ARICOMA

NIS2

Plánovaná revize právních předpisů v oblasti kybernetické bezpečnosti se s příchodem směrnice NIS2 zaměřuje na závazná opatření a posílení mechanismů pro reakci na kybernetické bezpečnostní incidenty, s cílem zlepšit celkovou ochranu digitální infrastruktury.

Tyto změny budou mít dopad nejen na organizace, které již dnes mají být v souladu s požadavky zákona č. 181/2014 Sb. o kybernetické bezpečnosti a navazující vyhlášky č. 82/2018 Sb., ale také na mnohé další subjekty, které dosud nebyly do regulace zahrnuty a nemusely plnit žádné povinnosti v této oblasti.

Nový zákon o kybernetické bezpečnosti by měl začít platit v říjnu roku 2024. Zákonem bude poskytnuta roční přechodná lhůta pro adaptaci na nové požadavky a jejich postupné plnění.

Pomůžeme vám s implementací NIS2 ve třech krocích.
Směrnice NIS2 přináší významné změny do oblasti kybernetické bezpečnosti. Na základě rozhodnutí o implementaci této směrnice do národního práva se rámec povinností stanovených v dokumentu přenáší do vnitrostátní legislativy prostřednictvím nového zákona o kybernetické bezpečnosti a jeho vyhlášek.

Pomůžeme vám zejména s těmito oblastmi:

Analýza současného stavu informační bezpečnosti

Provedeme analýzu současného stavu vaší organizace s ohledem na kybernetickou bezpečnost. Do analýzy zahrneme především posouzení systému řízení bezpečnosti informací, bezpečnostní dokumentace, řízení aktiv, řízení rizik, řízení dodavatelů, řízení lidských zdrojů, řízení změn a řízení přístupů. Jako součást analýzy také posuzujeme zvládání kybernetických bezpečnostních událostí a incidentů a řízení kontinuity činností.

Analýza rizik

Nabízíme provedení analýzy rizik, pomocí které identifikujeme a ohodnotíme potenciální hrozby a zranitelnosti spojené s aktivy vaší organizace. Získáte jasný přehled o rizicích, které by mohly ohrozit vaši bezpečnost.

Zpracování či revize bezpečnostní dokumentace

Zpracujeme či upravíme dokumenty s ohledem na vaše stávající interní politiky. Konkrétně vám můžeme pomoci vytvořit plán zvládání incidentů, plán obnovy, analýzu dopadů, bezpečnostní příručku pro uživatele apod.

Školení

Pro zvýšení bezpečnostního povědomí vašich zaměstnanců (od běžných uživatelů, bezpečnostních správců až po vrcholový management) nabízíme školení přizpůsobené potřebám vaší organizace. Školení lze realizovat kromě prezenční formy také e-learningovou formou za pomoci zábavných videokurzů, ukončených vědomostním testem.

Penetrační testování

Prověříme schopnost vašich systémů odolávat kybernetickým útokům. Ve zprávě popíšeme slabá místa a navrhneme vhodná opatření k nápravě, abyste zamezili reálním útokům.

Posílení bezpečnosti IT infrastruktury

Pomůžeme vám identifikovat slabá místa v technickém zabezpečení interní sítě, implementovat bezpečnostní technologie jako například firewall či EDR řešení, které dokáže identifikovat, monitorovat a reagovat na podezřelé aktivity na koncových zařízeních.

Jak vám s NIS2 pomůžeme?

1

Definujeme požadavky

Úvodní schůzky s naším konzultantem zahrnují identifikaci všech požadavků zákona, které je nezbytné splnit.

2

Posoudíme situaci

Provedeme důkladnou analýzu aktuálního stavu informační bezpečnosti vaší organizace. Posoudíme vlivy směrnice NIS2 a doporučíme konkrétní kroky a opatření k plnému splnění všech požadavků směrnice, resp. kybernetického zákona a navazujících vyhlášek.

3

Realizujeme a implementujeme

Aktivně vám pomůžeme s provedením navrhovaných kroků, včetně přípravy dokumentů a sestavení školícího plánu pro zaměstnance. Celým procesem projdeme v těsné spolupráci s vámi.