PRZEMYSŁ 4.0

WatchGuard

NET COMPLEX
Bezpieczeństwo IT

PRZEMYSŁ 4.0

W erze przemysłu 4.0 coraz większa część zadań spoczywa na krzemowych barkach nowoczesnych urządzeń IoT. Urządzenia “smart” pozwalają zwiększyć wydajność. Wpływają też na bezpieczeństwo pracowników, ale jak postępująca modernizacja odbija się na bezpieczeństwie cyfrowych zasobów?

Urządzenia IoT to wciąż stosunkowo nowa technologia. Szczególnie w realiach polskiej gospodarki. Dlatego ilość luk i podatności w sprzętach tego typu, nawet tych domowych, jest znacznie wyższa niż w przypadku aktualizowanych na bieżąco i powszechnych systemów zainstalowanych na komputerach pracowników.

Zagrożenia dotykające branże przemysłową zbierają żniwo na całym świecie. Także w przedsiębiorstwach, które stoją w awangardzie nowej przemysłowej rewolucji. W Wielkiej Brytanii ponad połowa przedsiębiorców przyznaje, że padła ofiarą mniej lub bardziej skutecznego ataku.

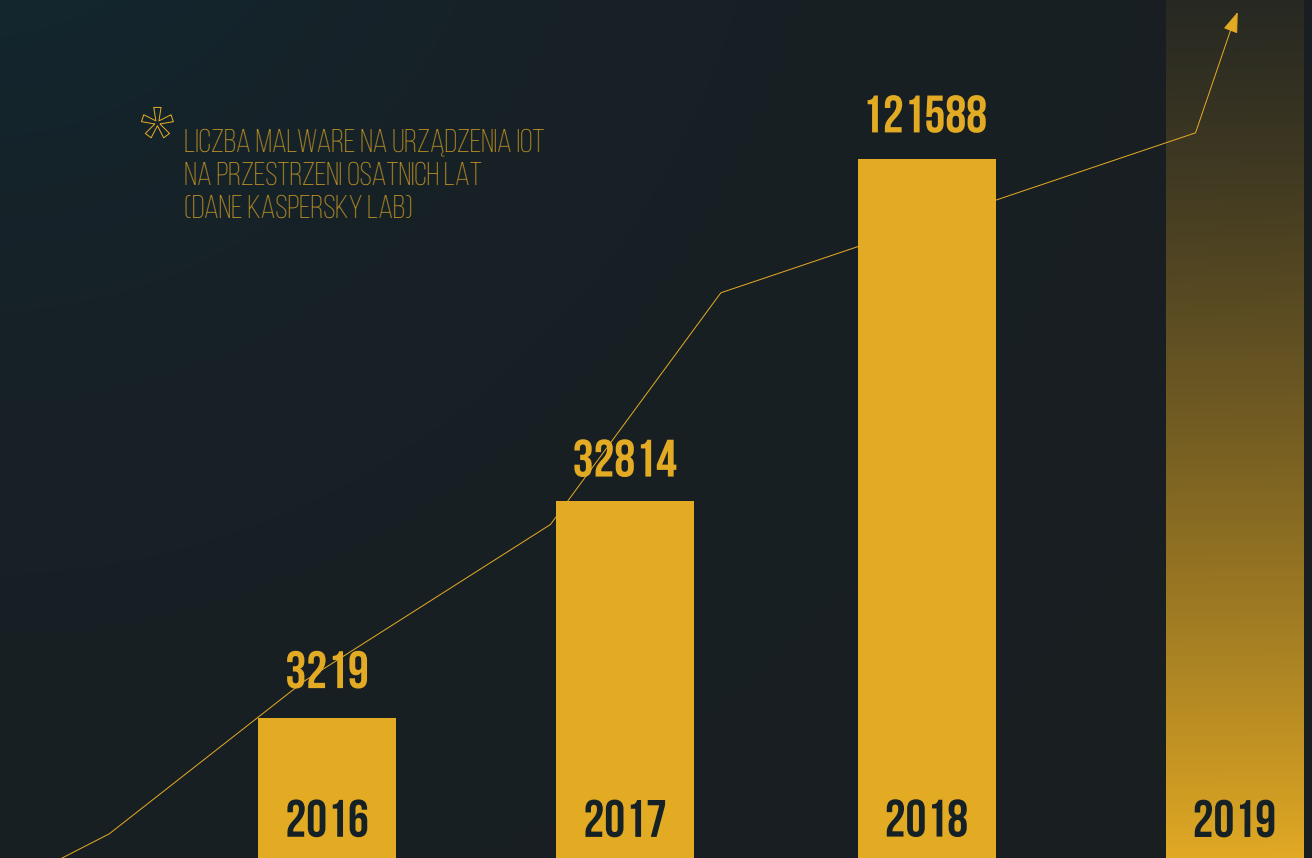
W Stanach Zjednoczonych jeden z ataków sparaliżował pracę kilku dużych agencji prasowych. W Niemczech jedna z większych hut stali padła ofiara ataku, który skutkował wstrzymaniem produkcji i spowodował trwałe straty.

Rodzime przedsiębiorstwa odstają jeszcze pod względem nowoczesnych rozwiązań od zachodnich firm. Jednak i w Polsce należy spodziewać się wzrostu zainteresowania technologią, która pozwala przecież maksymalizować zyski przedsiębiorców.

SECURITY SOLD SEPERATELY

Już w 2018 roku Garner prognozował wzrost ilości przemysłowych urządzeń IoT do poziomu 50 miliardów wdrożonych sprzętów IoT. Zarobią one dla przedsiębiorstw łącznie 19 trylionów dolarów. Imponujące zyski płynące z wprowadzonych uprawnień zachęcają kolejne firmy do przejścia na nowy poziom rozwoju.

Niestety, oferty producentów IoT wybierane są pod kątem efektywności i kosztów. Poziom bezpieczeństwa nie jest pierwszą wartością na którą zarząd zwraca uwagę. Dla cyberprzestępców oznacza to błogosławieństwo nowych wektorów ataku.



CLOUD MANAGED ACCESS POINT

Zarządzane z poziomu chmurowej konsoli punkty dostępowe WatchGuard posiadają wbudowany bezprzewodowy IPS (wireless Intrusion Prevention System). W ten sposób ochrona WatchGuard przenoszona jest na bezprzewodowe urządzenia IoT. Opatentowana technologia Market Packet pozwala zapewnić najbardziej niezawodny WIPS na rynku, z najniższą liczbą false positives. Dodatkowo WatchGuard Cloud Managed Wi-FI jest jedynym zweryfikowanym przez Miercom. Oznacza to gwarancję zabezpieczenia sieci przed wszystkimi sześcioma znanymi zagrożeniami Wi-Fi. Może być też używane razem z zastaną infrastruktury.

Access Point AP 420

Access Point stworzony by przetrwać ekstremalne warunki panujące w środowiskach produkcyjncych, na halach fabrycznych i na zewnątrz budynków przemysłowych

SEGMENTACJA IIOT

Dzielenie sieci na segmenty pozwala wyizolować urządzenia IIoT, a przez to zapobiegać rozprzestrzeniającymi się w sieci atakom. Szybkie i skuteczne wdrożenie segmentacji sieci możliwe jest dzięki Urządzeniom WatchGuard Firewall. Teraz w serii T dostępny jest także pancerny firewall sprzętowy w wersji Rugged. Sprzęt ten odporny jest na czynniki zewnętrzne takie jak kurz, wilgoć i skrajne temperatury.

Firebox T35-R *Zaprojektowany z myślą o zakładach produkcyjnych WatchGuard Firebox Rugged jest odporny na skrajne warunki, ekstremalną wilgotność i zmiany temperatury*

Chcieliśmy wdrożyć rozwiązanie, które pozwoli nie tylko chronić nasz biznes, ale także zapewnić gwarancję dostaw w kontrolowanym przez nas łańcuchu.

Nasze urządzenia WatchGuard nie wymagają wiele uwagi czy opieki - działają skutecznie od momentu wdrożenia , a to dokładnie to czego oczekiwaliśmy w naszym przedsiębiorstwie.

John Bogle, IT Manager, Sunday Engineering

IT KTÓRE POZOSTAJE W CIENIU

Shadow IT to maszyny i oprogramowanie używane w firmie bez wiedzy działu IT. Z pozoru to zupełnie niegroźne zjawisko. Pracownicy wymieniają się plikami i komunikują z kolegami z pracy za pośrednictwem usług z których korzystają też po pracy. Omijają za to rekomendowane platformy nad którymi dział IT sprawuje kontrolę.

Rosnąca skala zjawiska Shadow IT powinna jednak wzbudzać podejrzliwość działu cybersecurity. Dział operacyjny także może kupować, a potem wykorzystywać narzędzia, o których oficerowie bezpieczeństwa mogą nie wiedzieć. Taki sprzęt może umożliwić wycieki danych

WIDOCZNOŚĆ NIEAUTORYZOWANYCH URZĄDZEŃ

Nie możesz w pełni zabezpieczyć sieci, której nie rozumiesz. WatchGuard Network Discovery pozwala pracownikom IT zmapować całą sieć za firewallem. Technologia ta korzysta z nmap scan, DHCP, informacji w headerze HTTP lub aplikacji WatchGuard FireClient. Urządzenia w sieci oznaczone są ikonami, a do każdej przypisany jest szereg informacji:

- ✓ nazwa hosta
- ✓ adres IP
- ✓ adres MAC
- ✓ typu urządzenia (iOS, Android, MAC, Windows, etc)
- ✓ Otwarte porty - oraz aktywne protokoły

Dzięki jasnej klasyfikacji kadra IT może bardzo szybko podejmować skuteczne działania.

NAJCENNIEJSZE ZASOBY TO TE KTÓRYCH NIE KUPISZ!

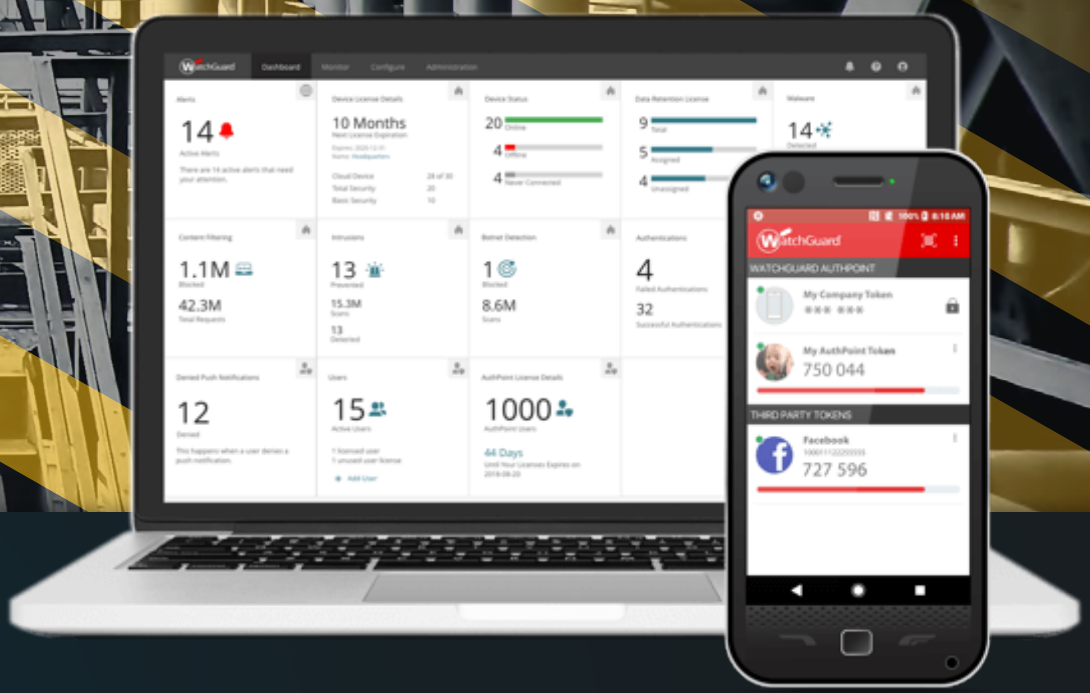
CHROŃ SWOJE KNOW-HOW

Kradzież własności intelektualnej od zawsze była znaczącym zagrożeniem w branży produkcyjnej. Aż 47% wycieków danych to właśnie kradzież własność. Kradzież cennych, niematerialnych zasobów przedsiębiorstwa to wyjątkowo kusząca perspektywa dla cyberprzestępców. Łupem mogą paść wszystkie cenne lub wrażliwe informacje takie jak dane o kontrahentach, projekty umów i oferty oraz gromadzone latami know-how przedsiębiorstwa.

Utrata takich zasobów oznacza dla przedsiąbiorstwa jedno - straty liczone w milionach. Dla przykładu, jeden z amerykańskich producentów klejów i epoksydów poniósł w wyniku kradzieży własności intelektualnej straty, które wyceniono na 15 milionów dolarów rocznie.

WIELOCZYNNIKOWA AUTENTYKACJA

Krytycznym krokiem na drodze do zabezpieczenia firmowych zasobów jest kontrola tego kto i w jaki sposób korzysta z danych. Kluczowa jest więc odpowiednia autoryzacja. Wieloskładnikowe weryfikowanie użytkowników sięgających po przetwarzane przez przedsiębiorstwo dane zapewnia WatchGuard AuthPoint.



CHESZ PRZETESTOWAĆ AUTHPOINT W SWOJEJ FIRMIE?

POMÓŻ NAM STWORZYĆ PIERWSZE POLSKIE CASE STUDY I ZDOBĄDŹ NAWET 100 DARMOWYCH LICENCJI

WYKWALIFIKOWANI PRACOWNICY DZIAŁU IT SĄ CORAZ TRUDNIEJ DOSTĘPNI

Na całym świecie zabraknie ich około 3.5 mln już w 2021. Szeroko zakrojona cyber moderniazacja przedsiębiorstw oznacza stale roznący popyt na oficerów bezpieczeństwa i informatyków. Branża produkcyjna jest szczególnie narażona na konsekwencje luk w kadrze IT. Zakłady produkcyjne, miejskie przedsiębiorstwa ciepłownicze lub wodociągowe wykorzystują najwięcej zaawansowanych narzędzi, które wymagają ochrony. Dodatkowo w przypadku sektora usług publicznych, świadczone przez przedsiębiorstwa usługi należą do krytycznych dla funkcjonowania całych społeczności. Dlatego też mogą być pod szczególnym ostrzałem cyberprzestępców i terrorystów.

WEBINARIUM # CYFROWA TRANSFORMACJA SEKTORA PRODUKCYJNEGO

Coraz bardziej zaawansowana technologia pozwala na jeszcze dalej idące zautomatyzowanie i usprawnienie pracy. Zjawisko to jest na tyle przełomową zmianą, że dorobiło się własnego terminu — Przemysł 4.0. Daleko idące zmiany dotykają także dostawców usług kluczowych. Zależność całych społeczności od dostaw energii elektrycznej czy wody pitnej nie umyka jednak cyberprzestępców. Dostrzegają oni kolejny, potencjalny target dla złośliwego oprogramowania.

W jaki sposób zabezpieczona powinna być sieć w Przedsiębiorstwie Energetyki Cieplnej czy wodno-kanalizacyjnym? Przyjrzyjmy się najlepszym praktykom informatyków dbających o bezpieczeństwo w sektorze usług kluczowych.

PLAN WYDARZENIA

- Myśl jak haker, działaj jak inżynier. 4 rewolucja przemysłowa i jej wpływ na bezpieczeństwo usług kluczowych
- Projekt sieci przemysłowej w praktyce
- Jakie ataki grożą obiektom przemysłowym?
- Od laptopa prezesa po IoT — zabezpiecz potencjalne wektory ataku

ZAPISZ SIĘ NA WEBINARIUM **06.12 GODZ. 10:00**

ŚNIADANIE # CYFROWA TRANSFORMACJA SEKTORA PRODUKCYJNEGO TECHNOLOGICZNE

Aby zminimalizować ryzyko zagrożenia, organizacje przemysłowe muszą wyjść poza ograniczenia dzisiejszych przepisów i zastanowić się, w jaki sposób poradzą sobie w przypadku ataku. Jak opracować i wdrożyć proporcjonalny i kompletny program naprawczy, który uwzględni aspekty krytyczne dla bezpieczeństwa systemów OT. Od edukacji każdego pracownika - personelu produkcyjnego i kierownictwa, po szkolenia specjalistów IT i bezpieczeństwa.

Pracujesz w sektorze energetycznym lub w usługach kluczowych? Weź udział w naszym Śniadaniu Technologicznym, na którym przedstawimy Ci zupełnie nowe podejście do kwestii cyberbezpieczeństwa urządzeń IoT.

PLAN WYDARZENIA

- Wprowadzenie do cyberbezpiecze w przemyśle 4.0
- Segmentacja sieci i izolacja kluczowych obszarów
- Uwierzytelnienie i autoryzacja maszyn
- Wyzwania i luki w zabezpieczeniach
- Ochrona danych i urządzeń IoT

ZAPISZ SIĘ NA WYDARZENIE **17.01 GODZ. 10:00**


NET COMPLEX
Bezpieczeństwo IT
WatchGuard