NIS2

S príchodom smernice NIS2 sa plánovaná revízia právnych predpisov v oblasti kybernetickej bezpečnosti zameriava na povinné opatrenia a posilnenie mechanizmov reakcie na kybernetické bezpečnostné incidenty s cieľom zlepšiť celkovú ochranu digitálnej infraštruktúry.

Tieto zmeny budú mať vplyv nielen na organizácie, ktoré už musia spĺňať požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a súvisiacej vyhlášky č. 362/2018 Z. z., ale aj mnohým ďalším subjektom, ktoré doposiaľ neboli zahrnuté do nariadenia a nemuseli plniť žiadne povinnosti v tejto oblasti.

Nový zákon o kybernetickej bezpečnosti by mal nadobudnúť účinnosť v roku 2024.
V zákone sa stanovuje jednoročné prechodné obdobie na prispôsobenie sa novým požiadavkám a ich postupné uplatňovanie.

Môžeme vám pomôcť implementovať NIS2 v troch krokoch.
Smernica NIS2 prináša do oblasti kybernetickej bezpečnosti významné zmeny. V nadväznosti na rozhodnutie o implementácii smernice do vnútroštátneho práva sa rámec povinností stanovený v dokumente transponuje do vnútroštátnych právnych predpisov prostredníctvom nového zákona o kybernetickej bezpečnosti a jeho vyhlášok.

Môžeme vám pomôcť najmä v týchto oblastiach:

Analýza súčasného stavu informačnej bezpečnosti

Analyzujeme súčasný stav vašej organizácie v oblasti kybernetickej bezpečnosti. Analýza bude zahŕňať najmä posúdenie systému riadenia informačnej bezpečnosti, bezpečnostnej dokumentácie, riadenia aktív, riadenia rizík, riadenia dodávateľov, riadenia ľudských zdrojov, riadenia zmien a riadenia prístupu. Súčasťou analýzy je aj riadenie udalostí a incidentov v oblasti kybernetickej bezpečnosti a riadenie kontinuity činností.

Analýza rizík

Ponúkame analýzu rizík na identifikáciu a posúdenie potenciálnych hrozieb a zraniteľností súvisiacich s aktívami vašej organizácie. Získate jasný prehľad o rizikách, ktoré by mohli ohroziť vašu bezpečnosť.

Vypracovanie alebo revízia bezpečnostnej dokumentácie

Vypracujeme alebo zrevidujeme dokumenty týkajúce sa vašich existujúcich interných zásad. Konkrétne vám môžeme pomôcť vytvoriť plán riadenia incidentov, plán obnovy, analýzu vplyvu, bezpečnostnú príručku pre používateľov atď.

Školenie

Na šírenie bezpečnostnej osvety vašich zamestnancov (od bežných používateľov, správcov zabezpečenia až po vrcholový manažment) ponúkame školenia prispôsobené potrebám vašej organizácie. Okrem prezenčnej formy je možné školenie realizovať aj formou e-learningu pomocou zábavných videokurzov, ktoré sú ukončené vedomostným testom.

Penetračné testovanie

Otestujeme schopnosť vašich systémov odolávať kybernetickým útokom. V správe popíšeme zraniteľnosti a navrhneme vhodné nápravné opatrenia, aby sme zabránili reálnym útokom.

Posilnenie bezpečnosti IT infraštruktúry

Môžeme vám pomôcť identifikovať slabé miesta v technickom zabezpečení vašej internej siete, implementovať bezpečnostné technológie, ako sú firewally alebo riešenia EDR, ktoré dokážu identifikovať, monitorovať a reagovať na podozrivé aktivity na koncových zariadeniach.

Ako vám môžeme pomôcť so systémom NIS2?

1

Definujeme požiadavky

Na úvodných stretnutiach s naším konzultantom zistíte všetky požiadavky zákona, ktoré je potrebné splniť.

2

Zhodnotíme situáciu

Vykonáme dôkladnú analýzu súčasného stavu informačnej bezpečnosti vo vašej organizácii. Posúdime vplyv smernice NIS2 a odporučíme konkrétne kroky a opatrenia na úplné splnenie všetkých požiadaviek smernice alebo kybernetického zákona a súvisiacich vyhlášok.

3

Realizujeme a implementujeme

Aktívne vám pomôžeme pri realizácii navrhovaných krokov vrátane prípravy dokumentov a zostavenia plánu školení pre zamestnancov. Počas celého procesu s vami budeme úzko spolupracovať.