OCHRONA INFRASTRUKTURY O KLUCZOWYM ZNACZENIU PRZED ZAGROŻENIAMI CYBERNETYCZNYMI

WIELOASPEKTOWE PODEJŚCIE DO KWESTII CYBERBEZPIECZEŃSTWA W CELU OCHRONY DZIAŁALNOŚCI ORGANIZACJI

MOTOROLA SOLUTIONS

ATAKI CYBERNETYCZNE INFILTRUJĄ SEKTORY INFRASTRUKTURY O KLUCZOWYM ZNACZENIU

Sektory publicznej i komercyjnej infrastruktury o kluczowym znaczeniu takie jak energetyka, łączno i ratownictwo stały się podstawowym celem cyberprzestępców. Jak pokazuje ankieta instytutu Aspen, przeprowadzona z udziałem 625 kierowników działów IT odpowiedzialnych za infrastrukturę o znaczeniu kluczowym na całym świecie, w opinii 72% takich respondentów skala ataków cybernetycznych jest coraz większa. W ostatnim roku prawie 9 na 10 z nich miało do czynienia z przynajmniej jednym przypadkiem naruszenia bezpieczeństwa. Blisko połowa spodziewa się, że w ciągu najbliższych trzech lat dojdzie do ataku cybernetycznego, który może pociągnąza sobą ofiary śmiertelne[2].

Dla organizacji odpowiedzialnej za zarządzanie systemami infrastruktury o kluczowym znaczeniu ochrona własnego systemu przed cyberatakami jest kwestią pierwszorzędną. Ataki cybernetyczne nadchodzą ze wszystkich stron i stają się codziennością – ich źródłem może być zarówno pracownik nieświadomie podłączający do laptopa pamięć USB z wirusem, który infekuje całą sieć, jak i zorganizowane grupy cyberprzestępców, których działania wymierzone w infrastrukturę o kluczowym znaczeniu prowadzą do paraliżu całego miasta bądź kraju.

Wykorzystanie umiejętności i narzędzi specjalistów od cyberbezpieczeństwa może zapewnić Państwa organizacji stabilne, systematyczne podejście do kwestii odporności cybernetycznej.

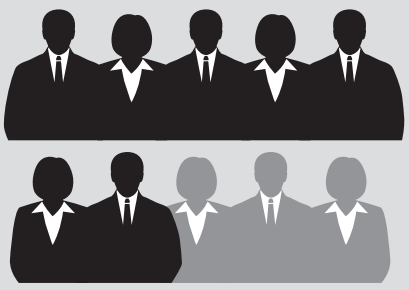
42.8 MLN

CYBERATAKÓW W 2014 R., WZROST O 48% W STOSUNKU DO ROKU POPRZEDNIEGO[1]

48%

OSÓB NA STANOWISKU CIO/ CSO UWAŻA, ŻE CYBERATAK MOŻE SPOWODOWAĆ OFIARY ŚMIERTELNE[2]

72%



SZEFÓW DZIAŁÓW IT JAKO GŁÓWNE ŹRÓDŁO WZROSTU CYBERATAKÓW WSKAZUJE BŁĘDY UŻYTKOWNIKÓW[2]

GŁÓWNYMI CELAMI ATAKÓW JEST SZESNAŚCIE BRANŻ

Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (Department of Homeland Security – DHS) sporządził wykaz 16 sektorów krajowej infrastruktury o kluczowym znaczeniu (National Critical Infrastructure – NCI)[3], które w przypadku ingerencji cybernetycznej mogłyby mieć wpływ na stabilność kraju i życie codziennie mieszkańców. Znaczenie ochrony takich systemów przed zagrożeniami cybernetycznymi i potencjalnymi atakami należy do głównych zadań kadry zarządzającej odpowiedzialnej za ich funkcjonalność.

Branża chemiczna

Obiekty handlowe

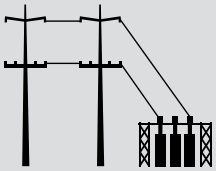
Komunikacja

Produkcja o znaczeniu krytycznym

Tamy

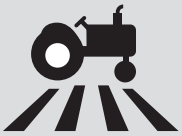
Baza przemysłowa obronności

Ratownictwo



Energetyka

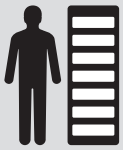
Usługi finansowe



Rolnicza produkcja żywności

Obiekty państwowe

Służba zdrowia i zdrowie publiczne



Informatyka

Reaktory, materiały i odpady jądrowe

Systemy transportowe

Gospodarka wodno-ściekowa

W CIĄGU OSTATNIEGO ROKU PRAWIE 9 NA 10 RESPONDENTÓW MIAŁO DO CZYNIENIA Z PRZYNAJMNIEJ JEDNYM PRZYPADKIEM NARUSZENIA BEZPIECZEŃSTWA SYSTEMÓW W SWOJEJ ORGANIZACJI[2]

SYSTEMATYCZNE PODEJŚCIE DO BEZPIECZEŃSTWA CYBERNETYCZNEGO
PROFESJONALNE USŁUGI MOTOROLA SOLUTIONS

Określenie i wdrożenie strategii w zakresie cyberbezpieczeństwa wiąże się z wieloma czynnikami. Jako organizacja zarządzająca infrastrukturą o kluczowym znaczeniu muszą Państwo znać i stosować branżowe normy cyberbezpieczeństwa oraz ramy kontroli ryzyka właściwe dla własnego sektora. Dodatkową komplikacją przy zapewnieniu odporności cybernetycznej jest konieczność bieżącego śledzenia dynamicznie ewoluującego charakteru zagrożeń cybernetycznych i słabych punktów sieci. Wczorajsze środki bezpieczeństwa mogą okazać się nieskuteczne wobec ataku cybernetycznego, który nastąpi jutro.

CERTYFIKOWANI, WYSZKOLENI EKSPERCI ZE ZNAJOMOŚCIĄ AKTUALNYCH TRENDÓW

Eksperci z firmy Motorola na bieżąco zapoznają się z nieustannie ewoluującymi globalnymi ramami i standardami cyberbezpieczeństwa. Niezależnie od tego, czy w grę wchodzi DISA STIG, NERC, NIST 800-53, ISO27001, CES, CIS, czy inna norma, Motorola jest gotowa do podjęcia współpracy z Państwa organizacją w celu wspólnego opracowania planu zapewnienia odpowiedniego poziomu zgodności. Choć jest to ważny etap, nasze kompleksowe podejście na nim się nie kończy. Ściśle współdziałamy z Klientem w celu poznania stanu jego ryzyka, opracowania planu zabezpieczenia jego integralności operacyjnej w ujęciu priorytetowym, a także określenia odpowiednich narzędzi i usług koniecznych do eliminacji występujących zagrożeń i słabych punktów.

RAMY CYBERBEZPIECZEŃSTWA	SYSTEMATYCZNA ANALIZA I PLAN
IDENTYFIKACJA OCENA RYZYKA	Przeprowadzenie szczegółowej analizy ryzyka Wykrycie potencjalnych słabych punktów
OCHRONA OPRACOWANIE ZABEZPIECZEŃ	Opracowanie polityk i procedur Wdrożenie odpowiedniego mechanizmu kontroli dostępu i audytu
WYKRYWANIE WCZESNE UJAWNIENIE	Stały monitoring w trybie całodobowym przez 365 dni w roku Umożliwienie czynności audytowych
REAGOWANIE PODJĘCIE DZIAŁAŃ	Przyjęcie stabilnego planu reakcji Korelacja, analiza, selekcja i reakcja na wykryte zdarzenia
DZIAŁANIA ODTWORZENIOWE PRZYWRÓCENIE FUNKCJONALNOŚCI	Wdrożenie planu awaryjnego Wprowadzenie ulepszeń w celu zapobieżenia atakom w przyszłości

CZY PAŃSTWA ORGANIZACJA JEST PRZYGOTOWANA NA CYBERATAKI?

5 ETAPÓW OCHRONY INFRASTRUKTURY O KLUCZOWYM ZNACZENIUSTRATÉGIQUE

ÉTAPE 1
Ocena środowiska przez zewnętrznych ekspertów ds. bezpieczeństwa posiadających kompleksową wiedzę na temat cybernetycznych i fizycznych słabych punktów systemu bezpieczeństwa i zagrożeń.

ÉTAPE 2
Opracowanie stabilnego planu zarządzania ogółem ryzyka i eliminacji wykrytych słabych punktów.

ÉTAPE 3
Aktywne monitorowanie systemu pod kątem potencjalnych zagrożeń w trybie całodobowym przez 365 dni w roku.

ÉTAPE 4
Maksymalizacja ciągłości działalności operacyjnej poprzez wprowadzenie poprawek w systemach i aktualizację elementów oprogramowania odpowiedzialnych za bezpieczeństwo.

ÉTAPE 5
Stała weryfikacja planów cyberbezpieczeństwa w celu eliminacji pojawiających się zagrożeń.

83%

RESPONDENTÓW UWAŻA CYBERATAKI ZA JEDNO Z TRZECH GŁÓWNYCH ZAGROŻEŃ

DLA DZISIEJSZYCH ORGANIZACJI, A JEDYNIE 38% DEKLARUJE PRZYGOTOWANIE NA TAKI ATAK[4]

AKTYWNY MONITORING DLA ZAPEWNIENIA STAŁEJ OCENY ZAGROŻEŃ

Cyberprzestępcy nie pracują „od-do”. Nie wystarczy po prostu zabarykadować sieci przy pomocy zaawansowanych firewalli, oprogramowania anti-malware, algorytmów szyfrujących i skomplikowanych mechanizmów kontroli dostępu. Konieczny jest stały monitoring systemu w trybie całodobowym przez 365 dni w roku, obejmujący wyszukiwanie nietypowych czynności, anomalii ruchu, podejrzanych przypadków logowania, zbyt wysokiej liczby prób nieudanego logowania itp. Sam monitoring to jednak za mało. Wymagana jest również analiza trendów systemowych, aby umożliwić diagnostykę potencjalnych incydentów cybernetycznych w czasie rzeczywistym. Według danych amerykańskiego Centrum Badań Strategicznych i Międzynarodowych (Center for Strategic and International Studies – CSIS) w 85% przypadków wykrycie naruszenia bezpieczeństwa trwa kilka miesięcy – średnio pięć[5].

Oferowana przez firmę Motorola usługa monitoringu bezpieczeństwa zapewnia kompleksową metodykę zdalnego monitorowania systemu Klienta pod kątem złośliwych ataków z wektorów zewnętrznych i wewnętrznych. W przypadku podejrzenia potencjalnego ataku nasi doświadczeni i wysoko wykwalifikowani eksperci podejmują zdecydowane środki zaradcze.

DWA PODEJŚCIA W ZAKRESIE OCHRONY SIECI

MONITORING ZDALNY

Dedykowani analitycy ds. cyberbezpieczeństwa w naszym Security Operations Center (SOC) prowadzą monitoring sieci Klienta w trybie całodobowym przez 365 dni w roku, podejmując w razie potrzeby działania naprawcze.

- Monitorowanie systemu Klienta przy pomocy najnowszych narzędzi analitycznych
- Międzysystemowa korelacja zdarzeń i pozyskiwanie informacji koniecznych do kompleksowej reakcji
- Identyfikacja, analiza i rozwiązywanie potencjalnych incydentów cybernetycznych

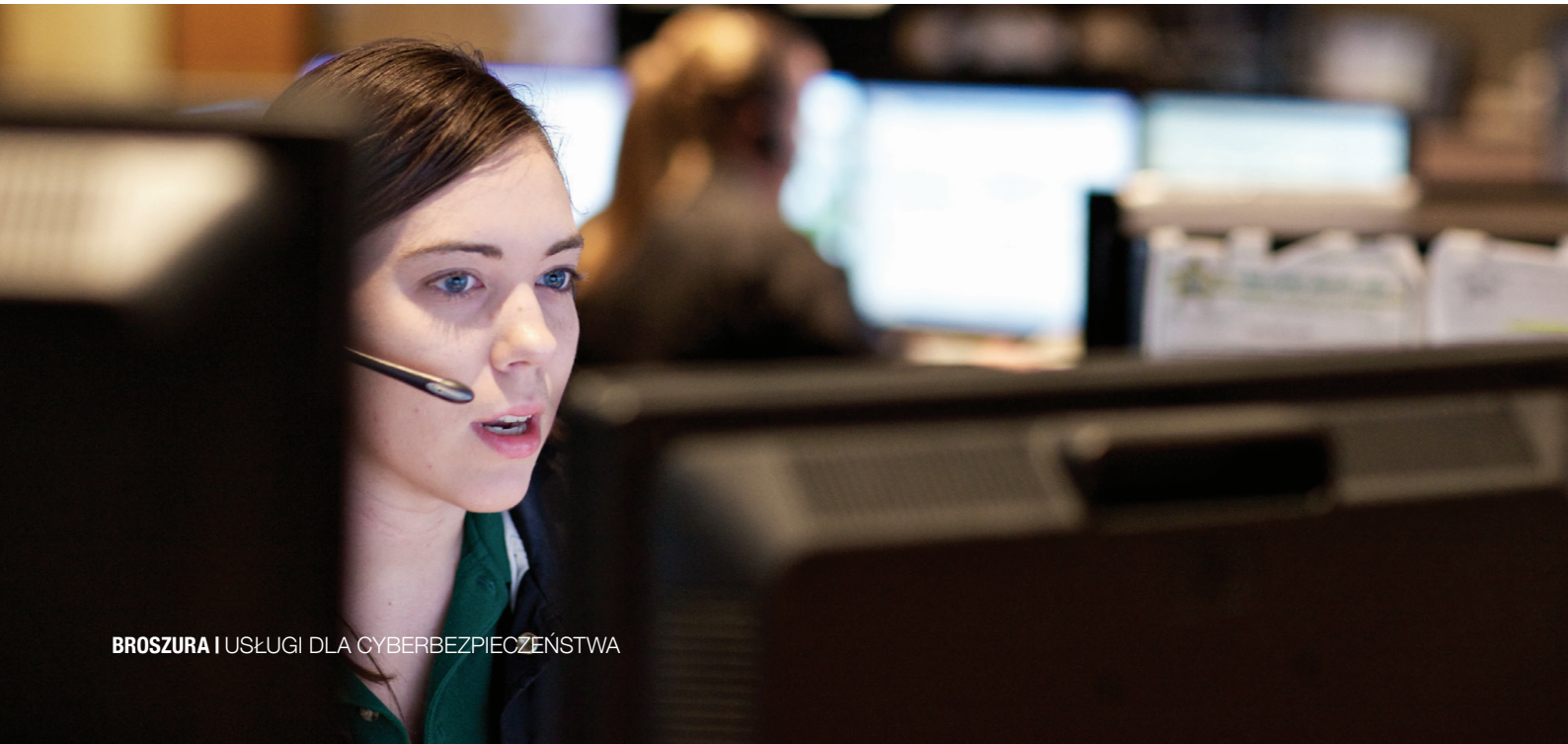
MONITORING NA MIEJSCU

Monitorowanie sieci przy pomocy narzędzi dostarczonych przez firmę Motorola Solutions.

- Indywidualny zestaw narzędzi umożliwiający monitorowanie systemu w ramach wyodrębnionego środowiska sieci Klienta
- Regularnie aktualizowane pulpity z niezbędnymi informacjami umożliwiającymi zespołowi Klienta identyfikację istotnych zdarzeń z zakresu bezpieczeństwa i podejmowanie stosownych działań – w tym przegląd stanu systemu z poziomu strony startowej
- Całodobowy dostęp do zespołu certyfikowanych ekspertów ds. bezpieczeństwa w firmie Motorola Solutions

SPRAWNE I SKUTECZNE SECURE OPERATIONS CENTER

Wykwalifikowani analitycy z Motorola Security Operations Center pracują przez całą dobę, chroniąc sieć Klienta przed zbliżającymi się zagrożeniami w obszarze cyberbezpieczeństwa przy zastosowaniu trójaspektowego podejścia: monitoringu w czasie rzeczywistym, aktywnej analityki i zdecydowanych działań w przypadku wykrycia incydentu. W razie identyfikacji potencjalnego zagrożenia wdrażamy działania zmniejszające zagrożenie i informujemy o nim organizację Klienta.



PRZETESTOWANE AKTUALIZACJE Z ZAKRESU BEZPIECZEŃSTWA ZAPEWNIAJĄ CIĄGŁOŚĆ DZIAŁANIA SYSTEMU

Obecne systemy do radiokomunikacji ruchomej lądowej o znaczeniu kluczowym oparte na protokole IP korzystają z różnorodnego oprogramowania firm trzecich, poczynając od programów antywirusowych, po produkty Microsoft®. Każdy taki program ma inny harmonogram aktualizacji. W przypadku ASTRO® 25 regularne uzupełnianie systemu o najnowsze aktualizacje oprogramowania ma kluczowe znaczenie dla jego ochrony w kontekście znanych słabych punktów i potencjalnych ataków cybernetycznych.

Aby uniknąć poważnych szkód, przed dodaniem takich aktualizacji zabezpieczeń do systemu konieczne jest ich przetestowanie. Pomoc przy walidacji aktualizacji zabezpieczeń zapewnia zespół certyfikowanych ekspertów ds. bezpieczeństwa firmy Motorola, co zmniejsza nakłady pracy obciążające personel Klienta. Wszystkie aktualizacje zabezpieczeń zostają wcześniej przetestowane w naszym dedykowanym laboratorium testowym, aby wyeliminować wszelkie ewentualne problemy w momencie instalacji oprogramowania w systemie Klienta. Zweryfikowane aktualizacje mogą następnie zostać zainstalowane przez firmę Motorola lub pobrane i zainstalowane przez personel IT Klienta.

OPCJA DOSTAWY ODPOWIADAJĄCA POTRZEBOM ORGANIZACJI KLIENTA

ZDALNA AKTUALIZACJA OPROGRAMOWANIA ODPOWIEDZIALNEGO ZA BEZPIECZEŃSTWO

Serwisanci firmy Motorola Solutions instalują w systemie poprawki oprogramowania odpowiedzialnego za bezpieczeństwo: wszystkie poprawki zostają zweryfikowane pod kątem optymalnego funkcjonowania, zbadana zostaje wydajność systemu o znaczeniu kluczowym, sporządzone zostają raporty na temat stanu systemu.

POBRANIE POPRAWEK PRZEZ KLIENTA

Po zatwierdzeniu poprawek przez zespół certyfikowanych ekspertów ds. bezpieczeństwa z firmy Motorola Solutions personel techniczny Klienta może pobrać najnowsze aktualizacje z bezpiecznej strony sieci Extranet i zainstalować oprogramowanie.

75%

ATAKÓW DOTYCZY SŁABYCH PUNKTÓW, KTÓRE MOŻNA BYŁO WYELIMINOWAĆ PRZY POMOCY DOSTĘPNYCH POPRAWEK[5]

MOTOROLA SOLUTIONS ZNA POTRZEBY INFRASTRUKTURY O KLUCZOWYM ZNACZENIU ORAZ ROLĘ, JAKĄ ODGRYWA ONA W ZAPEWNIANIU SPOŁECZEŃSTWU BEZPIECZEŃSTWA

Przypadki naruszania bezpieczeństwa przez ataki cybernetyczne stały się codziennością. Rolą każdej organizacji jest przygotowanie się na nie. Ochronę własnych systemów przed ingerencją cybernetyczną warto powierzyć liderowi w dziedzinie systemów łączności o kluczowym znaczeniu, jakim jest firma Motorola Solutions. Nasi eksperci ds. cyberbezpieczeństwa to wykwalifikowani profesjonaliści w swojej dziedzinie, przygotowani do współdziałania z organizacją Klienta w celu zagwarantowania jej poziomu usług dającego pewność właściwej identyfikacji zagrożeń cybernetycznych i zarządzania nimi. Więcej informacji o naszych usługach dla cyberbezpieczeństwa można uzyskać od przedstawiciela firmy Motorola Solutions.

ŹRÓDŁA:

1. Raport OAS Trends Micro na temat cyberbezpieczeństwa i infrastruktury o znaczeniu kluczowym w Amerykach za rok 2015
2. Raport na temat gotowości infrastruktury o znaczeniu kluczowym za rok 2015, The Aspen Institute
3. www.dhs.gov/critical-infrastructure-sectors
4. Raport ISACA na temat globalnego stanu cyberbezpieczeństwa za rok 2015
5. www.csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

Szczegółowe informacje na temat usług dla cyberbezpieczeństwa można uzyskać od przedstawiciela firmy Motorola Solutions, a także na stronie **motorolasolutions.com/cybersecurity**

Motorola Solutions Systems Polska s.p. z.o.o. Ul. Czerwone Maki 82 30-392 Krakow **motorolasolutions.pl**

MOTOROLA SOLUTIONS