Smernica NIS2 o kybernetickej bezpečnosti

Čo je NIS2?

NIS2 je smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Európskej únii. Smernica nadobudla účinnosť 16. januára 2023 a členské štáty EÚ ju musia transponovať do svojej legislatívy do 17. októbra 2024. Smernica zavádza viaceré nové pravidlá pre zaistenie kybernetickej bezpečnosti a ochrany organizácií proti hackerským útokom.

Koho sa NIS2 týka?

Nová smernica voči pôvodnej smernici a zákonu č. 69/2018 Z.z. o kybernetickej bezpečnosti významne rozširuje rozsah organizácií, pre ktoré je požadovaná implementácia opatrení v oblasti kybernetickej bezpečnosti. Vo všeobecnosti sa **NIS2** týka nasledovných oblastí priemyslu a sektorov:

Doprava, energetika, bankovníctvo a infraštruktúra finančných trhov, zdravotníctvo, vodovodné služby, verejná správa (na centrálnej aj regionálnej úrovni), odpadové hospodárstvo, poštové a kuriérske služby, výroba, spracovanie a distribúcia potravín, výroba zdravotníckych potrieb, výroba a distribúcia chemických látok, výroba zdravotníckych pomôcok, počítačových výrobkov, strojov, motorových vozidiel a el. zariadení, letectvo a kozmonautika, poskytovatelia digitálnej infraštruktúry a digitálnych služieb a výskumu, poskytovatelia riadených bezpečnostných služieb a poskytovatelia riadených služieb (poskytovatelia IT služieb).

Dôležitým kritériom pre určenie, ktoré organizácie budú podliehať novým pravidlám kybernetickej bezpečnosti, bude aj ich veľkosť, okrem horeuvedených faktorov.

Aké povinnosti z pohľadu implementácie bezpečnostných opatrení NIS2 prináša?

Organizácie patriace pod pôsobnosť **NIS2** budú musieť zaviesť technické a prevádzkové opatrenia, ktorých cieľom je zvýšenie odolnosti organizácií voči kybernetickým hrozbám. Tieto opatrenia sú založené najmä na nasledovných princípoch:

- podporovanie **aktívnej kybernetickej ochrany**, ktorá zahŕňa aktívnu prevenciu, odhaľovanie, monitorovanie, analýzu a zmierňovanie narušení bezpečnosti
- implementácia opatrení na riadenie kybernetických rizík, ktoré sú primerané existujúcim rizikám a ktoré by mali zahŕňať aj **technické opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom, ich odhaľovanie, reakciu na ne a zotavenie sa z nich**, ako aj opatrenia na zmiernenie ich vplyvu

- využívanie **inovatívnych technológií vrátane umelej inteligencie**, ktorej používanie by malo zlepšiť odhaľovanie a prevenciu kybernetických útokov
- zaistenie **bezpečnosti sietí a informačných systémov**
- presadzovanie bezpečnostného modelu nulovej dôvery (tzv. **Zero Trust**)
- presadzovanie implementácie opatrení, resp. riešení podporujúcich, resp. zabezpečujúcich:
  - segmentáciu siete
  - **správu identít a riadenie prístupov**
  - aktualizáciu a bezpečnú konfiguráciu zariadení a systémov
  - technológie zabezpečujúce **ochranu dát použitím kryptografie a šifrovania**
  - integráciu technológií posilňujúcich kybernetickú bezpečnosť, ako sú systémy umelej inteligencie alebo strojového učenia
- **zabezpečenie kontinuity činností**, ako je riadenie zálohovania a obnova systémov po havárii a krízové riadenie
- implementácia riešení na **odhaľovanie a odstraňovanie zraniteľností** sietí a informačných systémov
- využívanie riešení **viacstupňovej (MFA) alebo kontinuálnej autentifikácie**

Okrem smernice **NIS2**, ktorej požiadavky budú musieť byť postupne implementované v rámci jednotlivých organizácií, je už v súčasnosti platný zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti, ktorý už v dnes platnom znení veľkú časť vyššie uvedených opatrení obsahuje.

Čo to znamená pre organizácie spadajúce pod NIS2 a s čím vie Alanata pomôcť?

1. Implementovanie bezpečnostných procesov a vypracovanie bezpečnostnej dokumentácie

Information Security Management | **Risk Assessment** | **Security Policies & Documentation** | **Cybersecurity Audits / Compliance**

2. Implementovanie centrálnych nástrojov na zaznamenávanie udalostí a monitorovanie sietí a informačných systémov a ich používateľov

LOG Management | **NDR** (Network Detection & Response)

3. Implementovanie nástrojov na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí

SIEM (Security Infomation & Event Management) | **XDR** (Extended Detection & Response) | **EDR** (Endpoint Detection & Response) | **XIoT Threat Detection**

DLP (Data Leak Prevention)

4. Zabezpečenie detekcie, evidencie a riešenia kybernetických bezpečnostných incidentov

SOC as a service (Security Operation Center)

SOAR (Security Orchestration, Automation & Response)

5. Implementovanie nástrojov na zabezpečenie ochrany bezpečnosti a integrity sietí a na zabezpečenie viditeľnosti v rámci siete

NextGen FW

DDOS ochrana

Zero Trust Network Access

NAC (Network Access Control)

SD-WAN Security

6. Implementácia aktívnej kybernetickej ochrany web aplikácií

WAF (Web Application Firewall)

Web App and API Protection

7. Implementovanie riešení na detekciu a prevenciu prienikov a proaktívneho blokovania škodlivej sieťovej prevádzky

NDR (Network Detection & Response)

Network IPS (Intrusion Prevention System)

8. Implementovanie nástrojov na správu a overovanie identít a na riadenie prístupov

PAM (Privileged Access Management)

IDM (Identity Management)

AM (Access Management)

Adaptive Authentication / Fraud detection

CASB (Cloud Access Security Broker)

9. Implementovanie nástrojov podporujúcich bezpečnostnú hygienu v rámci infraštruktúry

Patch Management

Hardening

10. Implementovanie riešení na bezpečné mobilné pripojenie do siete a vzdialený prístup použitím dvojfaktorovej autentifikácie

MFA
(Multi Factor Authentication)

11. Implementovanie riešení zabezpečujúcich ochranu dát použitím kryptografie a šifrovania

Data Protection

PKI Infrastructure

HSM
(Hardware Security Module)

12. Implementovanie procesov a nástrojov určených na detegovanie existujúcich zraniteľností programových a technických prostriedkov

Vulnerability Management

Infrastructure vulnerability scanning / pen. testing

WEB app vulnerability scanning / pen. testing

Threat Intelligence Feeds

13. Implementovanie systémov na ochranu proti škodlivému kódu a filtrovanie obsahu na rôznych úrovniach

AntiX ochrana

Web / Browsing Security

Sandboxing / Zero Day attacks protection

Email Security

14. Implementácia procesov a riešení podporujúcich zabezpečenie kontinuitu činností poskytovaných IT služieb

Business Continuity Management / ISO 22301

Data Backup & Archiving

- preventívne opatrenie
- reaktívne opatrenie
- monitoring

Alanata a. s.
Krasovského 14
851 01 Bratislava

+421 2 502 67 111
info@alanata.sk
www.alanata.sk

Alanata
Technology Meets Business