Jste připraveni na aktualizovanou regulaci kybernetické bezpečnosti NIS2?

NIS – základní fakta

Cílem směrnice NIS je zvýšit úroveň celkové bezpečnosti, odolnosti sítí a informačních systémů v celé EU.

1

Proč NIS2

Evoluce spojená s digitální transformací si vyžádala reakci v podobě novelizace stávající směrnice NIS.

2

Dopad v ČR

Až dalších 6 000 firem a organizací v ČR bude nově muset řešit kybernetickou bezpečnost.

3

Zásadní změna – rozšíření regulovaných subjektů

NIS2 se bude týkat např. zdravotnictví, energetiky, dopravy, digitální infrastruktury, infrastruktury finančních trhů a bankovnictví, poštovních a kurýrních služeb, výroby a zpracování potravin, výroby a distribuce chemikálií, ...

4

Povinnosti pro subjekty

Přijmout technická a organizační opatření k zajištění bezpečnosti sítí a informačních systémů. Řízení rizik, zvládání a hlášení incidentů, testování digitální a provozní odolnosti.

5

Vymahatelnost

Pokuty a sankce ve výši až 10 milionů EUR či 2 % z celkového celosvětového ročního obratu.

“

Rizika, zejména nové typy kybernetických útoků, technik a taktik, které útočníci využívají, se s rostoucí digitalizací služeb neustále vyvíjejí. Proto se stejně tak musí neustále inovovat i obranné a detekční strategie.

Petr Plecháček
Associate partner v EY Technology consulting

EY
Building a better working world

EY přístup k řešení

EY jako technologicky nezávislá společnost nabízí služby v oblasti adopce požadavků NIS2.

Kybernetickou bezpečnost a požadavky NIS2 nevyřeší jedna technologie.
Kybernetická bezpečnost musí být součástí celé vaší firemní kultury.

Fáze 1

Připravenost, soulad a strategie NIS2

- Připravenost a strategie pro zajištění souladu s NIS2
- Pochopení prostředí kybernetických hrozeb a dopadu kybernetických útoků na podnikání

Fáze 2

Zajištění digitální a provozní odolnosti

- Plán reakce na incidenty
- Schopnost detekovat, měřit, plánovat a reportovat

Fáze 3

Bezpečnost provozní technologie (OT)

- Zajištění vrstvené architektury pro zvýšení kybernetické odolnosti provozních technologií
- Adekvátní ochrana koncových provozních technologií (OT)

Cílem programu je adopce požadavků regulace NIS2 v nezbytné míře s orientací na relevantní hrozby, automatizaci a budoucí udržitelnost.

Identifikace relevantních rizik

Zaměření se na hrozby související s odvětvím s využitím historických dat globálních útoků

Obranná cvičení

Simulace reálných postupů, technik a taktik používaných útočníky pro testování schopností detekce a reakce

Konstantní měření stavu bezpečnosti

Efektivní reporting a identifikace skutečné bezpečnostní hrozby vašeho odvětví

Plán reakce na bezpečnostní incidenty

Mapa sekvenčních postupů a reakcí dle úrovně závažnosti incidentu

Zlepšení detekčních schopností

Zlepšení kvality a rozsahu detekce útoků (SIEM, SOAR, EDR, ...)

ey.com