

NIS2 a její dopad na společnost



NIS2 je nová směrnice Evropské unie, která se stane součástí právního řádu České republiky v podobě nového zákona o kybernetické bezpečnosti.



Nové povinnosti v oblasti informační a kybernetické bezpečnosti: identifikace a hodnocení aktiv, analýza rizik, nastavení procesů pro řešení bezpečnostních incidentů, audit bezpečnostních opatření, nastavení šifrování, zabezpečení nouzové komunikace, zpracování plánů obnov a kontinuity činností apod.



Zavedení systému řízení bezpečnosti informací

Přípravná fáze: Příprava projektu

Výstupem je plán projektu s cílem zavedení NIS2, zahrnující níže uvedené fáze:

PRVNÍ FÁZE

Analýza současného stavu systému bezpečnosti informací

Výstupem je popis a posouzení současného stavu bezpečnosti informací v rovině:

- organizační (interní předpisy, procesy, jejich dokumentace)
- technické (zavedené bezpečnostní prvky)
- legislativní (dopad legislativy, jaký režim, jaké povinnosti)

DRUHÁ FÁZE

Návrh posílení systému bezpečnosti informací

Výstupem je identifikace a popis slabín systému bezpečnosti informací a konzultace vedoucí k rozhodnutí společnosti o tom, která opatření k posílení systému bezpečnosti informací zavede.

TŘETÍ FÁZE

Implementace vybraných opatření k posílení systému bezp. informací

Výstupem je zavedení vybraných opatření. Poskytneme konzultace a rady pro jejich efektivní zavedení a nastavení tak, aby dohromady se zbytkem systému tvořily soulad a byly efektivní.

ČTVRTÁ FÁZE

Provoz systému bezpečnosti informací

Poskytneme konzultace a rady pro zajištění dlouhodobého provozu systému řízení bezpečnosti informací.

Naučíme vás, jak se o systém starat, aby byl trvale funkční a nezkostnatěl.

Ing. Jiří Berger, MBA – znalec

Znalec v oboru kybernetika a výpočetní technika

NIS2 a její dopad na společnost



Ohrožení

- **Ztráta významných dlouhodobých zákazníků**, kteří NIS2 implementují a tento požadavek přenesou i na své dodavatele.
- **Ztráta obchodního kreditu firmy** při incidentu nebo nedostatečném nastavení pravidel kybernetické bezpečnosti.
- Maximální **pokuta za nedodržení** bude 10 000 000 EUR, nebo 2 % z celkového celosvětového ročního obrátu společnosti. Minimální výše není stanovena, sankce by však neměla být likvidační.
- **Správní tresty**, včetně pozastavení platnosti certifikace a pozastavení výkonu řídicí funkce (u poskytovatelů regulovaných služeb v režimu vyšších povinností).
- Možnost **pozastavení výkonu řídicí funkce fyzické osobě**, pokud se bude vrcholné vedení regulované organizace soustavně vyhýbat plnění svých zákonných povinností.



Kontakt

Ing. Jiří Berger, MBA

soudní znalec v oboru kybernetika
a výpočetní technika

tel. +420 603 434 861
jiri.berger@e-fractal.cz



Harmonogram



Lze očekávat **časovou náročnost v řádu měsíců** na zavedení souladu se směrnicí NIS2