CYBERX

ASTOR

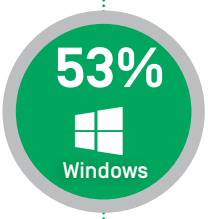
# Analiza podatności infrastruktury przemysłowej na cyberataki

**W oparciu o analizę przeszło 850 sieci kontrolujących przemysł w różnych sektorach, na sześciu kontynentach, z użyciem narzędzi do analizy ruchu sieciowego**

**Podsumowanie informacji z 2019 Globalnego Raportu nt. bezpieczeństwa sieci ICS i IIOT w przemyśle**


### Mit fizycznej separacji („Air gap"): 40% zakładów wykorzystuje co najmniej jedno bezpośrednie połączenie internetowe

» Niezależnie od tego, czy ze względu na wygodę czy przez nieuwagę, wiele sieci przemysłowych nadal jest połączonych z publicznie dostępnym Internetem. Mając na uwadze cyfryzację jako kluczowy czynnik biznesowy, sieci OT, szczególnie w większych firmach, to coraz częściej sieci firmowe – co powoduje zwiększenie powierzchni narażonej na atak, a więc także ryzyka cyberataków.




### Zdezaktualizowany system Windows: 53% zakładów nadal korzysta z przestarzałego systemu Windows, takiego jak XP

» Systemy te są bardzo narażone na ataki z użyciem oprogramowania typu ransomware, ataki ukierunkowane i inne szkodliwe formy oprogramowania – ponieważ nie są już wspierane przez firmę Microsoft. Incydenty z wirusami NotPetya i WannaCry wymusiły jednak zwrócenie uwagi na tę kwestię, dlatego od 2017 roku obserwujemy znaczącą poprawę.


### Ukrywanie się na widoku: 69% niezaszyfrowanych haseł krążących po sieci

» Brak szyfrowania w starszych protokołach, jak SNMP czy FTP, naraża wrażliwe dane na kradzież – co czyni rekonesans w sieci, a więc także naruszanie integralności danych stosunkowo łatwym zadaniem dla przestępców.


### Ochrona anty-antywirusowa: 57% zakładów nadal nie wykorzystuje oprogramowania antywirusowego, które automatycznie aktualizuje sygnatury wirusów

» Chociaż właściciele kluczowej infrastruktury i systemów kontroli w przemyśle jednoznacznie przeciwstawiali się programom antywirusowym, wielu z nich przestało traktować takie środki jak zakłócające procesy OT, dlatego coraz więcej dostawców certyfikuje także producentów takiego oprogramowania.

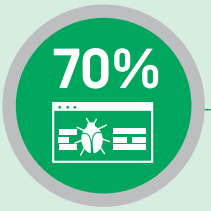

### Niefrasobliwa otwartość: 16% zakładów dysponuje co najmniej jednym punktem dostępu (WAP)

» Nieprawidłowo lub słabo skonfigurowane punkty WAP zwiększają powierzchnię narażoną na atak, ponieważ dostęp do nich mogą uzyskiwać nieupoważnieni klienci, tacy jak pracownicy lub podwykonawcy korzystający z laptopów i innych urządzeń mobilnych. Integralność punktów WAP jest także narażona z uwagi na luki w bezpieczeństwie WPA2 (patrz: ataki KRACK).

Punkty dostępu, takie jak rutery czy bramy VPN, są także narażone na zaawansowane szkodliwe oprogramowanie, jak VPNFilter, które pozwala przestępcom przechwytywać ruch sieciowy MODBUS, wykonywać mapowanie sieci, niszczyć oprogramowanie układowe rutera i przeprowadzać ataki na urządzenia końcowe OT za pomocą zhakowanych ruterów. Oznacza to, że rutery należy teraz regularnie inwentaryzować i „łatać", aby do takich ataków nie dochodziło.


### Nadmierna dostępność: 84% zakładów dysponuje co najmniej jednym urządzeniem dostępnym zdalnie

» Protokoły dostępu i zarządzania zdalnego, jak RDP, VNC czy SSH ułatwiają administratorom zdalne konfigurowanie urządzeń – ale jednocześnie pozwalają przestępcom z wykradzionymi danymi logowania dowiadywać się, jak dokładnie konfigurowane są urządzenia, a następnie nimi manipulować.




### Mediana wyników bezpieczeństwa we wszystkich branżach: 70%

» W roku 2017 ogólna mediana bezpieczeństwa uzyskana dla wszystkich branży wyniosła 61%, gdzie 80% stanowi zalecany minimalny wynik. W roku 2018 uzyskano wartość na poziomie 70%, co pokazuje, że robione są postępy – ale nadal konieczne są poprawki.

**67%** Produkcja

**68%** Branża chemiczno-farmaceutyczna

**79%** Energetyka i usługi

**81%** Rafinerie i gazownictwo

### Zróżnicowana kombinacja wyspecjalizowanych protokołów branżowych

» Sieci branżowe obejmują złożoną, niejednolitą kombinację wyspecjalizowanych protokołów OT, co komplikuje bezpieczeństwo takich środowisk. Tradycyjne narzędzia do monitorowania środowiska IT są „ślepe" na takie protokoły, co skutkuje całkowitym brakiem widoczności zasobów IT, topologii sieciowej i aktywności w sieci.

Platforma CyberX, specjalnie stworzona z myślą o cyberbezpieczeństwie OT, wykorzystuje rozległą znajomość protokołów OT, luk w bezpieczeństwie i działania urządzeń W naszej próbce z 2018 roku napotkaliśmy szereg protokołów, które zilustrowano na poniższym schemacie słownym:

PCCC OSISoft Profinet/Profibus 800xA
ICCP DeltaV DNP3 C37.118
Ovation GE-SRTP GOOSE MMS
EC60870-5 WonderwareSuitelink PCS7 SiemensS7/S7-Plus
HoneywellExperion BeckhoffAMS
EtherNet/IP SiemensSICAM VNet/IP
SchneiderElectricFoxboro
BeckhoffTwincat BSAP Emerson OPCDA/AE/UA ControlNet


CyberX wykonała analizę z użyciem zanonimizowanych i zagregowanych metadanych, po usunięciu wszystkich informacji identyfikujących. Dane umożliwiające identyfikację użytkowników są oddzielane na wczesnym etapie procesu, a szczególną uwagę przyłożono do zachowania poufności informacji.

**POBIERZ RAPORT**

Kompletny raport można pobrać ze strony cyberx-labs.com/risk-report-2019

CYBERX

## O platformie CyberX: wiemy, co jest potrzebne.

» Platforma CyberX stanowi jedyną platformę cyberbezpieczeństwa dla przemysłu stworzoną przez ekspertów ds. cyberbezpieczeństwa stopnia wojskowego, posiadających doświadczenie w ochronie kluczowej infrastruktury na terenie całego kraju. Różnica ta zapewnia fundament dla najszerzej wdrażanej platformy, tak aby możliwe było ciągłe ograniczanie ryzyka dla systemów ICS i zapobieganie kosztownym przestojom w produkcji, awariom bezpieczeństwa czy incydentom zagrażającym środowisku naturalnemu.

Do najważniejszych użytkowników platformy CyberX należą dwa z pięciu kluczowych przedsiębiorstw energetycznych oraz pięć największych przedsiębiorstw chemicznych w Stanach Zjednoczonych, pięć globalnych korporacji farmaceutycznych, a także liczne przedsiębiorstwa elektryczne i gazowe działające w Europie oraz w regionie Azji i Pacyfiku. Wśród partnerów strategicznych znajdują się tacy liderzy, jak Palo Alto Networks, IBM Security, Splunk, Optiv Security, DXC Technologies czy Deutsche-Telekom/T-Systems.

Klienci wybierają platformę CyberX, ponieważ to najprostsze w obsłudze, najbardziej zaawansowane i oferujące najlepszą interoperacyjność rozwiązanie do automatycznego wykrywania zasobów, identyfikowania kluczowych luk w bezpieczeństwie i wektorów ataków, a także nieustannego monitorowania sieci ICS pod kątem szkodliwego oprogramowania i ataków ukierunkowanych. Co więcej, platforma CyberX zapewnia najbardziej sprawną integrację z istniejącymi systemami organizacji pracy SOC, oferując zunifikowane narzędzie do zarządzania bezpieczeństwem IT/OT.

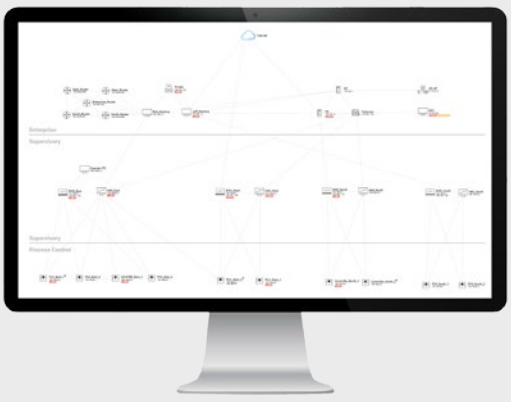
Więcej informacji można uzyskać na stronie **CyberX-Labs.com** lub korzystając z adresu **@CyberX_Labs.**

ASTOR

» Firma ASTOR jest dostawcą nowoczesnych technologii z zakresu systemów IT dla przemysłu, automatyki przemysłowej i robotyki oraz wiedzy biznesowej i technicznej dla polskich i zagranicznych przedsiębiorstw przemysłowych. Firma powstała w 1987 roku w Krakowie. Obecnie posiada siedem oddziałów w całej Polsce, m.in. w Warszawie, Poznaniu, Katowicach i Wrocławiu.

Oferta ASTOR obejmuje m.in. systemy sterowania General Electric i Horner APG, oprogramowanie przemysłowe Wonderware, roboty przemysłowe Kawasaki i Epson, a także ekonomiczne urządzenia automatyki własnej marki Astraada.

W 2016 roku ASTOR otrzymał nagrodę od firmy doradczej Frost&Sullivan, za osiągnięcie pozycji lidera polskiej automatyki przemysłowej w zakresie budowania wartości dla klienta. Kierunek wspierania rozwoju i transformacji naszych Klientów wyznacza Przemysł 4.0. Więcej informacji o firmie na stronie **www.astor.com.pl/cyberbezpieczenstwo**



XSense ujawnia wszystkie zasoby sieci ICS wykorzystując pasywną analizę ruchu sieciowego i generuje topologie sieci w oparciu o model PERA.