CLOUDICA Be sure of IT

Microsoft

Wzmocnij strategię czyberbezpiecz -eństwa w ramach przygotowań do wejścia w życie NIS 2

Europejska dyrektywa w sprawie bezpieczeństwa sieci i informacji (NIS2) wprowadza nowe środki mające na celu zapewnienie, że organizacje działające w Unii Europejskiej (UE) lub we współpracy z nią mają wysoki wspólny poziom bezpieczeństwa sieci i infrastruktury.

Dyrektywa określa cele, które muszą spełnić wszystkie państwa członkowskie UE. Aby osiągnąć te cele do października 2024 r., poszczególne państwa muszą wdrożyć zapisy NIS2 do własnego prawa z możliwością wprowadzenia pewnych specyfik krajowych. Dyrektywy unijne są wiążące pod względem minimalnych wymagań wdrożenia.

Jako dostawca technologii bezpieczeństwa rozumiemy wyzwania, jakie stawia dyrektywa NIS2. Pozwól, że Ci pomożemy.

Rozwiązania zabezpieczające Microsoft, które pomogą spełnić wymagania NIS2

Dyrektywa NIS2 określa minimalne środki zarządzania ryzykiem w cyberprzestrzeni oraz obowiązki sprawozdawcze. Na szczęście wytyczne NIS2 pokrywają się z zasadami Zero Trust w rozwiązaniach zabezpieczających Microsoft, które zapewniają solidną ochronę przed cyberatakami na całej powierzchni ataku.

E-mail	Punkty końcowe	Tożsamości	Obciążenia chmury	Aplikacje chmury
Wyłudzanie informacji	Urządzenia niezarządzane	Dane logowania do konta	Zatrzymane usługi	Dostęp do aplikacji
Linki URL	Szyfrowanie plików	Infrastruktura	Usunięte kopie zapasowe	Eksfiltracja danych
Załączniki	Naruszone dane	Tożsamości obciążeń	Szyfrowanie plików	

Zintegrowana strategia bezpieczeństwa

Kluczem do skutecznej obrony przed cyberatakami są odpowiednio dobrane systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM) oraz szybkiego reagowania na wykrycie (XDR). Rozwiązania Microsoft zapewniają w pełni zintegrowane podejście do zabezpieczeń oraz usprawnione badanie zagrożeń i reagowanie na nie.

Microsoft Sentinel

Zyskaj wgląd w zagrożenia i zarządzanie nimi w całej infrastrukturze cyfrowej dzięki nowoczesnemu rozwiązaniu SIEM

Microsoft XDR

Powstrzymuj ataki i koordynuj reagowanie między zasobami dzięki rozwiązaniu XDR wbudowanemu w platformy Microsoft 365 i Azure

Analiza zagrożeń w usłudze Microsoft Defender XDR

Ujawniaj i eliminuj współczesne zagrożenia przy użyciu dynamicznej analizy cyberzagrożeń

W jaki sposób rozwiązania zabezpieczające Microsoft mogą pomóc?

1. Zapobieganie

- Najlepsza w branży ochrona przed ransomware
- Zalecenia konfiguracji w oparciu o zagrożenia
- AI i uczenie maszynowe automatycznie powstrzymują zagrożenia

2. Wykrywanie

- Detekcja oparta na AI natychmiast zatrzymuje atak
- Równoczesne działanie na różnych urządzeniach, tożsamościach, aplikacjach, poczcie e-mail, danych i obciążeniach chmury

3. Reagowanie

- Ujednolicone środowisko badania i usuwania zagrożeń
- Centrum dowodzenia i kontroli w usłudze Microsoft Sentinel
- Automatycznie tworzone kopie zapasowe danych pozwalają szybko wrócić do pracy

Zgodność z wymaganiami NIS2

- Analiza ryzyka
- MFA
- Szyfrowanie
- Szkolenia
- Bezpieczeństwo łańcucha dostaw
- Bezpieczeństwo sieci
- Obsługa incydentów
- Monitorowanie bezpieczeństwa

Chroń firmę przed cyberatakami i zapewnij zgodność z przepisami dzięki rozwiązaniom zabezpieczającym Microsoft

72%
mniejsze prawdopodobieństwo naruszenia bezpieczeństwa

50%
wyższa wydajność zespołów IT i bezpieczeństwa

25%
niższe koszty licencji rozwiązań zabezpieczających

Źródło: Badanie przeprowadzone na zlecenie przez Forrester Consulting: „The Total Economic Impact™ Of Microsoft Security", luty 2023 r. Wyniki dotyczą organizacji złożonej.

Pomożemy Ci wykonać pierwsze kroki

Jako partner Microsoft z wieloletnim doświadczeniem w dostarczaniu rozwiązań zabezpieczających chcemy zaoferować klientom najwyższy poziom zabezpieczeń i zapewnić im zgodność z przepisami wchodzącej niebawem w życie dyrektywy NIS2. Skorzystaj z naszej oferty.

Porozmawiajmy o tym, co możemy wspólnie zrobić.

Skontaktuj się z nami już dziś