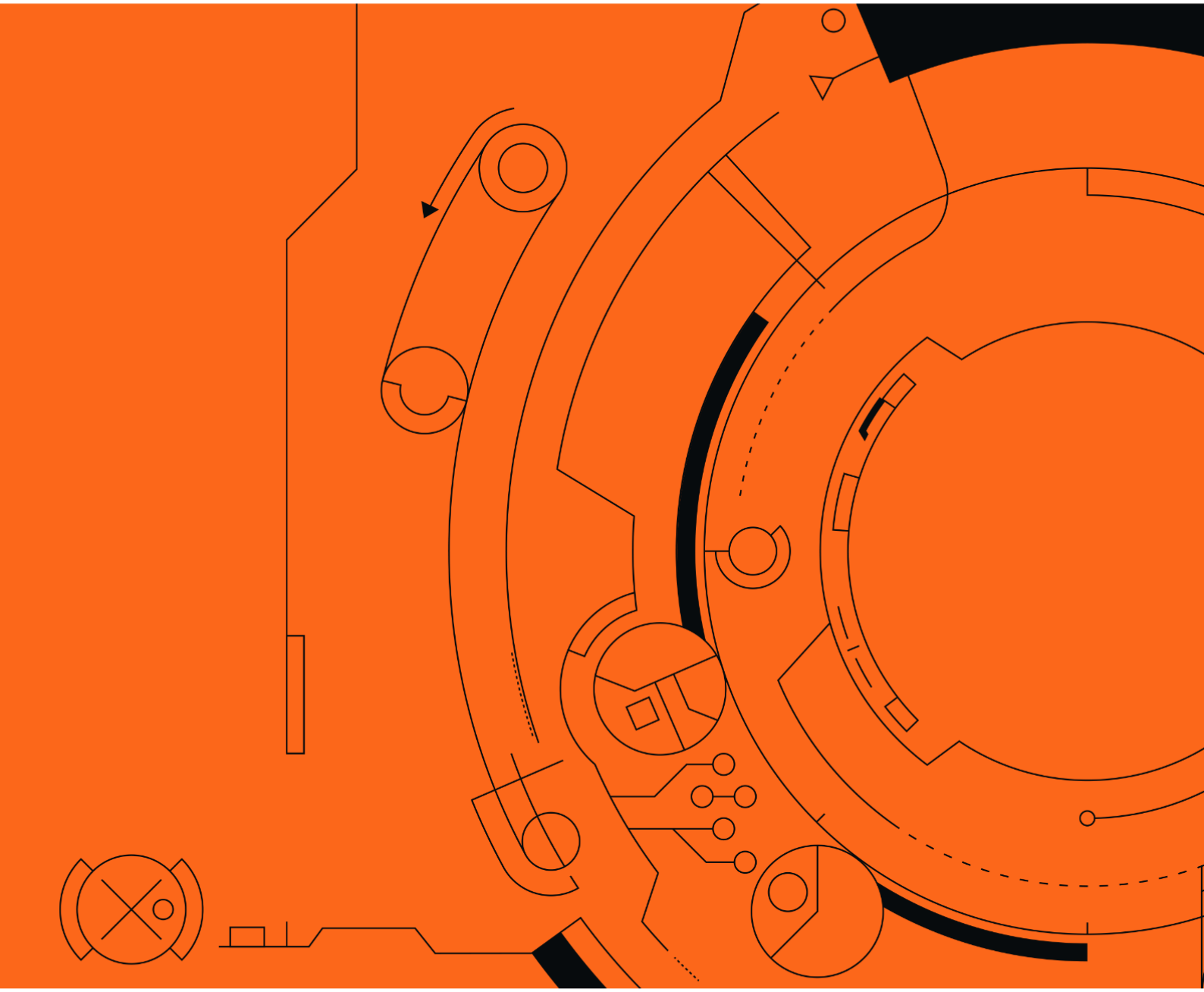
TEKNISKA® | Everything connects



SZTUKA (CYBER)WOJNY

CYKL RAPORTÓW O ZAGROŻENIACH

01: **RANSOMWARE** – UJĘCIE OGÓLNE

27/01/2022

Spis treści

Wstęp

W ostatnich miesiącach coraz częściej słyszy się o atakach ransomware skutkujących przerwami działania systemów przemysłowych. W tym minikompendium wiedzy na temat cyberbezpieczeństwa zgłębimy temat ataków ransomware i zaproponujemy kilka rozwiązań, których wdrożenie zwiększy odporność Twojej organizacji na tego typu zagrożenia.

01 Charakterystyka ransomware

Ransomware to oprogramowanie mające na celu zażądanie okupu za Twoją własność. Działania atakujących porównać można do porywaczy, którzy po przechwyceniu bliskiej osoby lub przedmiotu żądają zapłaty za ich zwrot. Ransomware ma za zadanie zawłaszczyć Twoje dane – i może zrobić to na dwa sposoby:

- uniemożliwiając Ci dostęp do Twoich danych – za pomocą silnej kryptografii zaszyfruje Twoje dane i zażąda zapłaty za ich odszyfrowanie,
- uniemożliwiając Ci kontrolę nad Twoimi danymi – atakujący po prostu wykradną Twoje dane
  i zagrożą ujawnieniem ich publicznie, o ile nie zapłacisz okupu.

Obecnie atakujący często wykorzystują oba warianty. Po wykradzeniu Twoich danych uniemożliwiają Ci do nich dostęp i żądają okupu.

Ransomware był główną przyczyną zatrzymania pracy gigantów – takich jak Norsk Hydro (2019 r., Ransomware LockerGoga) czy Colonial Pipeline (2021 r., ransomware Darkside). W obu tych przypadkach nie doszło do infekcji w sieci przemysłowej, jednak unieruchomienie sieci IT uniemożliwiło prowadzenie normalnej pracy zakładów, powodując w konsekwencji kolosalne straty. Choć w obu przypadkach udało się przywrócić funkcjonowanie sieci, to procesy te były czasochłonne.

01.1. Historia i ewolucja

Historycznie ransomware wywodzi się od programów straszących użytkowników komputerów. Początkowo na ekranie komputera pojawiała się informacja o zablokowaniu dostępu do systemu (np. w wyniku działania służb zwalczających piractwo lub pornografię dziecięcą) i informująca o możliwości przywrócenia dostępu do komputera po zapłaceniu mandatu. Z biegiem czasu zagrożenie to wyewoluowało, dodając rzeczywiste szyfrowanie do arsenału sztuczek wykorzystywanych przez złośliwe oprogramowanie – począwszy od wielu mniej lub bardziej udanych prób wdrożenia własnych metod szyfrowania danych, kończąc na wykorzystywaniu silnych metod kryptograficznych stosowanych na co dzień do legalnego zabezpieczania danych. Technika wykradania danych również pojawiła się w wyniku reakcji twórców malware na coraz częściej stosowane przez obrońców kopie bezpieczeństwa danych.

01.2. Okup i szanse odzyskania danych

Atakujący dają gwarancję odzyskania danych po zapłacie okupu i często dotrzymują słowa, aby podtrzymać swoją wiarygodność. Doskonale wiedzą, że w przypadku utraty wiarygodności ich ofiary niechętnie będą płacić okup, a przecież w tym ataku chodzi właśnie o uzyskanie korzyści finansowych. W tym celu gangi tworzące ransomware zatrudniają całe zespoły świadczące usługi wsparcia dla swoich ofiar. Istnieją całe centra obsługi telefonicznej dedykowane dla obsługi zaatakowanych firm i osób. Niektóre gangi – w celu „osłodzenia" ofierze faktu pogwałcenia jej praw – oferują dokument opisujący podatności wykorzystane w ataku wraz z poradami ich eliminacji. Część atakujących pozwala wybrać ofierze jeden z mniej istotnych plików, który zostanie odszyfrowany jako potwierdzenie technicznych możliwości zwrotu danych.

Zdarzają się jednak sytuacje, w których ofiary pomimo zapłacenia okupu nie są w stanie uzyskać dostępu do swoich danych – np. w sytuacji, w której oprogramowanie antywirusowe zareaguje po zaszyfrowaniu danych i usunie pliki złośliwego oprogramowania lub kiedy atakujący nie wykażą się znajomością materii i popełnią błąd w swoim oprogramowaniu. Mogą również wystąpić różnego rodzaju komplikacje jak np. zbyt wolne działanie oprogramowania do odszyfrowania danych unieruchamiające organizację zdecydowanie ponad planowany czas przywrócenia sprawności. Problemem może być też prawo. W niektórych krajach zapłatę okupu traktuje się jako wspieranie organizacji przestępczych i terrorystycznych. Możliwe jest zatem, że stajemy się w świetle prawa przestępcami, płacąc okup.

Wspomniane wyżej gangi, tworząc całą infrastrukturę wokół swojego ransomware, liczą na szybki i spory zysk z inwestycji. Dlatego na forach i bazarach dla cyberprzestępców pojawiają się reklamy oferujące usługi ransomware. W niektórych przypadkach, jeśli atakującym udało się uzyskać dostęp do sieci celu, zamiast żmudnie tworzyć swój własny program ransomware, przygotowywać kosztowną infrastrukturę i zatrudniać ludzi, wystarczy wynająć dostępną usługę i za odpowiedni procent z zysków zlecić to „profesjonalistom".

02 Wektory ataku, czyli jak ransomware dostaje się do organizacji

Ransomware może dostać się do Twojej organizacji w wyniku ataku celowanego oraz w wyniku masowych kampanii niewycelowanych w Twoją organizację. W obu tych przypadkach do Twojej sieci atakujący dostarcza plik, który zawiera złośliwe oprogramowanie. Plik ten może być umieszczony na jakimś serwerze w Internecie i oczekiwać na jego pobranie i uruchomienie. Aby ten plik przekazać do systemów ofiary, należy ją jakoś zachęcić lub zmusić do jego pobrania. Najczęstszym sposobem na to jest odpowiednia wiadomość poczty elektronicznej lub komunikatora internetowego. Zdarzają się również przypadki wykorzystania stron dostawców usług i sprzętu, na które pracownicy Twojej organizacji zaglądają w celu pobrania poprawek lub dokumentów. Możliwe jest również zaatakowanie podatnych serwerów, które Twoja firma udostępnia w Internecie, i dostarczenie złośliwego oprogramowania w ten sposób. Za pomocą takich metod do organizacji przekazywany jest plik lub odnośnik do pliku, który wstępnie przekazuje atakującym kontrolę nad zainfekowanym urządzeniem. Następnie atakujący wykonuje dalszy rekonesans w sieci organizacji, którą zainfekował, i próbuje dokonać dalszych infekcji wewnątrz sieci, zwiększając swoją obecność i wpływ na działanie i przepływ informacji w sieci. Ten proces w dużej mierze można zautomatyzować, tak aby człowiek – operator złośliwego oprogramowania – otrzymał gotowy raport pozwalający na podjęcie decyzji o dalszych krokach.

Dalsza propagacja wewnątrz sieci celu możliwa jest przez wykorzystanie podatności w jej wnętrzu. O ile z reguły skupiamy się na bezpieczeństwie granicy sieci, tak wewnątrz zdarzają się podatności – takie jak błędna konfiguracja, podatne na ataki oprogramowanie, stosowanie prostych haseł lub ogólnie słabe uwierzytelnienie stosowane w sieci, a nawet celowe (tymczasowe) rozluźnienie reguł bezpieczeństwa. O niektórych z tych problemów być może wie Twój personel, jednak z powodu braków kadrowych lub finansowych podjęto decyzję o akceptacji ryzyka z nimi związanego lub zignorowano to ryzyko. Podatności wykorzystywane w trakcie ataków często związane są z domyślnie włączonymi usługami systemów operacyjnych – jak np. usługa RDP (zdalny pulpit) lub SMB (m.in. współdzielenie zasobów dyskowych i drukarek).

Wiele rodzin złośliwego oprogramowania automatycznie wykonuje skanowanie Twoich zasobów, sonduje możliwości wykorzystania wspomnianych wyżej podatności i wykonuje ataki, próbując infekować kolejne systemy. Każdy z tak zainfekowanych systemów staje się częścią kontrolowanej przez atakujących sieci. Komputery w tej sieci mogą wykonać dowolne działania – jak np. zbieranie danych i wysyłanie ich do atakujących lub pobranie ransomware i zaszyfrowanie danych Twojej organizacji.

Aby uniemożliwić dostęp do danych, technicznie można wykonać kilka akcji:

- zaszyfrowanie każdego pliku z osobna – wymaga to sporo czasu i może zostać zauważone przez użytkownika, jeśli np. na pulpicie komputera pojawią się nowe pliki zamiast dotychczasowo przechowywanych tam danych.
- zaszyfrowanie MBR nośnika (stanowiącego spis treści danych zawartych na dysku) – jest to metoda najszybsza, gdyż wymaga zaszyfrowania niewielkiej przestrzeni dysku, jednak specjaliści informatyki śledczej będą w stanie odzyskać same dane z dysku.
- zaszyfrowanie całej przestrzeni dysku – to najwolniejsza metoda, ale uniemożliwi proste odzyskanie danych.

Najczęściej atakujący wykonują tę pierwszą akcję lub łączą ze sobą akcję pierwszą i drugą. Szybko szyfrując rekord MBR, uniemożliwiają dostęp do danych po wyłączeniu komputera, a następnie metodycznie szyfrują pliki.

03 Profilaktyka

Profilaktyka jest tańsza od leczenia, dlatego Tekniska rekomenduje wykonanie następujących działań podnoszących odporność Twojej organizacji na wpływ ataku z wykorzystaniem ransomware.

03.1. Stosuj zasadę ograniczonego dostępu do systemów i danych

W wojskowości, z której doświadczeń cyberbezpieczeństwo czerpie wiele swoich koncepcji, stosuje się dwie zasady i w odniesieniu do cyberbezpieczeństwa interpretuje się je w poniższy sposób:

- zasada najmniejszych wymaganych uprawnień – każdy system i użytkownik powinien mieć tylko te uprawnienia, które są mu potrzebne do wykonania powierzonych mu zadań, a reszta uprawnień powinna być mu zabroniona.
- zasada ograniczonego dostępu do danych – użytkownik lub system powinien mieć dostęp wyłącznie do danych istotnych dla powierzonych mu działań.

03.2. Przygotuj lub zaktualizuj bazę informacji o swoich zasobach

Aby chronić swoją sieć i systemy OT, musisz posiadać zawsze aktualną bazę informacji o zasobach – tzw. inwentaryzację. Taka baza w najskromniejszym wydaniu powinna informacje o:

- nazwie zasobu,
- adresach MAC i IP,
- lokalizacji zasobu,
- osobie odpowiedzialnej za ten zasób,
- logicznych połączeniach (z czym się komunikuje i w jakich protokołach).

Inwentaryzację można wykonać w różny sposób. Jedną z dobrych możliwości jest korzystanie ze zintegrowanej bazy zasobów w systemie ciągłego monitorowania np. w Radiflow iSID.

03.3. Wdróż lub zweryfikuj segmentację Twojej sieci

Architektura sieci jest bardzo ważnym elementem wielowarstwowego budowania zdolności cyberobrony (koncepcja defence-in-depth). Bezpieczną architekturę sieci najlepiej oprzeć o branżowe standardy (np. IEC 62443) i najlepsze praktyki:

01 Podziel sieć na mniejsze segmenty (strefy bezpieczeństwa wg standardu IEC 62443) odpowiedzialne za konkretne procesy biznesowe i wytwórcze.
02 Stwórz i zweryfikuj pojedyncze drogi komunikacji pomiędzy strefami bezpieczeństwa (kanały wg standardu IEC 62443).
03 Z sieci przemysłowej nie powinno być dostępu do zasobów w sieci Internet.
04 Jeśli zdalny dostęp jest niezbędny, powinien odbywać się przez VPN do stacji przesiadkowej w DMZ-OT.
05 Zbuduj sieć w taki sposób, by nie było bezpośredniej komunikacji pomiędzy sieciami OT a IT (wymiana danych powinna następować przez stacje/serwery znajdujące się w DMZ-OT).
06 Ustal politykę komunikacji pomiędzy strefami i wymuś jej stosowanie w torze kanałów komunikacyjnych:
- polityka powinna odzwierciedlać minimalne uprawnienia wymagane do wykonania zadań systemów i personelu,
- polityka powinna uniemożliwić dostęp do sieci Internet z sieci i systemów krytycznych dla działania Twojej organizacji,
- sieci i systemy o niższych wymaganiach bezpieczeństwa nie powinny mieć dostępu do sieci i systemów krytycznych.

03.4. Zmniejsz powierzchnię ataku na urządzenia końcowe

Wiedząc, w jaki sposób propaguje się w sieci ransomware oraz mając świadomość, że głównie atakowane są systemy z rodziny Windows, należy:

- utrzymywać stacje robocze i serwery zaktualizowane, stosując zalecane i sprawdzone przez dostawcę systemu ICS łatki/patche,
- włączyć wszystkie zbędne dla działania systemu ICS usługi (np. związane ze współdzieleniem plików przez sieć),
- zablokować możliwość podłączania do komputera/serwera zewnętrznych nośników pamięci USB, CD/DVD itp.,
- stosować Windows Firewall i zostawić otwarte tylko porty niezbędne do działania systemu ICS,
- stosować Windows Defender lub inne rozwiązanie do zabezpieczania stacji PC rekomendowane przez dostawcę ICS,
- wdrożyć inne zalecenia producenta systemu operacyjnego w zakresie ochrony przed ransomware.

03.5. Wdróż/zweryfikuj poprawność Monitorowania Bezpieczeństwa Sieci

Symptomy obecności złośliwego oprogramowania w sieci OT lub działań atakującego powinny zostać wykryte na wczesnym etapie, zanim dojdzie do zniszczenia zasobów. Do tego celu najlepiej nadaje się system ciągłego monitorowania i wykrywania zagrożeń (IDS) przeznaczony dla sieci przemysłowych.

01 Ciągłe monitorowanie to wymóg związany z ustawą o Krajowym Systemie Cyberbezpieczeństwa.
02 Zainstaluj system monitorowania (NSM/IDS).

03 Zbieraj dane minimum z punktów styku kanałów komunikacyjnych – optymalnie zbieraj dane z wewnątrz stref bezpieczeństwa.

Rozwiązanie IDS – takie jak **Radiflow iSID** – dzięki różnym silnikom detekcji (behawioralny i sygnaturowy) potrafi wykryć anomalie i zmiany w ruchu sieciowym oraz symptomy propagacji złośliwego oprogramowania.

03.6. Wdróż/zweryfikuj poprawne wykonywanie kopii bezpieczeństwa danych

Jedną z podstaw zapewnienia ciągłości działania jest posiadanie zweryfikowanych kopii bezpieczeństwa, dlatego zainstaluj i skonfiguruj centralny system ich wykonywania:

- zabezpiecz nim przynajmniej dane i systemy krytyczne z punktu widzenia ciągłości działania Twojej organizacji,
- cyklicznie wykonuj testy przywracania tych danych i systemów,
- upewnij się, że w sytuacji ataku możesz przywrócić świeże dane,
- upewnij się, że masz kopie bezpieczeństwa w trybie offline (niepodłączone do sieci), aby atakujący nie mógł ich zniszczyć.

03.7. Wdróż/zweryfikuj mechanizm zarządzania podatnościami

Atakujący i stworzone przez nich złośliwe oprogramowania wykorzystują podatności w systemach, którymi są błędy konfiguracyjne oraz błędy w samym oprogramowaniu. Aby móc przeciwdziałać wykorzystaniu podatności, trzeba je zidentyfikować i następnie nimi zarządzać (usuwać i stosować inne środki zaradcze). W tym celu:

01 Zainstaluj skaner podatności.
02 Cyklicznie wykonuj:
   a. skan podatności,
   b. przegląd raportów o podatnościach.
03 O ile to możliwe, zaplanuj aktualizacje podatnego oprogramowania w oknach/postojach serwisowych.
   a. Jeśli nie jest to możliwe, dostosuj politykę bezpieczeństwa, tak aby zminimalizować ryzyko związane z tą podatnością.
   b. Skanery podatności, oprócz informacji o dostępności aktualizacji oprogramowania, powinny również informować o możliwości obejścia problemu (minimalizacji ryzyka – np. przez zmiany konfiguracyjne).

Uwaga: skanowanie podatności w sieciach OT nie powinno być wykonywane na działających produkcyjnie systemach (chyba że posiada się sprawdzone i zweryfikowane zestawy testów, które nie zaburzają procesu).

03.8. Przygotuj/zweryfikuj plan przywracania po awarii/katastrofie/ataku

Elementem skutecznego programu cyberbezpieczeństwa jest plan przywracania po awarii. W tym celu:

01 Zidentyfikuj zasoby krytyczne dla zapewnienia ciągłości biznesowej i ustal priorytety ich odtwarzania.
02 Ustal maksymalny czas niedostępności dla poszczególnych systemów (RTO):
   a. rozważ wymagania prawne,
   b. rozważ wymagania ekonomiczne.
03 Zweryfikuj możliwości uzyskania szybkiej pomocy w trakcie incydentu:
   a. kontrakty z firmami oferującymi usługi reagowania na incydenty,

b. wewnętrzne możliwości reagowania na incydenty,
c. weryfikacja ścieżki komunikacji z zespołami reagowania na incydenty,
d. weryfikacja typu SLA zdefiniowanego dla procesu reagowania na incydenty,
e. zbadanie możliwości eskalacji do CSIRT Sektorowego/organów ścigania.

03.9. Zweryfikuj/zdefiniuj proces szkolenia pracowników

Najsłabszym ogniwem jest zawsze człowiek, który jest silnie podatny na skuteczny rodzaj ataku, jakim jest socjotechnika (w tym *phishing*). Atakujący w różny sposób może spowodować, że pracownik wykona działania, które doprowadzą do skompromitowania systemu.

Dlatego bardzo ważne są:
- cykliczne szkolenia podnoszące świadomość zwykłych użytkowników,
- szkolenia dla personelu technicznego z zakresu reagowania na incydenty.

04 Detekcja

Pomimo najlepszej profilaktyki może się zdarzyć, że będziesz celem ataku. Warto wiedzieć, na co zwrócić uwagę i co może świadczyć o infekcji. Twoją uwagę powinny zwrócić następujące anomalie:

- komunikacja pomiędzy zasobami, które do tej pory się nie komunikowały, może świadczyć o próbie rekonesansu wewnątrz Twojej sieci lub o próbie propagacji złośliwego oprogramowania.
- próby połączeń świadczące o nieznajomości sieci:
  - skanowanie portów,
  - skanowanie ICMP,
  - duża ilość pakietów resetujących połączenia TCP (RST),
  - zwiększona ilość komunikacji ICMP raportującej błędy *host unreachable, port unreachable, network unreachable* może świadczyć o trwającym rekonesansie lub próbach propagacji.
- nowe próby połączenia poza sieć, zwłaszcza do Internetu i szczególnie w sytuacji, w której zasoby wcześniej nie komunikowały się do Internetu i polityka bezpieczeństwa zabrania tej komunikacji.
- nagły wzrost ilości danych przesyłanych poza sieć wewnętrzną.

Nasi klienci mogą zastosować metody dostępne w rozwiązaniu iSID firmy Radiflow w celu zastawienia „pułapek" na atakujących. System ten automatycznie reaguje na większość ww. symptomów, możliwe jest również utworzenie własnych reguł detekcji dla podobnych symptomów – jak np. wykrywanie komunikacji na portach innych niż porty na liście dozwolonej komunikacji.

Powyższe symptomy mogą świadczyć o trwającej infekcji, jednak istnieje spora szansa, że atakujący dopiero rozpoznaje sieć Twojej organizacji, przez co możesz zyskać czas na reakcję. Natomiast wystąpienie poniższych symptomów najczęściej świadczy o rozpoczęciu szyfrowania dysku, więc może okazać się, że dla tego konkretnego systemu jest już za późno. Symptomy te są następujące:
- nagły, nietypowy i ciągły wzrost obciążenia procesorów:
  - może świadczyć o trwającym szyfrowaniu danych,
  - może świadczyć o działaniu oprogramowania obliczeniowego (np. koparki kryptowalut).
- nagły, nietypowy wzrost operacji odczytu i zapisu na dyskach twardych.
- pojawienie się żądania okupu:
  - zmiana tapety na żądanie okupu,
  - otwarty plik tekstowy z żądaniem okupu,
  - system nie uruchamia się poprawnie i wyświetla żądanie okupu.

05 Reakcja

W przypadku potwierdzenia incydentu związanego z ransomware niezwłocznie uruchom procedurę zaplanowaną w trakcie działań opisanych powyżej w rozdziale o profilaktyce. Poniższą listę należy traktować jako poglądową. Szczegółowe akcje powinny być poparte analizą Twojego systemu.

01 Uruchom zaplanowaną procedurę.
02 Jeśli istnieje kontrakt na wsparcie w przypadku ataku/incydentu – uruchom go.
03 Jeśli masz obowiązek poinformowania regulatora o incydencie, rozpocznij zbieranie niezbędnych danych do przekazania regulatorowi.
04 Ogranicz skutki ataku:
   a. Jeśli możesz, separuj sieć fizycznie:
      i. odłącz od zainfekowanej sieci strefy systemów krytycznych,
      ii. wyłącz punkty dostępowe sieci Wi-Fi.
      iii. wyłącz komputery podłączone do sieci (nawet te, które nie wykazują symptomów),
      iv. wyłącz serwery plików.
   b. Jeśli to możliwe, ostrzeż użytkowników, aby nie łączyli się do zainfekowanej sieci.
05 Rozpocznij procedurę analizy incydentu:
   a. Ustal „pacjenta zero", czyli pierwszą zainfekowaną maszynę w sieci.
   b. Określ metodę infekcji.
   c. Ustal metodę eliminacji podatności umożliwiającej atak.
06 Określ skalę incydentu:
   a. Ile hostów i stref (sieci) zostało zainfekowanych?
   b. Czy są na liście systemy krytyczne?
   c. Jakie systemy przemysłowe zostały dotknięte?
07 Rozpocznij procedurę przywracania systemu z kopii zapasowej:
   a. Zacznij od systemów krytycznych.
   b. Zapewnij pracę systemów krytycznych odseparowanych od sieci.
   c. Nie dopuść do komunikacji pomiędzy hostami przywróconymi i zainfekowanymi:
      i. do czasu ustalenia i eliminacji przyczyny infekcji nie łącz stref bezpieczeństwa,
      ii. do czasu eliminacji skutków infekcji nie łącz stref bezpieczeństwa.

06 Informacje o raporcie

Informacje o raporcie	
Autor dokumentu	**Piotr Urbańczyk** Architekt cyberbezpieczeństwa systemów SCADA, GIAC GRID
Weryfikacja merytoryczna	**Stefan Bednarczyk** Specjalista ds. cyberbezpieczeństwa, GIAC GICSP

07 Kim jesteśmy

07.1. Dlaczego Tekniska?

W Tekniska od blisko 20 lat dostarczamy rozwiązania i know-how w obszarze sieci przemysłowych i cyberbezpieczeństwa w OT. Jesteśmy praktykami i specjalistami w swojej dziedzinie, a nasze wieloletnie doświadczenie sprawia, że doskonale rozumiemy realne potrzeby naszych klientów – zarówno inżynierów automatyków, serwisantów, inżynierów sieciowych czy projektantów, jak również osób odpowiedzialnych za rozwój kompetencji, zarządów i managerów. To właśnie ich wspieramy na co dzień.

Prócz dostarczania i wdrażania rozwiązań z zakresu transmisji danych i cyberbezpieczeństwa w OT, szkolimy specjalistów na każdym etapie rozwoju w Akademii Tekniska oraz oferujemy możliwości rozwoju własnego biznesu, dzięki współpracy z Tekniska w ramach programu partnerskiego.

Najważniejsze informacje o Tekniska:

- Działamy na rynku od 2002 r.
- Nasz zespół to w większości wysoko wykwalifikowana kadra inżynierska.
- Specjalizujemy się w:
  - produktach i usługach dla sieci przemysłowych,
  - produktach i usługach bezpieczeństwa dla sieci OT i OT/IT,
- Zrealizowaliśmy jedno z większych wdrożeń bezpieczeństwa OT w Polsce.
- Od początku działalności dostarczyliśmy i wdrożyliśmy ponad 100 000 urządzeń dla polskiego przemysłu.
- Wiele z nich pracuje nieprzerwanie od ponad 17 lat w trybie 24/7 i mimo wymagających warunków środowiskowych.

07.2. Nasz zespół

Tekniska to zespół. Tekniska to osobowości. Tekniska to My. Wyznajemy motto „Everything connects", a u naszych podstaw leży technologia.

Zespół Tekniska tworzą doświadczeni i certyfikowani inżynierowie, ale przede wszystkim – ludzie z pasją i zaangażowaniem, który wierzą w moc współdziałania i biznesowej szczerości. Działamy razem, rozwiązując problemy naszych partnerów w zakresie transmisji danych i cyberbezpieczeństwa w IT/OT i dzieląc się zdobytym know-how, doświadczeniem i wiedzą.

Nieustannie podnosimy nasze kwalifikacje. Możemy pochwalić się licznymi międzynarodowymi certyfikatami cyberbezpieczeństwa m.in.: GRID, GICPS, Certified Penetration Testing Engineer, Certified Network Forensics Examiner ISO 9001 czy ISO 27001. Lead Autidor.

Naszych klientów wspieramy na każdym etapie projektu – od analizy i projektu, poprzez wdrożenie, aż po serwis i wsparcie merytoryczne.

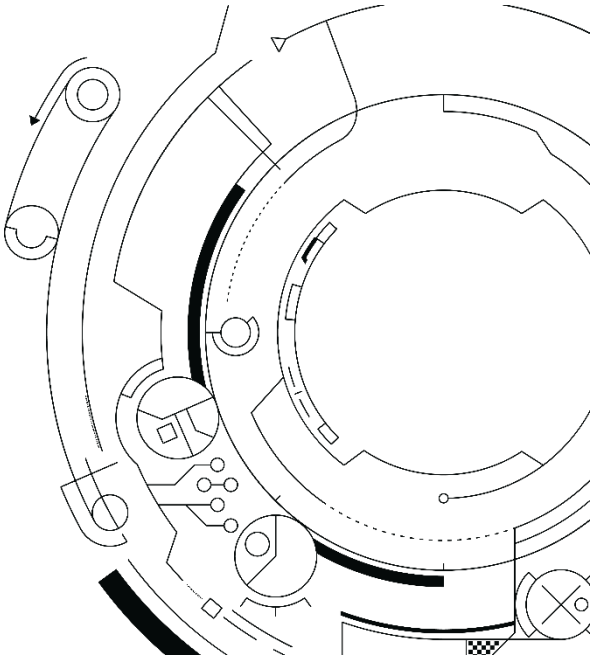
08 Porozmawiajmy

Jesteśmy otwarci na dialog ze wszystkimi, zarówno z kadrą zarządzającą jak i inżynierami automatykami, serwisantami.

Zespół Tekniska

Cybersecurity Team

48 32 33 111 06–09 (wew. 104, 111)
cybersecurityteam@tekniska.pl



TEKNISKA® | Everything connects

TEKNISKA POLSKA
Przemysłowe Systemy Transmisji Danych Sp. z o.o.
44-121 Gliwice, ul. Łabędzka 9–9A
Kapitał założycielski: 50.000 zł

ODWIEDŹ NAS
WWW.TEKNISKA.PL

Praca z Tekniska to realne korzyści dla Twojej firmy

01 Zoptymalizowana, wydajna i bezpieczna sieć

02 Niezawodność systemów transmisyjnych zapewniająca ciągłość procesu

03 Działania w zgodności z normami prawnymi i bezpieczeństwa

04 Optymalizacja kosztów utrzymania serwisu

05 Realizacja projektów w formie "turn-key"

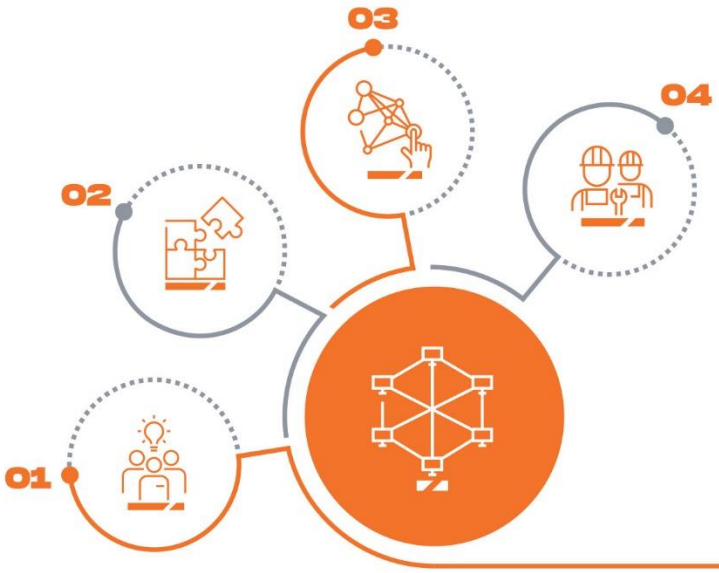
Sprawdź, co jeszcze możemy dla Ciebie zrobić

CYBERBEZPIECZEŃSTWO

01 Usługi wdrożeniowe

02 Usługi analityczne i projektowanie

03 Serwis i utrzymanie

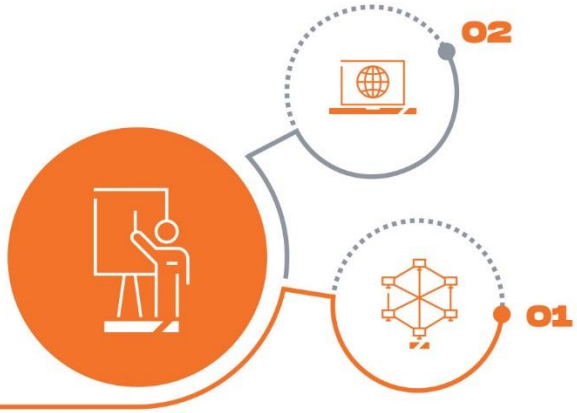


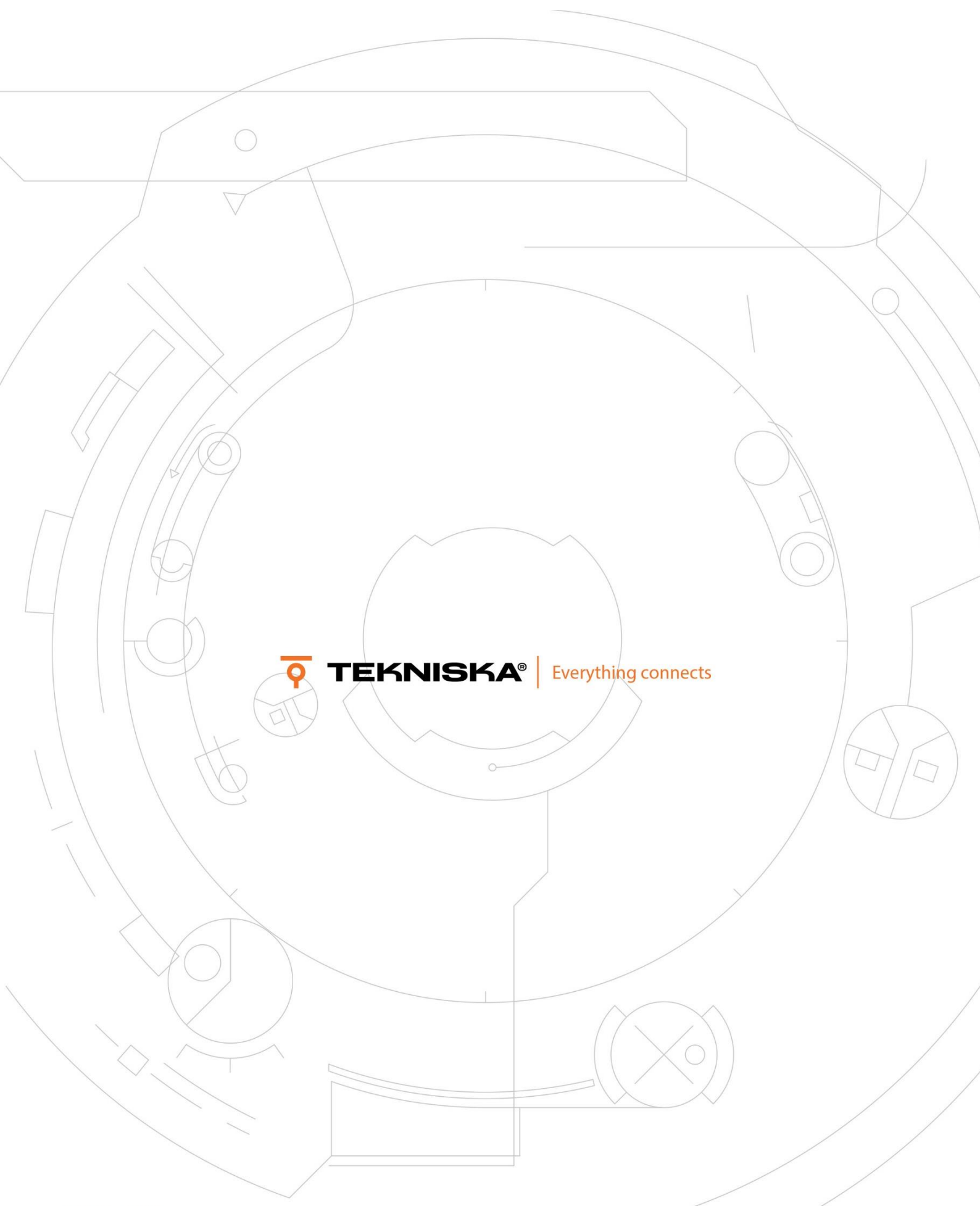
SIECI OT

01	Konsultacje
02	Usługi projektowe
03	Usługi wdrożeniowe
04	Usługi serwisowe i utrzymania

SZKOLENIA

01	Sieci OT
02	Cyber





Tekniska Polska
Przemysłowe Systemy
Transmisji Danych Sp. z o. o.
ul. Łabędzka 9-9A
44-121 Gliwice, Poland

NIP 6312631825
KRS 0000383694

+48 32 33 111 06 ÷ 09
tekniska@tekniska.pl

WWW.TEKNISKA.PL

ISO 9001
ISO/IEC 27001
AC 014