Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

Komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

z zaleceniami dla podmiotów KSC, ze szczególnym uwzględnieniem sektora ochrony zdrowia

W ostatnim czasie obserwowana jest wroga działalność grup hakerskich, szczególnie ukierunkowana na podmioty z sektora ochrony zdrowia. Cyberataki te cechują się podobnymi taktykami, technikami i procedurami (TTPs). Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa publikuje wskaźniki kompromitacji (IoCs) – załącznik nr 1 oraz zalecenia utwardzające - załącznik nr 2.

Dokonanie przeglądu zasobów teleinformatycznych pod kątem IoCs z załącznika nr 1 może pozwolić na wykrycie obecności cyberprzestępców w własnej infrastrukturze, a dzięki temu ustrzec się przed zaszyfrowaniem i kradzieżą danych w ramach ataku typu ransomware.

Weryfikacji powinny dokonać szczególnie podmioty z sektora ochrony zdrowia, jednak zalecane jest to wszystkim organizacjom, gdyż grupa hakerska, z którą wiązane są ostatnie cyberataki, atakowała także podmioty z innych sektorów.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa przedstawia także zalecenia, których wdrożenie w ramach organizacji pozwoli podnieść jej bezpieczeństwo i ustrzec się przed skutecznym przeniknięciem cyberprzestępców do infrastruktury.

Komunikat powstał przy współpracy Ministerstwa Cyfryzacji i sektorowego zespołu cyberbezpieczeństwa CSIRT CeZ oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK i CSIRT GOV.

Załączniki:

Załącznik nr 1: Wskaźniki kompromitacji (IoCs)

Załącznik nr 2: Zalecenia

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Załącznik nr 1

do Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z zaleceniami dla podmiotów KSC, ze szczególnym uwzględnieniem sektora ochrony zdrowia

- Wskaźniki kompromitacji (IoCs)

Połączenia do VPN:

170.62.100[.]118

178.238.10[.]243

208.131.130[.]107

23.234.113[.]182

23.234.117[.]55

62.164.177[.]19

66.235.168[.]200

66.235.168[.]21

66.235.168[.]213

66.235.168[.]216

89.238.165[.]238

89.38.227[.]190

45.227.254[.]50

Eksfiltracja do s3:

16.1.15[.]2

Potencjalnie powiązane detekcje malware:

SHA256 3ac9c4bb817b07f51c608e7477a7057f3ed154c291f8d942b9189aad4f05d745

SHA256 b4708e9b2c941cd87bd09037fa15c8f7f3f40c3aea9c1f25711c6c079043b37b

Użyte narzędzia:

rclone

nmap

Advanced IP Scanner

Net Scan (netscan.exe)

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Załącznik nr 2

do Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z zaleceniami dla podmiotów KSC, ze szczególnym uwzględnieniem sektora ochrony zdrowia

- ZALECENIA

Realizacja nawet części z wymienionych działań pozwoli znacząco ograniczyć ryzyko wystąpienia incydentu oraz zminimalizować jego ewentualne skutki dla ciągłości działania podmiotu (zalecane jest jak najszersze wdrożenie poniższych zaleceń).

1. Ochrona brzegowa i dostęp zdalny

- **Aktualizacja systemów:** Weryfikacja wszystkich firewalli brzegowych pod kątem pracy na najnowszych, stabilnych wersjach oprogramowania (firmware). **Dostęp administracyjny do urządzeń musi być realizowany wyłącznie z wydzielonej sieci zarządzającej (managementowej).**
- **Zarządzanie uprawnieniami:** Przegląd i autoryzacja wszystkich kont o podwyższonych uprawnieniach na urządzeniach sieciowych.
- **Zabezpieczenie dostępu zdalnego:**
    - Weryfikacja zasadności kont VPN oraz połączeń RDP. **RDP dostępne bezpośrednio z sieci publicznej nie powinny istnieć** – dostęp do zasobów wewnętrznych musi odbywać się wyłącznie poprzez szyfrowany tunel VPN.
    - Wdrożenie polityki *Least Privilege*: dopuszczenie tylko niezbędnego ruchu sieciowego do celów służbowych.
    - Wymuszenie **uwierzytelniania wieloskładnikowego (MFA)** dla wszystkich połączeń VPN i RDP.
    - Weryfikacja odporności VPN na ataki typu *brute force* (np. ograniczenie ilości nieudanych logowań do N prób).
    - Ograniczenie użytkownika do tylko jednej aktywnej sesji w danym czasie.
- **Monitoring i Geofencing:**
    - Cykliczne monitorowanie ruchu sieciowego i analiza podejrzanych zdarzeń.
    - Wdrożenie Geo-blockingu: ograniczenie ruchu przychodzącego wyłącznie do regionu Polski lub Europy.
- **Kontrola ruchu wychodzącego:** Udostępnienie ruchu do sieci publicznej (egress) tylko i wyłącznie z urządzeń, które wymagają tego do poprawnej pracy operacyjnej.

2. Poświadczenia i konta (Active Directory)

- **Analiza anomalii logowań:** Weryfikacja logowań o niestandardowych godzinach, odbiegających od typowego harmonogramu pracy podmiotu.
- **Nadzór nad uprawnieniami:** Szczególny nadzór nad aktywnością kont o wysokich uprawnieniach (IT, Kadra Zarządzająca). Zaleca się wdrożenie systemów klasy PAM (Privileged Access Management), które automatyzują ten proces, eliminując konieczność ręcznego przeglądania sesji. Warto rozważyć wdrożenie systemu klasy SIEM (Security Information and Event Management) i za pomocą reguł stworzyć alerty dotyczące nietypowych zachowań.

- **Audyt i higiena kont:**
    - Regularny przegląd serwerów oraz systemów wykorzystywanych przez organizację i natychmiastowe usuwanie kont byłych pracowników oraz kont nieużywanych.
    - **Bezwzględny zakaz logowania się kontami z uprawnieniami Administratora Domeny na stacjach roboczych** (ochrona przed kradzieżą tokenów).
    - Profilaktyczny reset haseł dla kluczowych kont administracyjnych. Przy ustanawianiu nowego hasła musi ono być o odpowiedniej długości (min. 16-20 znaków); z kombinacją wielkich i małych liter, cyfr oraz znaków specjalnych. Każde konto administracyjne powinno mieć osobne, unikalne hasło dla każdego z wykorzystywanych systemów.
- **Ochrona AD:**
    - Ograniczenie dostępu sieciowego do kontrolerów domeny do niezbędnego minimum.
    - Monitorowanie operacji na bazie „NTDS.dit" oraz zmian w uprawnieniach grup wrażliwych. Wskazane jest wykorzystanie narzędzi typu SIEM lub dedykowanych skanerów bezpieczeństwa AD, które w czasie rzeczywistym alarmują o próbach nieautoryzowanego dostępu do bazy poświadczeń.
- **Wsparcie zewnętrzne:** Ścisłe monitorowanie połączeń dostawców i firm trzecich. Uprawnienia powinny być przyznawane czasowo i **tylko do niezbędnych zasobów**. Należy regularnie weryfikować ważność i zasadność utrzymywania poszczególnych kont serwisowych.

3. Ochrona Punktów Końcowych (Endpoint AV/EDR)

- **Skanowanie profilaktyczne:** Pełne skanowanie wszystkich hostów i serwerów (ze szczególnym uwzględnieniem systemów Windows).
- **Analiza logów bezpieczeństwa: KRYTYCZNE: Regularny, codzienny przegląd dzienników zdarzeń AV/EDR pod kątem alertów typu „malware detection". Ignorowanie tych alertów jest najczęstszą przyczyną udanych ataków ransomware.**
- **Modernizacja:** Docelowe wdrożenie rozwiązań klasy EDR/XDR dla zapewnienia lepszej widoczności ataków bezsygnaturowych.

4. Logowanie i monitoring (SIEM)

- **Centralizacja:** Zbieranie logów w dedykowanym, bezpiecznym kolektorze (np. syslog, rsyslog) oraz ich agregacja przez okres minimum roku wstecz.
- **Automatyzacja:** Wykorzystanie systemów klasy SIEM do cyklicznego monitorowania i korelacji zdarzeń.
- **Izolacja:** Kolektor logów musi znajdować się w odseparowanym, chronionym segmencie sieci.

5. Kopie zapasowe (Backup)

- **Separacja uprawnień:** System backupu **nie może** pracować na poświadczeniach domenowych. Należy stosować wyłącznie konta lokalne dla serwerów backupu i systemów zarządzania.

- **Segmentacja:** System kopii zapasowych musi znajdować się w całkowicie odizolowanym segmencie sieci.
- **Weryfikacja i Retencja:** Regularne testy odtwarzania danych oraz kopii odmiejscowionych. **Absolutnym minimum jest przechowywanie kopii w trybie WORM (Write Once, Read Many) z ustaloną retencją, co uniemożliwia ich usunięcie lub zaszyfrowanie przez atakującego.**

6. Usługi zewnętrzne i narzędzia

- **Usługi publikowane:** Monitorowanie logów z usług dostępnych publicznie (np. telemedycyna, portale pacjenta). Kluczowe jest wdrożenie mechanizmów wykrywania i blokowania ataków typu Brute Force oraz aktualizacja systemów (rekomendowane możliwości przeprowadzenia aktualizacji w 24h od wykrycia krytycznej podatności) i odpowiednio maksymalna ich izolacja od systemów wewnętrznych na wypadek kompromitacji.
- **Narzędzia administracyjne:** Monitorowanie wykorzystania narzędzi do synchronizacji i transferu danych (np. Rclone, WinSCP) – ich nagłe pojawienie się na stacjach roboczych może świadczyć o próbie eksfiltracji danych przez cyberprzestępców.