POZNAĆ RYZYKO, ZANIM STANIE SIĘ ONO FAKTEM

PROFESJONALNE USŁUGI DLA CYBERBEZPIECZEŃSTWA

KOMPLEKSOWE I SYSTEMATYCZNE PODEJŚCIE DO ZARZĄDZANIA RYZYKIEM I OCHRONY INFRASTRUKTURY O KLUCZOWYM ZNACZENIU

BUDOWANIE ODPORNIEJSZYCH SIECI W EPOCE ROSNĄCEGO ZAGROŻENIA CYBERATAKAMI

Cyfrowy świat niesie ze sobą nieograniczone możliwości zwiększania wydajności, maksymalizacji wartości, a wreszcie poprawy jakości życia miliardów ludzi. Jednocześnie ma miejsce erupcja incydentów z zakresu cyberbezpieczeństwa, która jest źródłem wyjątkowych wyzwań zarówno dla podmiotów gospodarczych, jak i dla organów państwa. Wszechobecne są dziś ataki polimorficzne, zdolne do samodzielnej modyfikacji przy każdym uruchomieniu. Choć wiele organizacji chciałoby sądzić, że ich najbardziej wrażliwe informacje o kluczowym znaczeniu są bezpieczne, coraz częściej można się przekonać, że nikt nie jest całkowicie odporny na zagrożenia. Sfera cyberbezpieczeństwa nie ogranicza się do hakerskich ataków i technicznych mechanizmów kontroli.

Dynamika i szybka ewolucja cechuje również obszar regulacji i egzekwowania prawa w zakresie cyberbezpieczeństwa, co znów rodzi wyzwania związane z koniecznością dostosowania się do niezliczonych ilości norm branżowych przy jednoczesnym zachowaniu odpowiednich mechanizmów kontroli bezpieczeństwa. Ewolucja sieci o kluczowym znaczeniu, które stają się dynamicznymi systemami sieci wzajemnie połączonych o większej liczbie platform typu open source i rozwiązań opartych na chmurze, oznacza konieczność zarządzania i nadzoru obejmującego cały cykl eksploatacji systemu. Wiąże się to z potrzebą skoordynowanej i systematycznej weryfikacji zasobów ludzkich, procesów i technologii w celu zapewnienia organizacyjnej gotowości do zapewniania ochrony, wykrywania ewoluujących zagrożeń i reagowania na nie.

JAK ZBADAĆ STAN RYZYKA ZWIĄZANEGO Z CYBERBEZPIECZEŃSTWEM

Pakiet profesjonalnych usług dla cyberbezpieczeństwa (Cybersecurity Professional Services) firmy Motorola zapewnia proces kompleksowej i systematycznej identyfikacji, oceny i zarządzania ryzykiem związanym z cyberbezpieczeństwem we wszystkich systemach przedsiębiorstwa. Pakiet umożliwia szczegółowe zbadanie stanu ryzyka związanego z cyberbezpieczeństwem w otoczeniu operacyjnym Państwa organizacji. Motorola zapewnia kompleksową ocenę profilu powierzchni ataku, analizę stosunku kosztów do korzyści oraz szczegółowe zalecenia dotyczące działań naprawczych. Technologie i procesy biznesowe zmieniają się nieustannie, co oznacza, że zagrożenia również stale ewoluują, a stan bezpieczeństwa organizacji nigdy nie pozostaje statyczny. Okresowa ocena stanu bezpieczeństwa ułatwia prowadzenie bieżącej ewidencji słabych punktów i określanie priorytetu niezbędnych działań naprawczych w oparciu o ogólny poziom ryzyka prowadzonej działalności.

W 2014 r. amerykański Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST) opublikował dokument pt. „Ramy ulepszania cyberbezpieczeństwa infrastruktury o kluczowym znaczeniu" (Framework for Improving Critical Infrastructure Cybersecurity) przeznaczony dla organizacji dążących do osiągnięcia określonych wyników w obszarze bezpieczeństwa cybernetycznego. Obejmuje on praktyki różnych organów normalizacyjnych o sprawdzonej skuteczności wdrożeniowej. W opracowaniu ram obok instytucji państwowych i partnerów branżowych uczestniczyła również spółka Motorola Solutions. Oznacza to, że w ocenach przeprowadzanych przez firmę Motorola wykorzystane są zalecenia NIST, co odbywa się poprzez odwzorowanie ram cyberbezpieczeństwa NIST w procesach i procedurach bieżącego zarządzania ryzykiem danej organizacji w celu ustalenia jej aktualnych poziomów ryzyka związanego z profilem cyberbezpieczeństwa oraz sformułowania zaleceń.

RAMY CYBERBEZPIECZEŃSTWA NIST

IDENTYFIKACJA	OCHRONA	WYKRYWANIE	REAGOWANIE	DZIAŁANIA ODTWORZENIOWE
Otoczenie biznesowe	Polityki	Anomalie i zdarzenia	Planowanie reakcji	Planowanie działań odtworzeniowych
Kontrola ryzyka	Procesy	Procesy detekcyjne	Komunikacja	Ulepszenia
Zarządzanie zasobami	Bezpieczeństwo danych	Stały monitoring	Analiza	Komunikacja
Ocena ryzyka	Kontrola dostępu		Zmniejszanie ryzyka	
Zarządzanie ryzykiem	Technologia ochronna		Ulepszenia	
	Podnoszenie świadomości i szkolenia			

Infrastruktura o kluczowym znaczeniu ma charakter zróżnicowany i skomplikowany – w systemach tego rodzaju bezpieczeństwo jest konieczne dla zdolności szybkiego ich odtwarzania po wszelkiego rodzaju zagrożeniach, w tym także po zdarzeniach fizycznych i cybernetycznych. Nasze prace mające zapewnić możliwość ograniczenia ryzyka i prowadzenia działań zarządczych opierają się na identyfikacji aktywów, ocenie ryzyka w kontekście konsekwencji, słabych punktów i zagrożeń, określaniu priorytetów zmniejszania ryzyka, wdrażaniu programów ochronnych oraz pomiarze skuteczności.

LEPSZE ZARZĄDZANIE RYZYKIEM DZIĘKI IDENTYFIKACJI I REDUKCJI ZAGROŻEŃ

W ciągu długoletniej współpracy z podmiotami z sektora bezpieczeństwa publicznego, administracji rządowej i przedsiębiorstw zespół ds. profesjonalnych usług dla cyberbezpieczeństwa firmy Motorola wypracował holistyczne i metodyczne podejście do zarządzania ryzykiem, które zapewnia kompleksowe i treściwe wyniki uwzględniające priorytety ryzyka. Właściciele ryzyka i decydenci otrzymują ocenę właściwych czynników ryzyka opartą na starannych obliczeniach i materiale faktycznym.

ZAKRES	Do przeprowadzenia indywidualnej analizy ryzyka wybrane zostają wyłącznie właściwe mechanizmy kontroli typu technicznego, zarządczego i operacyjnego. Czynności z zakresu zmniejszania ryzyka, takie jak zmiany w architekturze bezpieczeństwa, integracja określonych produktów lub wdrożenie kontroli proceduralnej, są zalecane i omawiane z zainteresowanymi stronami dopiero po przeprowadzeniu metodycznej oceny środowiska i wykryciu, przeanalizowaniu i wyjaśnieniu czynników ryzyka oraz określeniu ich priorytetów.
PODEJŚCIE	Motorola Solutions analizuje potencjalne scenariusze zagrożenia i ocenia potencjalne skutki ryzyka w obszarze poufności, integralności i dostępności misji organizacji w oparciu o fizyczną obserwację, osobiste rozmowy oraz komercyjne i własne narzędzia manualne i komputerowe.
METODYKA	Wszelkie właściwe czynniki są brane pod uwagę i uwzględniane przed oceną i w jej trakcie. Po pozyskaniu wszelkich niezbędnych danych na temat zakresu oceny opracowywany jest profil zagrożenia, który zostaje ujęty w formie sprawozdawczej karty zarządzania ryzykiem (Risk Scorecard) ze wskazaniem niskich, umiarkowanych, wysokich i krytycznych wartości dla poszczególnych ustaleń/problemów. W związku z każdym problemem/ustaleniem sporządzane jest następnie zalecenie w sprawie zmniejszenia lub akceptacji ryzyka.

PROFESJONALNE USŁUGI DLA CYBERBEZPIECZEŃSTWA

ZARZĄDZANIE

- Analiza wpływu na działalność (Business Impact Analysis)
- Identyfikacja/klasyfikacja aktywów
- Ocena gotowości do stosowania ram NIST
- Ramowa struktura zarządzania i instytucjonalizacja
- Karta zarządzania ryzykiem cybernetycznym i kluczowe wskaźniki efektywności organizacyjnej (Key Performance Indicators – KPI)
- Polityka organizacyjna i opracowywanie norm
- Skuteczność procesów operacyjnych
- Modelowanie zagrożeń/informacje na temat zagrożeń
- Ocena ryzyka związanego z własnością intelektualną
- Ocena ryzyka związanego z procesami produkcyjnymi i procesami rozwoju oprogramowania przeniesionymi za granicę
- Bezpieczny cykl rozwojowy
- Analiza zagrożeń/badanie zagrożeń
- Ocena skutków w zakresie zgodności z wymogami regulacyjnymi
- Proces polityki zarządzania dostawcami zewnętrznymi
- Szkolenia i podnoszenie świadomości

ASPEKTY OPERACYJNE

- Doraźne zapytania klientów
- Pomoc w zakresie bezpieczeństwa operacyjnego
- Pomoc w zakresie reagowania na incydenty
- Analizy z zakresu informatyki śledczej
- Zindywidualizowany monitoring bezpieczeństwa
- Dedykowany monitoring procesu wykrywania anomalii
- Badania z zakresu inżynierii społecznej

ASPEKTY TECHNICZNE

- Oceny ryzyka technicznego w obszarze cyberbezpieczeństwa
  - Skanowanie pod kątem słabych punktów
  - Bezpieczeństwo aplikacji internetowych
  - Badania pod kątem penetracji sieci LAN i sieci bezprzewodowych
  - Badania fizyczne pod kątem penetracji
  - Ocena wdrożeń w chmurze
- Ocena zgodności
- Przegląd architektury sieciowej
- Rozwiązania z zakresu zarządzania tożsamościami i dostępem
- Ocena możliwości interakcji z systemami podmiotów zewnętrznych
- Ocena ryzyka związanego ze środowiskiem SCADA
- Wykrywanie urządzeń pracujących w sieci/inwentaryzacja aktywów
- Audyt aplikacji/przegląd kodów
- Architektura referencyjna bezpieczeństwa
- Bezpieczeństwo architektury przedsiębiorstwa
- Usługi kryptograficzne
- Bezpieczne wdrażanie technologii mobilnych
- Wdrożenie i monitoring systemu typu honeypot
- Zgodność z wymogami licencyjnymi oprogramowania typu open source

WARIANTY ŚWIADCZENIA PROFESJONALNYCH USŁUG DLA CYBERBEZPIECZEŃSTWA

W skład zespołu ds. profesjonalnych usług dla cyberbezpieczeństwa firmy Motorola wchodzą certyfikowani specjaliści ds. bezpieczeństwa przygotowani do stałego i aktywnego zapoznawania się z dynamicznie ewoluującym obszarem zagrożeń dla bezpieczeństwa i technologii służących zapewnieniu zgodności z wymogami. Wspólnie z Klientem określamy metodykę oceny, która w optymalny sposób odpowiada oczekiwanym wynikom biznesowym. Dostępne warianty:

REALIZACJA PRZEZ FIRMĘ MOTOROLA SOLUTIONS	WSPÓLNE ZAANGAŻOWANIE	KOORDYNACJA PODMIOTU ZEWNĘTRZNEGO
Zespół ds. profesjonalnych usług dla cyberbezpieczeństwa firmy Motorola przeprowadza kompleksową ocenę, a następnie formułuje zalecenia z uwzględnieniem priorytetów ryzyka.	Motorola Solutions kieruje danym zaangażowaniem, współdziałając z kadrą informatyczną Klienta w celu zapewnienia trwałości programu, wymiany informacji i współpracy eksperckiej.	Aby zapewnić udaną realizację zgodnie z oczekiwaniami klienta, do przeprowadzenia obiektywnej oceny pod nadzorem MSI wyznaczony zostaje renomowany podmiot zewnętrzny.

Ocena ryzyka związanego z cyberbezpieczeństwem wchodzi w skład naszego pakietu Premier, a w przypadku innych Klientów może być przeprowadzana na żądanie.

ROZWIĄZANIA MOTOROLA SOLUTIONS TO AKTYWNE USŁUGI ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z CYBERBEZPIECZEŃSTWEM

Jako światowy lider w dziedzinie technologii dla potrzeb operacji o znaczeniu w ponad 100 krajach firma Motorola Solutions jest w pełni świadoma zasadniczego znaczenia, jakie ma projektowanie, rozwijanie i wdrażanie technologii całkowicie skutecznych i bezpiecznych.

Coraz częściej można spotkać się z oczekiwaniami dotyczącymi bardziej kompleksowego podejścia do kwestii cyberbezpieczeństwa, z uwzględnieniem pełnego cyklu rozwojowego, wdrożeniowego i operacyjnego. Postęp technologiczny w dziedzinie komunikacji o kluczowym znaczeniu rozszerza powierzchnię ataku, co może zwiększyć podatność organizacji na przypadki naruszenia bezpieczeństwa.

Systemy o kluczowym znaczeniu są łakomym kąskiem dla cyberprzestępców, których zmysł technologiczny stale się rozwija. W efekcie połączenia tych tendencji rośnie ryzyko związane z dostępnością, poufnością i integralnością komunikacji głosowej i przesyłu danych o kluczowym znaczeniu. Dzięki zastosowaniu holistycznego podejścia do kwestii bezpieczeństwa systemu, obejmującego aktywne wykrywanie zagrożeń, reakcję w czasie rzeczywistym oraz działania naprawcze, Klient zyskuje komfortowe przekonanie, że jego system jest bezpieczny i odporny.

Szczegółowe informacje na temat profesjonalnych 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