cluster kybernetickej bezpečnosti

LEPŠIA ŠTIPKA PREVENCIE, AKO VRECE NÁPRAVNÝCH OPATRENÍ

Pripravte sa na rozšírenie pôsobnosti zákonných povinností v kybernetickej bezpečnosti.

NIS2

NIS2 je vynovená smernica NIS (Directive on security of network and information systems), ktorá začne platiť po preklopení do slovenského zákona o kybernetickej bezpečnosti už v roku 2024.

V roku 2023 majú firmy z verejného, ale aj súkromného sektora, čas na prípravu plnenia povinností.

PREČO BY SME SA MALI ZAUJÍMAŤ O NIS2?

Prvým dôvodom budú povinnosti plynúce z legislatívy. Druhým dôvodom je všeobecný stav kybernetickej bezpečnosti. **Rapídny nárast počtu kybernetických útokov nepostihuje iba veľké spoločnosti, ale aj malé a stredné podniky z dôvodu nižšej úrovne zabezpečenia.** Počet útokov typu ransomware podľa dostupných štatistík narástol medziročne až o 62%. Celkovo boli napadnuté 2 organizácie z 3. Náklady na riešenie útokov, neboli takisto zanedbateľné. Priemerná čiastka celkových nákladov bola v prepočte 1,9 mil €.

Efektívne čeliť útokom je však možné pomocou zavedenia bezpečnostných opatrení, ktoré práve NIS2 definuje a najmä sprísňuje. NIS2 vzhľadom na situáciu v štátoch EÚ, taktiež výrazne **rozširuje odvetvia a pododvetvia, ktoré budú povinne riešiť kybernetickú bezpečnosť.** Jedná sa o tieto nové odvetvia, ktoré pribudnú k súčasným:

- Zdravotníctvo - výroba a výskum liekov
- Diaľkové vykurovanie a chladenie
- Poskytovatelia služieb ICT
- Riadenie služieb IKT
- Vesmír
- Odpadové hospodárstvo
- Odpadová voda
- Kuriérske služby
- Potravinárstvo - výroba, distribúcia
- Výroba (automobilov, strojov, zdravotníckych prostriedkov, PC a elektronika
- Výskum
- Sociálne siete

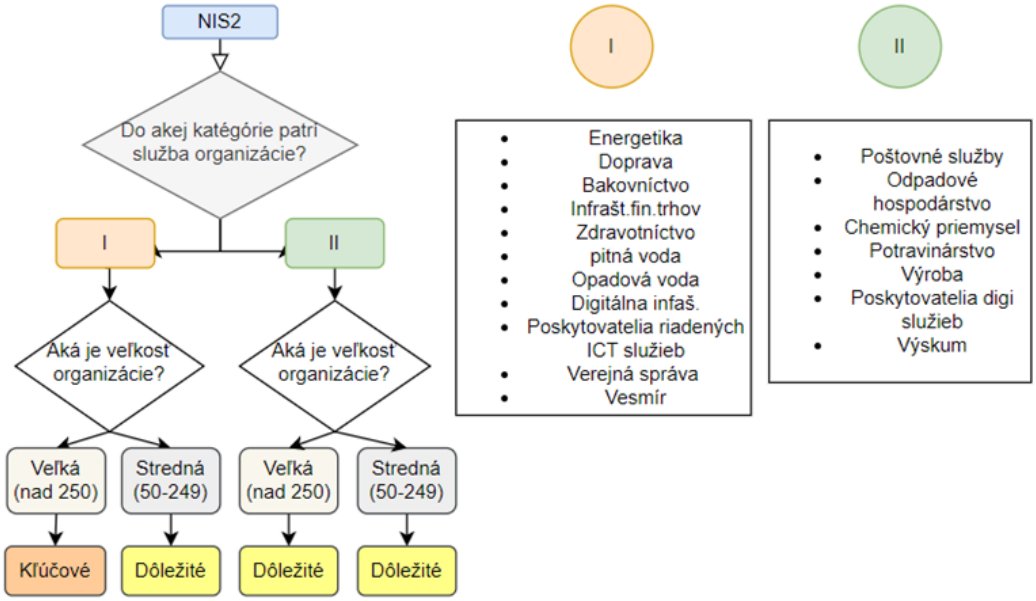
Rozsah bezpečnostných opatrení bude určený podľa regulovaného režimu, do ktorého spoločnosť spadne. **Bezpečnostné opatrenia sú povinné pre všetky regulované odvetvia.** Rozdiel bude len v prísnosti a rozsahu bezpečnostných opatrení.

REGULOVANÉ REŽIMY

Kľúčové subjekty (tzv.Essential) – **prísnejšie opatrenia**

Dôležité subjekty (tzv.Important) – **menej prísne opatrenia**

Prvá podmienka pre identifikáciu povinnej osoby je poskytovať aspoň jednu službu zo zoznamu regulovaných služieb. Druhá podmienka je veľkosť spoločnosti. **Regulované budú stredné a veľké podniky** (podľa platných definícií veľkostí podnikov). Pri niektorých službách bude organizácia regulovaná **bez ohľadu na veľkosť**.



KTO BUDE ZODPOVEDNÝ?

Novinkou, ktorú NIS2 prináša, je **zodpovednosť vrcholového manažmentu za zavedenie bezpečnostných opatrení** a ich dodržiavanie. V nadväznosti na zodpovednosť vrcholového manažmentu je povinnosť školení, nie len zamestnancov, ale aj spomínaného manažmentu.

ČO HROZÍ ZA NEDODRŽANIE POVINNOSTÍ?

Zmenou je aj výrazné navýšenie pokút za nedodržanie povinností ale aj iné typy sankcií.

- Pozastavenie licencie k poskytovanej službe, odobratie certifikácie
- Dočasný zákaz výkonu riadiacej funkcie fyzickej osobe v regulovanej organizácií
- Výška sankcie pre dôležitý subjekt – horná hranica 7 miliónov € alebo 1,4 % z obratu (to čo je vyššie)
- Výska sankcie pre kľúčový subjekt– horná hranica 10 miliónov € alebo 2 % z obratu (to čo je vyššie)

AKÉ POVINNOSTI BUDÚ PLYNÚŤ Z REGULÁCIE?

- Analýza rizík a politika bezpečnosti informačných systémov
- Riešenie incidentov (prevencia a odhaľovanie incidentov a reakcia na nich)
- Riadenie kontinuity prevádzky a krízové riadenie
- Zabezpečenie dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb, ako sú poskytovatelia služieb ukladania a spracovania dát alebo riadených bezpečnostných služieb
- Zabezpečenie obstarávania, vývoja a údržby siete a informačných systémov, vrátane zverejňovania informácií o zraniteľnostiach a ich riešení
- Politiky a postupy (testovanie a audit) za účelom posúdenia účelnosti opatrení na riadenie rizík v oblasti kybernetickej bezpečnosti
- Používanie kryptografie a šifrovania
  a mnoho ďalšieho...

Tápete v spomínaných pojmoch a kybernetickej bezpečnosti? Využite čas, ušetrite náklady a stres. Pripravte sa na plnenie povinností zo smernice. Nie ste na to sami.

Cluster Kybernetickej Bezpečnosti, Školská 10/119, 031 01 Liptovský Mikuláš
Telefón: +421 907 136 800, +421 948 220 263 Email: office@clusterkb.sk
www.clusterkb.sk

EURÓPSKA ÚNIA
Európsky fond regionálneho rozvoja
OP Integrovaná infraštruktúra 2014 – 2020

MINISTERSTVO HOSPODÁRSTVA SLOVENSKEJ REPUBLIKY