.

19. System umożliwia budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu z zastosowaniem co najmniej:

19.1. domen email,

19.2. adresów pojedynczych użytkowników.

20. System zapewnia funkcjonalność ochrony przeciwko falom nowych ataków (z ang. Outbreak), działającą niezależnie od silników antywirusowych.

21. System umożliwia przekierowanie wiadomości e-mail do kwarantanny pozwalający na dalszą analizę administratorom i/lub użytkownikom końcowym.

22. Dla kolejki kwarantanny możliwe jest zdefiniowanie jej maksymalnej wielkości oraz czasu, po którym wiadomości będą usuwane.

23. System umożliwia przeniesie wiadomości do kwarantanny dostępnej dla użytkowników końcowych. Użytkownicy końcowi mają możliwość podglądu, usunięcia i uwolnienia wiadomości poddanych kwarantannie.

24. System posiada rozbudowane narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. W tym celu system zapewnia mechanizmy ochrony oparte m.in. na:

24.1. Sygnaturach,

24.2. Słownikach,

24.3. Heurystyce, dla której możliwa jest regulacja czułości (kontrola ilości False-Positives).

25. System umożliwia weryfikację nadawcy wiadomości w oparciu o mechanizm SPF (Sender Policy Framework) oraz podjęcie akcji, m.in.:

25.1. odrzucenie lub przyjęcie wiadomości, jeżeli rekord SPF nie istnieje,

25.2. odrzucenie wiadomości, jeżeli rekord SPF nie pasuje do domeny nadawcy.

26. System umożliwia monitorowanie i ograniczanie liczby jednoczesnych połączeń z jednego adresu IP, ograniczenie maksymalnej liczby wiadomości na jedno połączenie, ograniczenie



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

maksymalnej ilości wiadomości na jednego odbiorcę oraz zdefiniowanie maksymalnego rozmiaru wiadomości.

27. Rozwiązanie pozwala na blokowanie przez określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów.
28. System posiada wbudowany moduł zarządzający i raportujący umożliwiający m.in.
    28.1. Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem (np. codziennie, co tydzień, co miesiąc).
    28.2. Dostarczanie raportów w postaci plików pdf i csv.
    28.3. Dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.
29. System posiada mechanizmy zaawansowanej ochrony antymalware.
30. Mechanizmy zaawansowanej ochrony antymalware obejmują m.in.:
    30.1. Sprawdzenie reputacyjne dla plików przesyłanych przez urządzenie,
    30.2. Aktywną analizę przesyłanych plików przez mechanizm sandboxingu w chmurze publicznej,
    30.3. Monitorowanie wsteczne dla plików już przesłanych.
31. Kontrola reputacji dla plików odbywa się z użyciem ogólnoświatowej bazy reputacji.
32. Kontrola reputacji odbywa się na podstawie unikalnych metadanych własnościowych pliku
    - sprawdzenie reputacyjne nie wymaga przesłania całego pliku na zewnątrz systemu kontroli poczty.
33. Funkcja wysyłania plików przesyłanych pocztą elektroniczną do analizy sandbox jest wbudowana w system ochrony poczty, bez konieczności stosowania zewnętrznych systemów firm trzecich.
34. System ochrony poczty umożliwia wybranie typów plików, które mają być wysłane do systemu sandbox.
35. System ochrony poczty ma wbudowany mechanizm analizy statycznej plików, w wyniku której podejmowana jest decyzja o wysłaniu plików do systemu sandbox. Pliki o bardzo niskim zagrożeniu (np. .docx bez makra) nie będą wysyłane do analizy sandbox.
36. Funkcja monitorowania wstecznego umożliwia informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez urządzenie. Dotyczy to sytuacji, gdy pliki przesyłane pocztą elektroniczną, po przejściu przez systemy ochrony antymalware i sandbox, są uznane za „dobre” lub „nieznane” i przesłane do odbiorcy. System przechowuje o tych plikach informacje (np. w postaci cache hash’y), by w przypadku zmiany dyspozycji (np. na skutek działania ekspertów bezpieczeństwa producenta, informacji zwrotnych od innych klientów itp.) administrator miał pełną świadomość, kto i kiedy takie pliki otrzymał, aby móc łatwo podjąć akcję remediacji.



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

37. System posiada wbudowany co najmniej jeden komercyjny silnik antywirusowy z własną bazą sygnatur.
38. System zawiera moduł DLP (z ang. Data Loss Prevention) umożliwiający identyfikację chronionych informacji m.in. z użyciem mechanizmów:
    38.1. słowa kluczowe,
    38.2. słowniki,
    38.3. wyrażenia regularne,
    38.4. właściwości przesyłanych plików np. rzeczywisty typ pliku, jego nazwa lub rozmiar.
39. System umożliwia przypisanie odpowiedniej wagi znaczenia do różnych słów kluczowych i wyrażeń regularnych.
40. System udostępnia predefiniowane schematy danych dla polityk DLP, np. identyfikacja numerów kont bankowych czy numerów ubezpieczenia społecznego. Schematy mogą być modyfikowane przez administratorów.
41. System umożliwia wydajne szyfrowanie wiadomości bez potrzeby instalacji dodatkowego sprzętu, dzięki integracji z chmurową usługą szyfrowania e-mail oferowaną przez producenta.
42. Wiadomości szyfrowane z użyciem chmurowej usługi producenta nie wymagają dodatkowego oprogramowania na stacji roboczej odbiorcy, są niezależne od klienta pocztowego, systemu operacyjnego oraz urządzenia. Wspierane jest zarówno szyfrowanie w modelu „push" (zaszyfrowana wiadomość jest dostarczona w formacie HTML do samodzielnego otworzenia przez użytkownika) jak i „pull" (użytkownik jest przekierowany do chmurowego portalu by odczytać zabezpieczoną wiadomość).
43. Decyzja o szyfrowaniu może być podjęta przez system na podstawie profilu szyfrowania. Profil ten może określać parametry wiadomości, które powinny być szyfrowane - m.in. „flagi" (np. dotyczące tematu wiadomości), polityki DLP czy dopasowanie do filtra zawartości.
44. System szyfruje wiadomości kluczem szyfrującym, który jest następnie przechowywany w chmurowym serwisie producenta. Odbiorca pozyskuje klucz do odszyfrowania wiadomości z chmury producenta - po uprzedniej rejestracji/uwierzytelnieniu.
45. Usługa szyfrowania zawiera funkcjonalności określenia daty ważności i wycofania wiadomości, a także powiadomienia o przeczytaniu. Te funkcje dostępne są w interfejsie webowym usługi bądź w odpowiednim dodatku (plugin/add-on) do klienta pocztowego.



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

### 4.3.2 System sandbox do dynamicznej analizy plików współpracujący z sensorami ochrony poczty elektronicznej

1. System zapewnia przetwarzanie min. 2000 (liczba zależna od liczby skrzynek pocztowych) próbek na dobę z możliwością rozszerzenia (za pomocą rozszerzenia licencji)
2. Środowisko sandbox w proponowanym rozwiązaniu nie powinno opierać się na mechanizmach emulacji systemów operacyjnych oraz aplikacji, ale na niestandardowym silniku wirtualizacji w celu utrudnienia możliwości jego wykrycia przez złośliwe oprogramowanie
3. Rozwiązanie wspiera nie mniej niż system operacyjny Windows 10 - 64 bitowy.
4. Obraz systemu operacyjnego maszyny wirtualnej nie może być najbardziej aktualny zawierający wszystkie patche. Instalowana jest jedna z najbardziej podatnych na zagrożenia wersji.
5. Analiza dynamiczna konkretnego pliku w systemie sandbox polega na uruchomieniu dedykowanej maszyny wirtualnej dla tego pliku. Wszelkie szczegółowe wyniki analizy dotyczą tylko tego badanego pliku oraz wszystkich jego pochodnych (innych plików wygenerowanych przez badany plik)
6. System obsługuje następujące typy plików:
    - 6.1. .DLL – biblioteki (PE32 i PE32+)
    - 6.2. .EXE – plik wykonywalny PE32
    - 6.3. .JS - JavaScript
    - 6.4. .JSE - encoded JavaScripts
    - 6.5. Pliki Office – (w tym .DOC, .DOCX, .MSG, .RTF, .XLS, .XLSX, .PPT, .PPTX)
    - 6.6. .PDF - Portable Document Format (razem z skryptami Java)
    - 6.7. .PS1 - Powershell
    - 6.8. .VBS - Visual Basic Script
    - 6.9. .ZIP – skompresowane archiwa oraz pliki tzw. kwarantanny
    - 6.10. .BAT - Batch
    - 6.11. .BZ2 – skompresowany bzip2
    - 6.12. .CHM – skompilowany plik pomocy - Ms Compiled HTML Help
    - 6.13. .EML - Wiadomości email zapisane w postaci pliku.
    - 6.14. .GZ – skompresowany gzip
    - 6.15. .HTA – aplikacja HTML
    - 6.16. .ISO - obraz ISO
    - 6.17. .JAR – archiwum Java
    - 6.18. .LNK - Windows shortcut



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

6.19. .MSI - Ms Installer

6.20. . MHTML - Mime HTML

6.21. . SEP - Tagged Image File Format

6.22. .SLK - Ms Symbolic Link (SYLK)

6.23. .SWF - Flash Files

6.24. .TAR - tar

6.25. Podawanie URLi do obiektów znajdujących się na Internecie

6.26. .VBE - Encoded Visual

6.27. . VBN - Virus Bin

6.28. .WSF - Windows Script File

6.29. .XML - XML Based Office Document Types (.DOCX, .XLSX, .PPTX) oraz Extensible Markup Language (.XML)

6.30. . XPS – XML Paper Specification

6.31. . XZ – skompresowane archiwum

7. Rozwiązanie sandboxingu jest w stanie zidentyfikować pliki i powiązać wyniki analizy przeszukując bazę danych zawierającą wyniki poprzednich analiz innych próbek oraz globalne informacje o zagrożeniach dostarczone przez producenta rozwiązania. Poszukiwanymi elementami są:

7.1. adresy IP wykorzystywane w komunikacji podczas detonacji

7.2. domeny wykorzystywane w komunikacji podczas detonacji

7.3. adresy URL wykorzystywane w komunikacji podczas detonacji

7.4. wskazania behawioralne

7.5. ścieżka

7.6. nazwa pliku

7.7. suma kontrolna: SHA256, SHA1, MD5

7.8. unikalny identyfikator przypisany podczas przesyłania plików do urządzenia sandboxingu

7.9. tagi

7.10. mutex

7.11. artefakty pobrane podczas analizy

7.12. rejestrowanie zdarzeń związanych z analizą plików

8. System sandbox analizując całą aktywność pliku porównuje każde pojedyncze jego zachowanie do swoich wbudowanych wskaźników zainfekowania systemu operacyjnego (Indication of Compromise). Poziom zagrożenia wyrażony jest dodatkowo czterema flagami: niski, średni, wysoki, krytyczny.



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

9. Liczba wskaźników zainfekowania systemu operacyjnego bazujących na elementach kodu jak i analizie zachowań wynosi ponad 2000.
10. System umożliwia użytkownikowi ręczne przesłanie pliku do analizy tak, by plik ten i wynik jego analizy były widoczne tylko dla tego użytkownika i były niewidoczne dla pozostałych użytkowników systemu sandbox z tej samej organizacji.
11. System umożliwia ponowne przesłanie pliku, który jest już obecny w systemie w celu próby ujawnienia nowych informacje o złośliwym kodzie i jego zachowaniu
12. Wszystkie informacje dotyczące analizy zagrożeń są dostępne i przeszukiwalne we wszystkich raportach z dostępnych analiz. System umożliwia przeszukiwanie danych o zagrożeniach za pomocą następujących elementów:
    - 12.1. artefakty
    - 12.2. domeny
    - 12.3. adresy IP
    - 12.4. ścieżki
    - 12.5. klucze rejestru
    - 12.6. adresy URL
    - 12.7. wskaźniki zagrożeń (Indication of Compromise)
13. Wszystkie wskaźniki zainfekowania systemu operacyjnego są opisane w taki sposób, aby obejmowały następujące informacje:
    - 13.1. nazwa wskaźnika
    - 13.2. opis
    - 13.3. kategoria
    - 13.4. znaczniki (tagi)
    - 13.5. poziom zagrożenia związany z tym wskaźnikiem
    - 13.6. pewność detekcji
    - 13.7. listę URL znalezionych w dokumentach
    - 13.8. informacje na temat artefaktów, ścieżek do plików, domen, z którymi program się komunikuje.
14. Każdy mechanizm opisujący szkodliwe zachowanie lub typową dla szkodliwego kodu charakterystykę struktur w danym pliku opisany w kilku zdaniach tak, aby w łatwy i przyjazny sposób można było zrozumieć na czym polega dane zagrożenie. Dodatkowo każde wykrycie powinno zawierać fragmenty pliku lub kodu, które by potwierdzały wykorzystanie danego mechanizmu w analizowanej próbce
15. System umożliwia pobranie nagrania ekranu wideo z procesu detonacji plików w celu sprawdzenia aktywności pulpitu



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

16. Oferowane rozwiązanie pozwala na różne opcje integracji z rozwiązaniami firm trzecich (bram sieciowych, serwerów proxy, systemy SIEM, itp.) na wielu poziomach dostępu do informacji poprzez moduły API:

    16.1. udostępnianie informacji o zagrożeniach przychodzących w formie subskrypcji (feeds)

    16.2. dostarczanie raportów z analizy pliku

### 4.3.3 System zabezpieczenia dwuskładnikowego dostępu do skrzynek pocztowych

1. Konsola zarządzania systemem oraz panel administracyjny znajdują się w chmurze.
2. Wszystkie komponenty rozwiązania oraz zbierane dane nie opuszczają terytorium UE, a retencja danych to jeden rok.
3. Rozwiązanie zbiera minimalną ilość informacji o użytkowniku pozwalającą na świadczenie usługi, a szczegółowe wytyczne w kwestii danych przetwarzanych przez dostawcę są udostępnione w formie oficjalnego dokumentu.
4. Ze względów bezpieczeństwa system rozdziela pierwszy oraz drugi składnik uwierzytelnienia w ten sposób, że:
    4.1. pierwszy składnik uwierzytelnienia przetrzymywany jest w ramach wyodrębnionego systemu trzeciego IdP tzw. (Identity Provider)
    4.2. drugi składnik uwierzytelnienia przetrzymywany jest w ramach osobnego i niezależnego systemu dostarczanego z chmury
    4.3. kompromitacja systemu przetrzymującego pierwszy składnik uwierzytelnienia nie powoduje kompromitacji systemu przetrzymującego drugi składnik uwierzytelnienia
    4.4. kompromitacja systemu przetrzymującego drugi składnik uwierzytelnienia nie powoduje kompromitacji systemu przetrzymującego pierwszy składnik uwierzytelnienia
5. System chmurowy odpowiedzialny za drugi składnik uwierzytelniania zbudowany jest w oparciu o odporną na awarię architekturę wysokiej klasy oraz charakteryzuje się wysoką dostępność infrastruktury.
6. System umożliwia kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia w postaci:
    6.1. instrukcji potwierdzenia logowania wysyłanej na urządzenie mobilne w ramach dedykowanej aplikacji instalowanej na urządzeniu mobilnym wspierającej systemy iOS i Android, tzw. powiadomienie “push” na urządzeniu mobilnym
    6.2. SMS



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

6.3. połączenia telefonicznego

6.4. klucza fizycznego USB U2F

6.5. tokenu sprzętowego, takiego jak na przykład RSA SecurID

6.6. potwierdzenia biometrycznego (odcisk palca, rozpoznawanie twarzy)

7. System umożliwia granularną (per aplikacja) kontrolę dostępu do aplikacji chmurowych lub znajdujących się w sieci lokalnej z wykorzystaniem drugiego (dodatkowego) składnika uwierzytelnienia.
8. System umożliwia zbieranie oraz wyświetlanie logów dotyczących przebiegu procesu uwierzytelnienia zawierających następujące informacje:

8.1. szczegółowy znacznik czasu (tzw. timestamp) opisujący minutę, godzinę, dzień, miesiąc i rok

8.2. rezultat przebiegu procesu uwierzytelnienia (pozytywny, negatywny w zależności od tego czy dostęp został przyznany czy nie)

8.3. nazwę użytkownika, który inicjował proces

8.4. nazwę aplikacji, do której próbowano uzyskać dostęp (np.: „O365 OWA")

8.5. urządzenie końcowe lub system operacyjny z którego nastąpiła próba uzyskania dostępu opatrzona dodatkowymi informacjami w postaci:

8.6. przybliżonej lokalizacji urządzenia końcowego

8.7. rodzaju użytego drugiego składnika uwierzytelnienia

9. System umożliwia wyświetlanie informacji dotyczących przebiegu procesu uwierzytelnienia na osi czasu (uwzględniając w/w rezultat przebiegu procesu uwierzytelnienia).
10. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na systemy operacyjne:

10.1. macOS

10.2. Windows

10.3. Android

10.4. iOS

11. System umożliwia identyfikację urządzeń końcowych wykorzystywanych w procesie uwierzytelnienia dwuskładnikowego z rozróżnieniem na:

11.1. urządzenia mobilne

12. Rozwiązanie objęte jest serwisem świadczonym bezpośrednio przez producenta
13. uprawniającym do wsparcia technicznego w formie mailowej, telefonicznej lub czatu na czas trwania umowy.



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

14. 14.
System posiada publicznie dostępną dokumentację dla administratora oraz użytkown ika.

15. System umożliwia administratorom rejestrację użytkowników w systemie chmurowym w następujące sposoby:

    15.1. Ręczne dodawanie pojedynczych użytkowników przez administratora

    15.2. Automatyczne dodawanie użytkowników dzięki synchronizacji z istniejącym Usług Katalogowych, Azure Usług Katalogowych lub OpenLDAP

    15.3. Zaimportowanie listy użytkowników z pliku CSV

    15.4. Samodzielną rejestracje użytkowników podczas logowania do niektórych aplikacji

    15.5. Samodzielną rejestrację użytkowników po uprzednim wysłaniu przez administratora maila lub wiadomości SMS z linkiem aktywacyjnym

16. System oferuje możliwość samodzielnej rejestracji urządzenia wymaganego w procesie dwuskładnikowego uwierzytelniania przez użytkownika końcowego oraz możliwość zarządzania tymi urządzeniami.

17. System umożliwia konfigurację wielu metod uwierzytelniania oraz wybór wielu metod preferowanej i używanych jednocześnie przez użytkowników.

18. System umożliwia skonfigurowanie polityki obowiązującej nowych, jeszcze niezarejestrowanych użytkowników z możliwymi akcjami takimi jak:

    18.1. Wymaganie samodzielnej rejestracji przez użytkownika

    18.2. Zezwolenie na dostęp do aplikacji bez weryfikacji drugiego składnika uwierzytelniania

    18.3. Zablokowanie dostępu do aplikacji

19. System umożliwia administratorom włączenie opcji, która pozwala użytkownikom na zapamiętanie urządzenia końcowego przez ilość dni lub godzin zdefiniowanych przez administratora dla aplikacji webowych w celu uniknięcia ponownego procesu uwierzytelniania dwuskładnikowego przez określony czas.

20. System umożliwia konfiguracje zaufanych sieci w formacie adres IP, zakres adresów IP lub sieci CIDR w politykach, co umożliwia pominięcie dwuskładnikowego uwierzytelniania dla użytkowników znajdujących się wewnątrz zaufanej sieci.

21. System posiada REST API, umożliwiające programistyczny dostęp do funkcji administracyjnych oraz zarządzających.

22. System umożliwia administratorom zablokowanie używania wybranych metod uwierzytelniania przez użytkowników.

23. System nie posiada ograniczeń na ilość zabezpieczanych aplikacji.



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

24. System umożliwia tworzenie grup użytkowników i przypisywanie tych grup do aplikacji w celu pozwolenia na uwierzytelnienie do danej aplikacji tylko użytkownikom będącym częścią danej grupy.
25. System umożliwia administratorom wygenerowanie tymczasowego kodu dla użytkownika w celu pominięcia dwuskładnikowego uwierzytelniania.
26. System umożliwia personalizacje logo, które będzie wyświetlane użytkownikom w procesie uwierzytelniania dwuskładnikowego.
27. System umożliwia konfigurację limitu nieudanych prób uwierzytelnienia oraz ewentualne zablokowanie dostępu dla danego użytkownika.
28. System umożliwia integrację, w celu przeprowadzenia dwuskładnikowego uwierzytelnianie, z aplikacjami i systemami takimi jak:
    - 28.1. SSL lub IPSec VPN dla rozwiązań: Cisco Anyconnect opartych o Cisco ASA jak i Cisco FTD, Meraki Radius VPN, Checkpoint SSL VPN, Palo Alto Networks SSL VPN, Fortinet Fortigate SSL VPN, F5 SSL VPN, Juniper SSL VPN, SonicWall SRA SSL VPN, Array SSL VPN, Barracuda SSL VPN, OpenVPN.
    - 28.2. Rozwiązania dostępu zdalnego wspierające uwierzytelnianie poprzez RADIUS
    - 28.3. Serwisy typu WEB m.in. OWA, ADFS
    - 28.4. Własne aplikacje poprzez wbudowanie gotowej biblioteki WebSDK [dostępne języki programowania to m.in.: Python, Ruby, Java, PHP, Perl, Node.js] lub wykorzystanie REST API przeznaczonego do uwierzytelniania
29. Wraz z rozwiązaniem dostarczona zostanie dedykowana konsola zarządzająca dostępna w chmurze.
30. Konsola zarządzająca jest dostępna przez interfejs WEB.
31. Konsola zarządzająca umożliwia monitorowanie aktywności w zakresie uwierzytelniania użytkowników w czasie rzeczywistym oraz centralne zarządzanie.
32. Konsola zarządzająca umożliwia zarządzanie, zgodnie z posiadaną licencją, następującymi elementami:
    - 32.1. Aplikacje
    - 32.2. Polityki
    - 32.3. Użytkownicy, w zakresie m.in.: ręczne dodawanie użytkowników pojedynczo, dodawanie listy użytkowników z pliku o formacie CSV, synchronizacja z Usług Katalogowych, zarządzanie samodzielną rejestracją użytkowników.
    - 32.4. Grupy użytkowników
    - 32.5. Urządzenia używane jako drugi składnik
    - 32.6. Wszystkie urządzenia końcowe



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

32.7. Ustawienia dla administratorów

33. Konsola zarządzająca umożliwia dostęp do szczegółowych raportów zgodnie z posiadaną licencją w tym m.in.:

    33.1. Raport zawierający szczegółowe informacje odnośnie przebiegu procesu uwierzytelniania wraz z możliwością wyeksportowania raportu w formacie np. JSON lub CSV

    33.2. Raport zawierający informacje dotyczące połączeń telefonicznych oraz wiadomości SMS użytych w procesie uwierzytelniania dwuskładnikowego wraz ze znacznikiem czasu oraz dokładnym numerem telefonu użytkownika z możliwością wyeksportowania raportu w formacie np. JSON, PDF lub CSV

    33.3. Raport zawierający informacje na temat akcji oraz zmian przeprowadzonych przez administratorów wraz ze znacznikiem czasu z możliwością wyeksportowania raportu w formacie np. JSON lub CSV

    33.4. Sumaryczny raport zawierający informacje na temat procesu uwierzytelniania wraz z przedstawieniem Top Aplikacji oraz Top Metod uwierzytelniania

    33.5. Raport przedstawiający informacje odnośnie nieudanych prób uwierzytelniania wraz z powodem niepowodzenia, a także m.in. Top odrzuconych użytkowników oraz aplikacji

34. Konsola zarządzająca umożliwia monitorowanie oraz elastyczne zarządzanie licencjami oraz płatnościami.

35. System umożliwia zdefiniowanie wielu administratorów o różnym poziomie uprawnień (RBAC).

36. System umożliwia logowanie do portalu zarządzającego administratorom w oparciu o SSO.

37. System umożliwia podział użytkowników w logiczne domeny oraz do nich przypisanie konkretnych administratorów.

38. System spełnia wymagania uwierzytelniania wieloskładnikowego opisane w PCI-DSS 3.2 sekcja 8.3

39. System spełnia wymagania NIST 800-63 oraz 800-171

40. System jest zgodny z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.)

41. System spełnia wymagania FFIEC dla aplikacji finansowych

42. System jest zgodny ze standardem SOC 2



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

## 5. System antywirusowy dla stacji roboczych i serwerów - centralnie zarządzany

Założono pracę na stanowiskach roboczych w oparciu o system operacyjny Windows oraz serwery z systemem MS Windows Server 2012 lub nowsze.

5.1 Opis wymagań minimalnych – wymagania ogólne

- Program musi wspierać platformę Windows 10 Pro x86 / x64
- Program musi posiadać polskojęzyczny interfejs konsoli programu i jego monitora na stacjach roboczych.
- Program musi posiadać certyfikaty niezależnych laboratoriów.
- Program musi zapewniać ochronę przed wszystkimi rodzajami wirusów, narzędzi hackerskich, oprogramowania typu spyware i adware, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
- Program musi posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów.
- Program musi posiadać możliwość wyeksportowania bieżącej konfiguracji programu w celu jej późniejszego zaimportowania na tym samym lub innym komputerze.
- Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
- Dostarczane licencje musza być bezterminowe tj. po wygaśnięciu subskrypcji musi istnieć możliwość dalszego korzystania z oprogramowania bez żadnych zakłóceń w działaniu komputera, na którym jest zainstalowane z ostatnią możliwą datą aktualizacji szczepionek.
- Program musi posiadać możliwość aktualizacji zarówno samego oprogramowania jak i bazy sygnatur, szczepionek itp. Przez okres co najmniej 36 miesięcy od dnia obioru przedmiotu umowy.

5.2 Ochrona w czasie rzeczywistym

- Program ma możliwość skanowania i klasyfikowania plików oraz odsyłaczy do zasobów sieciowych na podstawie informacji gromadzonych w oparciu o technologię chmury.
- Możliwość tworzenia reguł blokujących/zezwalających na korzystanie z danego urządzenia w zależności od konta, na którym pracuje użytkownik.
- Możliwość utworzenia listy zaufanych urządzeń na podstawie modelu bądź identyfikatora urządzenia dla określonego konta użytkownika systemu Windows.
- Ochrona przed wszystkimi typami wirusów, robaków i koni trojańskich, przed zagrożeniami z Internetu i poczty elektronicznej, a także złośliwym kodem.
- Możliwość wykrywania oprogramowania szpiegowskiego, pobierającego reklamy, programów podwyższonego ryzyka oraz narzędzi hackerskich.
- Wbudowany moduł skanujący ruch HTTP w czasie rzeczywistym niezależnie od przeglądarki.
- Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
- Możliwość określenia poziomu czułości modułu heurystycznego.
- Wbudowany moduł kontrolujący dostęp do rejestru systemowego.
- Moduł zapory ogniowej z możliwością zdefiniowania zaufanych podsieci, dla których nie będą stosowane żadne reguły zapory.
- Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami; możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
- Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.



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

- Leczenie i usuwanie plików z archiwów co najmniej następujących formatów RAR, ARJ, ZIP, CAB, JAR.
- Możliwość zablokowania dostępu do ustawień programu dla użytkowników nieposiadających uprawnień administracyjnych.

5.3 Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.

- Możliwość wysłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy, bezpośrednio z programu - do tego celu nie może być wykorzystany klient pocztowy
- Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
- Program posiada funkcję chroniącą pliki, foldery i klucze rejestru wykorzystywane przez program przed zapisem i modyfikacją.
- Program posiada możliwość wyłączenia zewnętrznej kontroli usługi antywirusowej.
- Program musi posiadać możliwość zablokowania operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, zmiany ustawień, usunięcia licencji oraz odinstalowania programu przy użyciu zdefiniowanej nazwy użytkownika i/lub hasła.
- Program musi zapewnić autoryzację urządzeń podłączanych do portu USB.

5.4 Skanowanie na żądanie

- Skanowanie na żądanie uruchamianych, otwieranych, kopiowanych, przenoszonych lub tworzonych plików
- W przypadku wykrycia wirusa monitor antywirusowy może automatycznie:
- Podejmować zalecane działanie, czyli próbować leczyć, a jeżeli nie jest to możliwe usuwać obiekt
- Rejestrować w pliku raportu informację o wykryciu wirusa
- Powiadamiać administratora przy użyciu poczty elektronicznej lub poleceniem NET SEND
- Poddać kwarantannie podejrzany obiekt
- Skaner antywirusowy może być uruchamiany automatycznie zgodnie z terminarzem; skanowane są wszystkie lokalne dyski twarde komputera.
- Informowanie o wykryciu podejrzanych działań uruchamianych aplikacji (np. modyfikacje rejestru, wtargnięcie do innych procesów) wraz z możliwością zezwolenia lub zablokowania takiego działania.
- System antywirusowy posiada możliwość skanowania archiwów i plików spakowanych niezależnie od poziomu ich zagnieżdżenia.

5.5 Aktualizacja baz danych sygnatur zagrożeń

- Program musi posiadać możliwość określenia harmonogramu pobierania uaktualnień, w tym możliwość wyłączenia aktualizacji automatycznej.
- Program musi posiadać możliwość pobierania uaktualnień modułów dla zainstalowanej wersji aplikacji.
- Program musi posiadać możliwość określenia źródła uaktualnień.
- Program musi posiadać możliwość skanowania obiektów poddanych kwarantannie po zakończonej aktualizacji.
- Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
- Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.



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

- Antywirusowe bazy danych na serwerach producenta aktualizowane nie rzadziej niż raz na godzinę 4 godziny.
- Pobieranie uaktualnień w trybie przyrostowym (np. po zerwaniu połączenia, bez konieczności retransmitowania już wczytanych fragmentów informacji).

5.6 Raportowanie

- Program musi posiadać możliwość raportowania zdarzeń informacyjnych.

5.5 System Scentralizowanego Zarzadzania

- Dostarczone rozwiązanie antywirusowe musi posiadać system scentralizowanego zarządzania. Jeżeli do uruchomienia tego systemu konieczna jest odrębna licencja należy dostarczyć wraz z oferowanym oprogramowaniem. Zamawiający wymaga zapewnienia możliwości dystrybucji nowych wersji sygnatur oprogramowania antywirusowego w oparciu o 12 lokalizacji na terenie kraju poprzez sieć WAN-PROK.
- System Scentralizowanego Zarzadzania musi wspierać co najmniej następujące platformy:
  a) Windows Server 2012 R2 Datacenter 64-bitowy lub nowszy
  b) Windows Server 2012 R2 Standard 64-bitowy lub nowszy
  c) Aktualne i wspierane systemy operacyjne z rodziny Linux
- System scentralizowanego zarządzania musi przechowywać ustawienia w relacyjnej bazie danych SQL Server lub innej dostarczanej wraz z rozwiązaniem.
- System scentralizowanego zarządzania musi posiadać polskojęzyczny interfejs konsoli programu.
- System scentralizowanego zarządzania musi umożliwiać automatyczne umieszczenie komputerów w grupach administracyjnych odpowiadających strukturze sieci (grupy robocze sieci Windows i/lub struktura Usług Katalogowych).
- System scentralizowanego zarządzania musi umożliwiać automatyczne umieszczanie stacji roboczych w określonych grupach administracyjnych w oparciu o zdefiniowane reguły.
- System scentralizowanego zarządzania musi posiadać pakiet instalacyjny dla stacji roboczej jak również systemów serwerowych.
- System scentralizowanego zarządzania musi umożliwiać ograniczenie pasma sieciowego wykorzystywanego do komunikacji stacji z serwerem administracyjnym. Reguły powinny umożliwić ograniczenia w oparciu o zakresy adresów IP.
- System scentralizowanego zarządzania umożliwia tworzenie hierarchicznej struktury serwerów administracyjnych jak również tworzenie wirtualnych serwerów administracyjnych.
- System scentralizowanego zarządzania umożliwia zarządzanie stacjami roboczymi i serwerami plików Windows, nawet wtedy, gdy znajdują się one za zaporą NAT/Firewall.
- Komunikacja pomiędzy serwerem zarządzającym a agentami sieciowymi na stacjach roboczych jest szyfrowana przy użyciu protokołu SSL.
- Konsola administracyjna posiada możliwość scentralizowanego inicjowania skanowania antywirusowego na stacjach roboczych włączonych do sieci komputerowej.
- Zarządzanie aplikacjami odbywa się przy użyciu profili aplikacji oraz zadań.
- Konsola administracyjna ma możliwość informowania administratorów o wykryciu epidemii wirusa.
- Serwer zarządzający ma możliwość automatycznej reakcji na epidemie wirusa (automatyczne stosowanie wskazanego profilu ustawień stacji roboczych oraz uruchomienia odpowiednich zadań).



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

- System centralnego zarządzania wyposażony w mechanizmy raportowania i dystrybucji polityk antywirusowych w sieciach korporacyjnych.
- System umożliwia centralną dystrybucję i instalację aktualizacji bibliotek sygnatur wirusów oraz umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowej wersji biblioteki.
- System centralnej dystrybucji i instalacji aktualizacji oprogramowania, który umożliwia automatyczne, niewidoczne dla użytkownika przesłanie i zainstalowanie nowego oprogramowania.
- System scentralizowanego zarządzania musi umożliwiać automatyczne wysyłanie raportów pocztą elektroniczną lub zapisywanie ich w postaci plików w zdefiniowanej lokalizacji (przynajmniej w formacie PDF).
- System scentralizowanego zarządzania musi umożliwiać podgląd w czasie rzeczywistym statystyk ochrony, stanu aktualizacji instalacji w sieci itp.
- System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o aplikacjach znajdujących się na stacjach roboczych.
- Program musi mieć możliwość dezinstalacji aplikacji niekompatybilnych jak również dowolnej aplikacji znajdującej się w rejestrze aplikacji użytkownika.
- System scentralizowanego zarządzania musi mieć możliwość zbierania informacji o sprzęcie zainstalowanym na komputerach klienckich.
- System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o obiektach poddanych kwarantannie oraz podejmowanie odpowiednich działań (np. przywracanie, skanowanie itp.).
- System scentralizowanego zarządzania musi umożliwiać przeglądanie informacji o obiektach, które zostały wykryte, ale program nie podjął względem nich żadnego działania.
- System scentralizowanego zarządzania musi umożliwiać automatyczne instalowanie licencji dostarczonego oprogramowania antywirusowego na stacjach roboczych.
- System scentralizowanego zarządzania musi umożliwiać automatyczne i regularne tworzenie kopii zapasowej serwera zarządzającego, która umożliwi przywrócenie w pełni działającego systemu zarządzania
- System scentralizowanego zarządzania musi umożliwiać wysłanie do stacji roboczych komunikatu o dowolnie zdefiniowanej treści.
- Program musi umożliwiać ukrycie przed użytkownikiem interfejsu aplikacji.
- Program musi umożliwić administratorowi wyłączenie niektórych lub wszystkich powiadomień wyświetlanych na stacjach roboczych.
- System scentralizowanego zarządzania musi umożliwiać administrację poprzez przeglądarkę internetową.
- System scentralizowanego zarządzania musi dać możliwość wykorzystania bramy połączenia dla komputerów, które nie mają bezpośredniego połączenia z Serwerem administracyjnym.
- System scentralizowanego zarządzania musi mieć możliwość sprawdzenia aktualnych wersji oprogramowania antywirusowego.
- System scentralizowanego zarządzania musi umożliwić wysyłanie powiadomień do wybranych użytkowników przy użyciu poczty elektronicznej lub wiadomości SMS.
- W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej oraz pobierania nowych wersji oprogramowania zarządzającego.



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

## 6. Dodatkowa ochrona stacji roboczych – system EDR

### – system stacjonarny lub realizowany jako usługa w chmurze

System antymalware składa się z następujących elementów:

I. Konsola do zarządzania systemem ochrony antymalware dla komputerów, serwerów oraz urządzeń mobilnych wraz z niezbędnymi usługami (w przypadku usługi chmurowej wraz z licencjami subskrypcyjnymi na okres do 3-lat).

II. Oprogramowanie agenta ochrony antymalware dla komputerów, serwerów oraz urządzeń mobilnych (chmura - subskrypcja na okres do 3 lat).

III. Konsola integracyjna dla całego dostarczanego systemu zabezpieczeń przed malware

   a. Integracja systemu ochrony komputerów, serwerów oraz urządzeń mobilnych

   b. Integracja systemu ochrony poczty elektronicznej

   c. Integracja systemu sandbox

### 6.1 Konsola zarządzająca systemem ochrony antymalware – podstawowe funkcjonalności

1. Konsola procesuje informacje o plikach, które przychodzą od podłączonych innych elementów ochrony antymalware całego systemu w tym:
   a. agenci ochrony stacji roboczych
   b. sondy IPS
   c. bramki ochrony e-mail
2. Konsola wspiera następujące systemy operacyjne stacji roboczych oraz serwerów:
   a. Windows
   b. Linux
   c. MacOS
   d. Android
   e. iOS
3. Konsola zapewnia narzędzia szybkiej reakcji na zdarzenia - co najmniej w postaci możliwości zweryfikowania reputacji danego pliku, jeśli był on już wcześniej widziany w sieci, i określenie jego statusu w trzech stanach (czysty, neutralny, złośliwy). Konsola zapewnia współdzielenie informacji o plikach z globalnym centrum (Threat Intelligence) w sposób zanonimizowany np. poprzez sumy kontrolne (SHA-256) lub inne rozwiązanie oferowane przez producenta.



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

4. Konsola umożliwia zdefiniowanie własnego zbioru typu Whitelist oraz Blocklist dla plików przez następujące mechanizmy:
    a. Zdefiniowanie pojedynczej sygnatury pliku
    b. Import pliku tekstowego z wieloma sygnaturami plików
    c. Automatyczne wygenerowanie sygnatury pliku poprzez upload pliku do konsoli
5. Konsola wykorzystuje mechanizmy uczenia maszynowego celem oceny pliku wykonywalnego i próby ustalenia jego dyspozycji (malware lub czysty) na podstawie analizy jego metadanych takich jak nagłówek, odnośniki do bibliotek DLL, atrybuty COFF.
6. Konsola wykorzystuje mechanizmy porównywania i grupowania sygnatur plików, pozwalający na blokowanie całej rodziny malware'u i pomagający wykrywać warianty malware'u polimorficznego.
7. Konsola umożliwia zdefiniowanie zbiorów adresów IP typu Blocklist w celu uniemożliwienia komputerom komunikacji z tymi adresami.
8. Konsola zapewnia możliwość automatycznej propagacji do systemów ochrony antymalware informacji o widzianych plikach oraz ich statusie celem ich blokowania
9. Konsola zapewnia automatyczne i niezwłoczne przesyłanie do systemów ochrony informacji o plikach, które podczas początkowej analizy otrzymały status „czysty" lub „neutralny", a których status został obniżony do statusu „złośliwy" – tzw. blokowanie wsteczne
10. Konsola zapewnia własny interfejs graficzny do analizy zdarzeń i dokonywania zmian konfiguracji polityk bezpieczeństwa.
11. Wymagana jest możliwość podłączenia do konsoli co najmniej 3 tysięcy konektorów (agentów AMP) na stacjach roboczych oraz innych narzędzi bezpieczeństwa jak: NGFW, NGIPS, bramki ochrony EMAIL.
12. Dostęp do zaawansowanych ustawień konsoli jest zabezpieczony poprzez mechanizm uwierzytelnienia dwuskładnikowego (ang. Multi-Factor Authentication - MFA)
13. Konsola umożliwia podział zarządzanych stacji roboczych na grupy, którym przypisuje się ich własną politykę. Do każdej takiej grupy istnieje możliwość przypisania innych administratorów. Administratorzy mogą zarządzać polityką komputerów i mają wgląd w zdarzenia tylko w ramach swojej grupy
14. Konsola jest wyposażona w moduł obrazujący poprzez różne kolory ilość infekcji w różnych grupach hostów
15. Konsola zawiera zestaw danych demonstracyjnych, którymi są przykładowe ataki (WannaCry, przechwytywanie wiersza poleceń) wraz z instrukcjami, dzięki którym administrator może zobaczyć w jaki sposób skutecznie odczytywać zdarzenia.



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

16. Konsola pozwala na zdefiniowanie polityki dla agentów w taki sposób, aby mogły działać na stacji roboczej razem z innym oprogramowaniem antywirusowym lub antymalware'owym omijając skanowanie ich katalogów. System zawiera wbudowane zestawy wykluczeń oraz zezwala na konfigurację tych wykluczeń przez administratora.

17. System zezwala na pełną konfigurację polityki w trybie monitorowania, tak by wszystkie mechanizmy działały i były generowane zdarzenia w konsoli zarządzania oraz monity informacyjne na stacji użytkownika, natomiast działania niepożądane nie są blokowane. Włączenie trybu blokowania odbywa się przez zmianę jednego parametru w polityce agenta.

18. Konsola posiada narzędzie do szybkiej identyfikacji aplikacji, które najczęściej są wykorzystywane przez złośliwe oprogramowanie w danej sieci do osadzenia się na komputerach lub do uzyskania do komputerów dostępu. Dane przedstawiane są administratorowi w następujący sposób:

    a. w formie wykresu z procentowym podziałem wykorzystania aplikacji

    b. na osi czasu pokazującej ilość zagrożeń wprowadzonych przez daną aplikację w danym czasie.

19. Konsola współpracuje z systemem sandbox w następującym zakresie:

    a. Konsola pozwala na ręcznie przesyłanie plików do analizy przez system sandbox i odczytanie wyników analizy bez potrzeby logowania się do systemu sandbox

    b. Konsola umożliwia odczyt wyników analizy próbki przez system sandbox bez konieczności logowania się do systemu sandbox w następującym zakresie:

        i. Nazwa pliku oraz jego sumy kontrolne (SHA-256, SHA-1 oraz MD5)

        ii. Typ pliku wykryty na podstawie tzw. „file magic number"

        iii. Znaczniki czasu rozpoczęcia procesu detonacji i jego zakończenia

        iv. Odczyt wskaźników detekcji behawioralnej ze szczegółami

        v. Odczyt żądań i odpowiedzi HTTP, zapytań DNS oraz nawiązywanych sesji TCP/IP

        vi. Odczyt uruchamianych procesów, artefaktów, zmian w rejestrach

        vii. Odczyt operacji na plikach (tworzenie, odczyt, modyfikacja, usunięcie pliku)

        viii. Możliwość pobrania całego badanego pliku

        ix. Możliwość pobrania badanego pliku w postaci PCAP

        x. Możliwość pobrania wszystkich plików wygenerowanych przez badaną próbkę



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

c. Konsola otrzymuje następujące szczegółowe informacje z analizy behawioralnej:

   i. nazwa wskaźnika

   ii. opis

   iii. kategoria

   iv. znaczniki (tagi)

   v. poziom zagrożenia związany z tym wskaźnikiem

   vi. pewność detekcji

   vii. listę URL znalezionych w dokumentach

   viii. informacje na temat artefaktów, ścieżek do plików, domen, z którymi program się komunikuje.

d. Konsola umożliwia pobranie nagrania ekranu wideo z procesu detonacji plików w celu sprawdzenia aktywności pulpitu

## 6.2 Oprogramowanie agenta ochrony stacji końcowej/serwera

1. Agent ochrony stacji roboczej obsługujący następujące systemy operacyjne z pełnym wsparciem producenta:

   a. Windows 8, 8.1, 10, 11

   b. Windows Server 2012, 2012 R2, 2016, 2019, 2022

   c. MacOS/OSX 10.14, 10.15, 10.16, 11.x, 12

   d. RHEL/CentOS 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.1, 8.2, 8.3, 8.4, 8.5

   e. Oracle Linux 6.10, 7.7, 7.8, 8.1, 8.2, 8.3, 8.4, 8.5

   f. Ubuntu TLS 18.04.x, 20.04.x

2. Agent ochrony dla urządzeń mobilnych obsługujący system Android 6.0 i nowsze oraz iOS 11.3 i nowsze

3. Agent ochrony stacji końcowej dostarcza następujące narzędzia i funkcje wspierające proces wykrywania oraz eliminacji zdarzeń naruszenia polityki bezpieczeństwa poprzez złośliwe lub niechciane oprogramowanie:

   a. „wskaźniki przełamania zabezpieczeń" – poszczególne zdarzenia dotyczące plików oraz pojedyncze zachowania elementów systemu operacyjnego/procesów/aplikacji są korelowane w incydenty i mają nadawane odpowiednie priorytety w celu zwrócenia uwagi administratora systemu na te najważniejsze



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

b. „reputacja plików” - zaawansowane metody analizy zbieranych informacji przez agenta o plikach powinny wystarczyć do określenia ich dyspozycji – czy są złośliwe, neutralne czy czyste

c. „wizualizacja zachowania systemu operacyjnego” – ciągła analiza zachowania monitorowanego systemu operacyjnego pod kątem aktywności na plikach oraz procesów w połączeniach sieciowych dająca możliwość ich wizualizacji w celu szybszego wykrycia przyczyny infekcji złośliwym oprogramowaniem

d. „elastyczne wyszukiwanie” – proste i nieograniczone wyszukiwanie szczegółowych informacji o wykrytych zdarzeniach pozwalające w szybki sposób

    i. zrozumieć formę wykrytego ataku

    ii. wskazać powiązane ze sobą zdarzenia

    iii. pomóc w szybki sposób usunąć zagrożenia z monitorowanego środowiska dzięki korelacji wyszukiwania na wielu warstwach zbieranych informacji

e. „rozpowszechnianie” – funkcja pozwalająca na wyświetlenie wszystkich plików, które zostały uruchomione na wszystkich monitorowanych systemach w danej organizacji i posortowanie ich według ilości wykryć

f. wsparcie dla sygnatur „OpenIOC” – w celu wykrycia targetowanych ataków administrator bezpieczeństwa ma możliwość wykorzystania mechanizmu OpenIOC. W szczególności mechanizm taki umożliwia wczytanie przygotowanych wcześniej szablonów opisujących nieprawidłowości występujące w skompromitowanych hostach i daje możliwość uruchomienia skanowania na żądanie – tzn. przeszukanie wszystkich monitorowanych stacji roboczych pod kątem tych nieprawidłowości. Funkcja ta pozwala na import ogólnie dostępnych szablonów OpenIOC, jak również posiada narzędzie edytora ułatwiającego pisanie własnych szablonów

g. „spis podatności”, który pokazuje listę podatnego oprogramowania wykrytego na monitorowanych stacjach końcowych i serwerach oraz sortuje wyświetlane informacje według poziomu zagrożenia, jakie te podatności ze sobą niosą. Narzędzie wspiera administratora w eliminowaniu – możliwie najszybciej - z monitorowanych systemów operacyjnych znanych podatności typowo wykorzystywanych przez malware

h. „kontrola rozpowszechniania infekcji” – funkcja pozwalająca uzyskać kontrolę nad podejrzanymi plikami i zatrzymać ich rozpowszechnianie się bez zwłoki związanej z zebraniem większej ilości dokładniejszych informacji. Funkcja ta umożliwia:

    i. zablokowanie konkretnego pliku/aplikacji rezydującej na wskazanych lub wszystkich monitorowanych systemach operacyjnych

    ii. opisanie zaawansowaną sygnaturą pliku, którego część zmienia się wraz z mutującym polimorficznym kodem i jego blokowanie bez względu na jego aktualną formę

    iii. blokowanie niechcianych aplikacji – w szczególności lista niechcianych aplikacji umożliwia wymuszenie polityki bezpieczeństwa blokującej zainfekowane



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

aplikacje, będące „bramą” dla malware i zatrzymuje proces nawracającej się infekcji

iv. zdefiniowanie listy niezbędnych aplikacji – w szczególności pozwala na określenie listy dopuszczonych aplikacji i zezwala na ich funkcjonowanie bez względu na poziom zagrożenia jaki ze sobą wnoszą, jeśli istnieje taka potrzeba lub wymaga tego biznes

v. blokowanie komunikacji zwrotnej złośliwego oprogramowanie C&C, w szczególności w przypadku komputerów znajdujących się poza siecią korporacyjną poprzez wykorzystanie reputacji adresów IP, przy czym baza reputacyjna utrzymywana przez dostawcę rozwiązania.

4. Agent ma możliwość uruchomienia jako proces bez własnego interfejsu graficznego widocznego dla użytkownika

5. Agent ma możliwość uruchomienia silnika antywirusowego skanującego dysk twardy i pamięć za pomocą tradycyjnych sygnatur antywirusowych. Silnik ten jest uruchamiany opcjonalnie i może być uruchomiony tylko dla wskazanej grupy stacji końcowych.

6. Agent ma możliwość pracy równocześnie z innymi systemami antywirusowymi poprzez zdefiniowanie wyjątków od skanowania. Definicja tych wyjątków jest możliwa na dwa sposoby:

    a. Wybór wyjątków z gotowej listy przygotowanej przez producenta rozwiązania dla wykorzystywanego równocześnie systemu antywirusowego.

    b. Możliwość zdefiniowania własnych wyjątków zawierających:

        i. Ścieżkę do konkretnego katalogu/folderu

        ii. Wskazanie konkretnego pliku wykonywalnego poprzez podanie ścieżki lub zdefiniowanie jego sumy kontrolnej SHA

        iii. Zdefiniowanie rozszerzeń plików

7. Agent wyposażony jest w mechanizm zabezpieczający przed atakami typu „exploit". Ochrona polega na przydzieleniu nowego obszaru pamięci dla aplikacji poprzez inny mechanizm niż standardowy algorytm przydziału pamięci przez systemy operacyjne. Operacja ta jest niewidoczna dla użytkownika.

8. Agent wyposażony jest w zaawansowany mechanizm zabezpieczenia krytycznych procesów systemów Windows przed wstrzyknięciem złośliwego kodu przez inne procesy.

9. Agent wyposażony jest w mechanizm zaawansowanego wykrywania ataków typu Ransomware, polegający na monitorowaniu zachowania się uruchomionych programów i operacji w przestrzeni dyskowej a także blokowaniu w przypadku nieprawidłowego ich zachowania.

10. Agent wyposażony jest w mechanizm izolacji stacji końcowej, polegający na zablokowaniu całego ruchu z tej stacji i do niej z wyjątkiem ruchu kontrolnego systemu antymalware.



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

7. Konsola stanowi jedno miejsce monitoringu stanu bezpieczeństwa we wszystkich elementach dostarczanego systemu antymalware:
    a. System zabezpieczenia stacji końcowych, serwerów i urządzeń mobilnych
    b. Systemu ochrony poczty elektronicznej
    c. Systemu sandbox
8. Konsola umożliwia tworzenie dashboardów przez administratorów oraz współdzielenie wybranych dashboardów.
9. Konsola posiada moduł wyszukiwania IoC (Indication of Compromise)
    a. Moduł pozwala na zapytanie jednocześnie o wiele typów IoC: adresy IP, nazwy domenowe, URLe, suma kontrolna SHA-256 plików
    b. Wyszukiwanie przez moduł polega na odpytaniu wszystkich zintegrowanych narzędzi bezpieczeństwa o zadane wartości a także zwróceniu wyniku w postaci:
        i. Informacji o zadanej wartości z każdego zintegrowanego narzędzia, jeżeli zdarzenie związane z tą wartością miało tam miejsce. Szczegółowy wynik zwracany jest w postaci tekstowej lub tabelarycznej
        ii. Grafu zależności i powiązań pomiędzy wszystkimi zadanymi wartościami a narzędziami bezpieczeństwa, przez które zagrożenie przeszło lub zostało zablokowane. Administrator z grafu ma możliwość szybkiego odczytania jak zagrożenie dostało się do wewnątrz, które narzędzia bezpieczeństwa to wykryły i jaka jest skala zagrożenia.
    c. Moduł udostępnia podręczne menu na grafie zależności (np. pod jednym z klawiszów myszy), które pozwala administratorowi na wykonywanie określonych operacji jednym kliknięciem:
        i. Wymuszenie przesłania pliku do analizy sandbox
        ii. Wyizolowanie stacji od sieci przy wykorzystaniu agenta ochrony stacji
        iii. Analiza IP, domeny, URL w wybranym zintegrowanym systemie bezpieczeństwa
10. Konsola pozwala na tworzenie automatycznych akcji wywoływanych na podstawie określonego zdarzenia. Przykład takiej akcji: wyizolowanie stacji końcowej i wysłanie wiadomości email do administratora bezpieczeństwa z informacją o tym zdarzeniu w momencie, gdy na stacji końcowej zostanie wykryte zagrożenie.
11. Konsola wyposażona jest w moduł zarządzania incydentami w zakresie co najmniej:
    a. Przypisywania incydentu do konkretnego administratora
    b. Modyfikacja danych o incydencie



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

c. Eksport danych o incydencie w formacie JSON

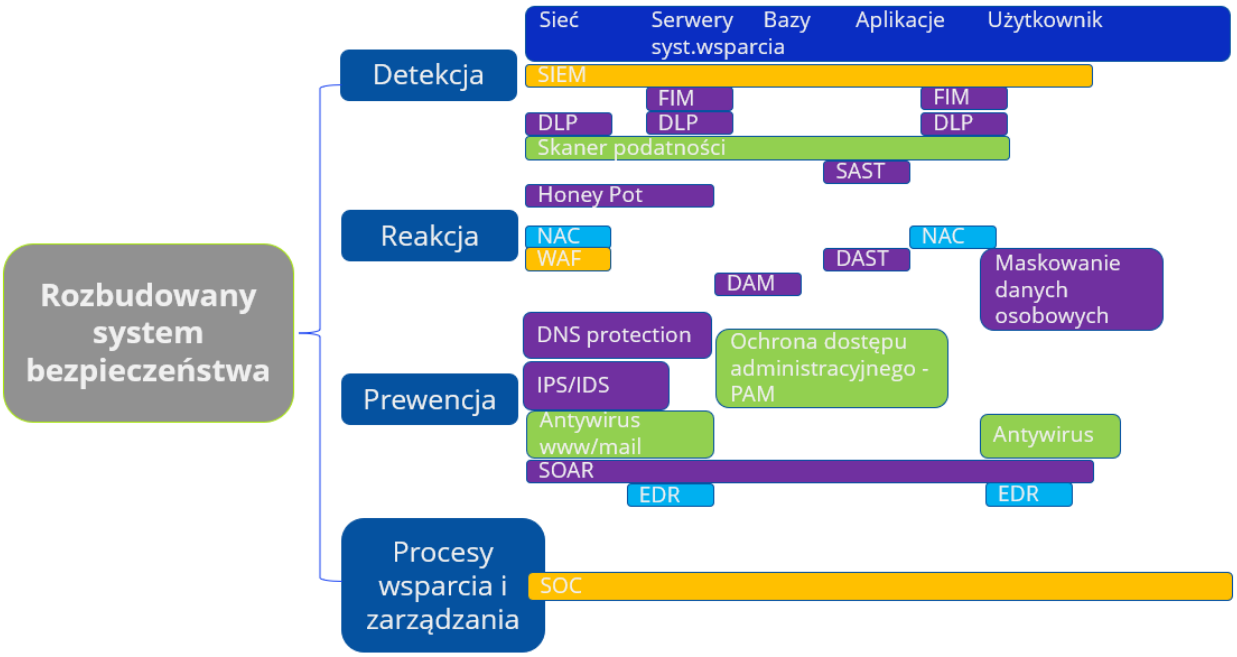
Konsola umożliwia zintegrowanie innych systemów firm trzecich.



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

## 7. Architektura docelowa systemu bezpieczeństwa

Poniżej przedstawiono strukturę systemów jaka rekomendowana jest w jednostkach będących Operatorami Usług Kluczowych. Strukturę taką można tworzyć jako rozbudowę architektury minimalnej.




7.1 składniki podstawowe architektury docelowej

1. usługa pocztowa w chmurze + system antymalware dla poczty (sandbox)
2. SZBI w tym polityka ciągłości działania,
3. firewall - zapora sieciowa z wbudowanym IPS oraz systemem antywirusowy
4. system dostępu do Internetu realizowany na zaporze sieciowej (firewall)
5. system antywirusowy dla stacji roboczych i serwerów - centralnie zarządzany
6. systemy kopii zapasowych z opcją repozytorium danych w chmurze
7. usługi bezpieczeństwa realizowane przez operatorów na łączach telekom. (antyDDoS, WAF, antymalware)

## 8. Dodatkowe systemy – składniki systemu bezpieczeństwa

**8.1 System wykonywania kopii bezpieczeństwa w chmurze**

- Centralna konsola zarzadzania
- Zautomatyzowany system tworzenia kopii w chmurze



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

- wersjonowanie plików do 90 dni
- szyfrowanie danych kluczem własnym użytkownika
- deduplikacja danych na źródle na poziomie blokowym
- Kompresja danych
- szyfrowane na komputerze za pomocą silnego algorytmu AES-256 dopuszczalny kluczem własnym użytkownika

### 8.2 System zarządzania dostępem i kontami uprzywilejowanymi

System klasy PAM **Privileged Access Management -** System pozwala na monitorowanie użytkowników uprzywilejowanych, nadzór nad dostępem i uprawnieniami do kont, procesów i systemów w infrastrukturze organizacji oraz umożliwia kontrolę nad kontami o wysokich uprawnieniach. PAM nie tylko minimalizuje ryzyko zewnętrznych cyberataków poprzez utrudniony dostęp do kont administracyjnych, ale również zapobiega wewnętrznym nadużyciom. Rozwiązanie to umożliwia także kontrolę nad pracami firm outsourcingowych lub innych stron trzecich, które otrzymują dostęp do krytycznych danych. PAM pozwala także sprowadzić autoryzowane czynności administratorskie do niezbędnego minimum, tym samym umożliwiając wykonywanie rutynowych działań w bezpieczny sposób. Zapewnia kontrolę, transparentność aktywności oraz możliwość przeprowadzenia audytu, zwiększając cyberbezpieczeństwo firmy.

Rodzaje kont uprzywilejowanych dzielimy na kilka rodzajów:

- lokalne konto administracyjne, które daje dostęp do zasobów,
- domenowe konto użytkownika z dostępem do stacji roboczych i serwerów w ramach domeny,
- konto alarmowe (*break glass*) używane w awaryjnych sytuacjach,
- konto techniczne lub serwisowe używane do obsługi systemu operacyjnego,
- konto Usług Katalogowych, które umożliwia zmianę haseł do kont,
- konto aplikacji, które daje dostęp do baz danych lub zapewnia dostęp do innych aplikacji.

Konta tego typu stanowią podwyższone ryzyko dla infrastruktury IT.

Ryzyko i zagrożenia związane z dostępem do kont uprzywilejowanych są jak najbardziej realne i obejmują między innymi:

- brak konkretnej wiedzy na temat użytkowników, którzy posiadają lub posiadali w przeszłości szeroki zakres uprawnień. Problem w szczególności dotyczy zapomnianych kont uprzywilejowanych, które stanowią potencjalny cel nie tylko cyberprzestępców, ale również byłych pracowników.
- Zbyt szeroki zakres uprawnień, który często wynika z przekonania, że ograniczony dostęp obniży wydajność pracy.
- Zmieniające się obowiązki pracownika, w wyniku czego zachowuje on przywileje, z których nie powinien korzystać.
- Dzielenie się kontami i hasłami, co utrudnia przypisanie wykonywanych czynności do jednej osoby.
- Kontrolowanie bezpieczeństwa danych osobowych w sposób niedoskonały, między innymi poprzez ponowne wykorzystanie danych uwierzytelniających.
- Omijanie lub lekceważenie polityki bezpieczeństwa ze strony pracowników.



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

Skuteczną ochronę kluczowych zasobów zapewnia:

- zabezpieczenie dostępu do krytycznych serwerów,
- powiązanie pojedynczej sesji z określonym użytkownikiem uprzywilejowanym,
- nadawanie uprawnień administratorom tylko do określonych zasobów,
- wsparcie w zarządzaniu tożsamością,
- pozwala na działanie w zgodności z regulacjami prawnymi,
- zarządzanie hasłami przy pomocy menadżera haseł,
- mechanizm automatycznej rotacji haseł,
- możliwość nagrywania sesji zdalnego pulpitu,
- możliwość nagrywania sesji terminalowych (linii poleceń).

### 8.3 Centrum operacyjne bezpieczeństwa

SOC (Security Operation Center) – celem jest zapewnienie Usługi monitorowania zdarzeń bezpieczeństwa występujących w infrastrukturze Zamawiającego. Usługa może być realizowana w dwóch trybach:

- Zamawiający posiada własny system klasy SIEM
- Zamawiający nie posiada systemu klasy SIEM

W przypadku posiadania systemu klasy SIEM możliwy jest wybór usługi wraz z utrzymaniem systemu.

Wymagania dla usługi:

Pierwsza Linia Wsparcia

W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

(1) Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA.
(2) Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
(3) Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
(4) Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.
(5) Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.
(6) Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
(7) Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
(8) Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.
(9) Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.

Druga Linia Wsparcia

W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

(1) Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA.



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

(2) Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń po incydentalnych.
(3) Przygotowanie Miesięcznych raportów z realizacji prac.

## 9. Podsumowanie

Powyższe rekomendacje to zbiór opisów funkcjonalnych, który celem jest ułatwienie tworzenia i doskonalenia systemów bezpieczeństwa informacji w placówkach ochrony zdrowia. Należy przy tym pamiętać, iż systemy cyberbezpieczeństwa, tak jak metody ataków w cyberprzestrzeni, podlegają ciągłym zmianom. Jest to proces ciągły i nie można mieć skutecznego systemu cyberbezpieczeństwa zbudowanego raz na zawsze. Dlatego istotnym działaniem osób zarządzających w placówkach ochrony zdrowia musi być właściwy proces szacowania i oceny ryzyka, przygotowanie procedur na sytuacje kryzysowe i awaryjne (tzw. polityka ciągłości działania). Każdy system chroniący przed atakiem można przełamać i dlatego tak ważne jest wykonywanie kopii bezpieczeństwa danych. Takie kopie muszą być robione często a także należy sprawdzać czy wykonywane kopie można odtworzyć w zakładanym czasie. Cały proces tworzenia i odtwarzania kopii bezpieczeństwa powinien być także opisany jako procedura (polityka kopii bezpieczeństwa).
W każdej jednostce ochrony zdrowia należy pamiętać o ochronie danych. Dane gromadzone w systemach to dane wrażliwe – zawierają informacje o stanie zdrowia pacjentów a także dane osobowe. Takie dane podlegają szczególnej ochronie zgodnie z Ustawą o ochronie danych osobowych.
Z punktu widzenia przepisów o ochronie danych osobowych należy pamiętać o kilku podstawowych działaniach wykonywanych nie jako pojedyncza akcje a jako ciągły proces:

- należy zapewnić rozliczalność przestrzegania przepisów
- należy stosować umowy powierzenia danych osobowych
- należy przestrzegać obowiązków informacyjnych wynikających z ustawy o ochronie danych osobowych
- należy odpowiednio zabezpieczyć dane przechowywane w formie elektronicznej
- należy zabezpieczyć papierową dokumentację medyczną
- należy prowadzić szkolenia personelu jednostki
- należy stosować politykę upoważnień osób zatrudnionych

Na zakończenie przypominamy o obowiązujących aktach prawnych:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560)
- Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806)
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180)
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080)



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

- Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999)
- Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa (Dz. U. poz. 1952)
- Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479)
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług (Dz. U. poz. 1831)
- Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830)
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (zwanym dalej „Rozporządzeniem KRI"), wydanym na podstawie delegacji zawartej w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
- ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848).
- Ustawa z 10 maja 2018 o ochronie danych osobowych
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO



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