ALEFNULA

Trust the Strong

Zákon o kybernetické bezpečnosti

Vláda ČR 2.1.2014 projednala návrh zákona o kybernetické bezpečnosti, který přináší významnou míru zabezpečení informačních technologií. Důvodem vzniku takového zákona je snaha konsolidovat obranu proti rostoucí hrozbě kybernetické kriminality, snížit dopady kybernetických incidentů a zavést právní regulaci v souladu s okolním světem, zejména s EU. Řešitelem kybernetické bezpečnosti se stal na základě usnesení vlády č. 781 z 19.10.2011 Národní bezpečnostní úřad (dále jen „NBÚ“). Ten se tak stal předkladatelem zákona o kybernetické bezpečnosti.

1 Pro koho je zákon o kybernetické bezpečnosti určen?

Na základě kvalifikačních kritérií NBÚ vypracuje seznam systémů, na které se bude zákon vztahovat. Systémy se rozdělí do 2 skupin:

Významné Informační Systémy (dále jen „VIS“) – základní úroveň bezpečnosti

Kritická Informační Infrastruktura (dále jen „KII“) – rozšířená úroveň bezpečnosti

Pro každou skupinu bude definován soubor činností a opatření v prováděcím právním předpisu k zákonu o kybernetické bezpečnosti, kterým musí v souladu s tímto zákonem každý správce takového systému vyhovět.

2 Co zákon pro správce určených systémů znamená?

Každý správce určeného systému musí především aplikovat soubor preventivních bezpečnostních opatření a plnit další reaktivní činnosti dle zákona. Bezpečnostní opatření se dělí na:

- **Organizační opatření**
- **Technická opatření**

Organizačními opatřeními se rozumí soubor procesů k zajištění vyšší bezpečnosti. Znění zákona se významně shoduje s požadavky certifikace ISO 27000. Technickými opatřeními se rozumí soubor technických nástrojů k zajištění vyšší bezpečnosti. Typicky se jedná o správnou implementaci a správu Firewallů, IPS sond, NetFlow sond, MDM systémů, kryptografických prostředků, ochrany proti škodlivému SW, SIEM nástrojů a dalších bezpečnostních prostředků...

3 Co by měl správce určeného systému dělat?

Správce určeného systému by měl analyzovat vlastní prostředí a definovat případné odchylky aktuální stavu od požadavků zákona. Měl by naplánovat další aktivity tak, aby byl v čase faktické účinnosti zákona (po 12 měsíční překlenovací lhůtě od data určení VIS, respektive KII) v souladu se zněním zákona.

4 Co můžeme nabídnout?

Orientujeme se v problematice zákona o kybernetické bezpečnosti. 20 let řešíme bezpečnostní strategie našich klientů formou správy ICT a implementačních projektů. Díky tomu můžeme správcům určených systémů nabídnout:

- **Informace** – formou workshopů a materiálů – vše zdarma
- **Konzultační služby** – formou auditů, studií a konzultačních činností – placená služba

Dejte nám 60 minut Vašeho času. Rádi za Vámi přijedeme a předáme Vám veškeré informace, které máme. Sami potom můžete zhodnotit, zda jsme vhodný partner pro zvládnutí problematiky Zákona o kybernetické bezpečnosti.

ALEF NULA, a.s.
U plynárny 1002/97, Praha 10
Česká republika
tel: +420 225 090 200
www.alef.com
cz-sales@alef.com

cisco Gold Partner