KYBERNETICKÁ BEZPEČNOST

VE SVĚTLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

S RŮSTEM ZÁVISLOSTI JEDNOTLIVÝCH ORGANIZACÍ A CELÉ SPOLEČNOSTI NA INFORMAČNÍCH SYSTÉMECH SE STÁVÁ NEZBYTNÝM ZAJIŠTĚNÍ JEJICH BEZPEČNOSTI VE VZTAHU NEJEN KE KYBERNETICKÝM HROZBÁM.

Se zvyšujícím se počtem nasazení informačních a komunikačních systémů pro podporu každodenních činností se zvyšuje závislost celé společnosti na správné funkci těchto systémů a proto se zvyšuje i potřeba dostatečné ochrany systémů a dat v nich uložených. Z tohoto důvodu se jednotlivé subjekty (zejména organizace) v rámci zajišťování informační bezpečnosti začínají chránit i před kybernetickými útoky a z kybernetické bezpečnosti se stává samostatná oblast v rámci bezpečnosti informací.

[LEGISLATIVA]

Na tento vývoj reagovala i státní správa zastoupená Národním úřadem pro kybernetickou a informační bezpečnost, který ještě jako Nárovní bezpečnostní úřad připravil a v roce 2014 vydal zákon o kybernetické bezpečnosti č. 181/2014 Sb. a navazující právní předpisy. Zákon pokrývá tři oblasti (v některých dokumentech označované jako „pilíře"), které mají za úkol zvýšit odolnost informačních a komunikačních systémů proti kybernetickým hrozbám a zefektivnit a zrychlit komunikaci a reakci v případě výskytu závažné kybertické hrozby:

- implementace bezpečnostních opatření zajišťujících základní nebo vyšší úroveň bezpečnosti informací a informačních systémů
- hlášení bezpečnostních incidentů CERTům a získávání informací o zranitelnostech a probíhajících útocích
- provádění reaktivních opatření a vytvoření legislativního rámce pro jejich prosazování ze strany NÚKIB.

VLASTNOSTI A VÝHODY

- Zvýšení úrovně zabezpečení informací v organizaci
- Splnění požadavků zákona a navazující vyhlášky
- Zvýšení připravenosti organizace v případě vzniku kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu
- Snížení rizik souvisejících s nedostupností, únikem či ztrátou informací v informačním nebo komunikačním systému
- Optimalizace nákladů na zajištění bezpečnosti informací na základě výsledků analýzy rizik

Povinnosti uvedené v zákoně se v plném rozsahu týkají zejména následujících skupin subjektů (typicky organizací) seřazených podle jejich předpokládané kritičnosti:

- správci a provozovatelé informačního nebo komunikačního systému, který je prvkem kritické infrastruktury,
- správci a provozovatelé informačního systému základní služby,
- správci významného informačního systému.

Z uvedené definice je vidět, že dopad zákona na subjekt určuje charakter jím provozovaných informačních nebo komunikačních systémů. Konkrétně se jedná o:

- komunikační nebo informační systémy kritické infrastruktury – tedy systémy takto určené NÚKIBem nebo Vládou ČR, informační systémy základní služby – tedy systémy takto určené NÚKIBem,
- významné informační systémy – tedy důležité IS systémy podporující činnost subjektů veřejné správy.

Výše uvedeným subjektům zákon ukládá zejména následující povinnosti:

- implementovat bezpečnostní opatření v minimálním rozsahu daném vyhláškou, doplněná o opatření vycházející z výsledků analýzy rizik,
- nastavit systém řízení bezpečnosti informací,
- určit osoby odpovědné za hlášení kybernetických událostí na CERT a za příjem informací od CERTů a za provádění reaktivních opatření (lokální CERT/CSIRT organizace; CSIRT - Cyber Security Response Team),
- předat kontaktní údaje CERTům.

Zákon i návazné právní předpisy vstoupily v platnost od 1. 1. 2015 a od té doby jsou průběžně aktualizovány tak, aby zohledňovaly vývoj hrozeb a bezpečnostní situaci ve světě a v ČR.

[NABÍZENÉ SLUŽBY]

Za účelem zajištění připravenosti organizace a splnění požadavků zákona nabízí ICZ následující skupiny služeb.

Analýza

V rámci této skupiny služeb ICZ nabízíme zhodnocení stavu bezpečnosti IS – provedení gap analýzy (identifikace které požadavky zákona a vyhlášky IS splňuje a které nikoliv).

Zavedení/revize systému řízení bezpečnosti

V oblasti systému řízení bezpečnosti ICZ nabízí služby vypracování, resp. revize stávajícího systému řízení bezpečnosti informací a provedení, resp. aktualizaci analýzy rizik. Při realizaci nabízené služby budou aplikovány požadavky zákona a vyhlášky a zohledněny požadavky normy ISO/IEC 27001:2013.

Návrh bezpečnostních opatření

V rámci této služby ICZ nabízí na základě zjištěného aktuálního stavu bezpečnostních opatření, požadavků vyhlášky a výsledků analýzy rizik návrh nových, resp. revizi stávajících bezpečnostních opatření. Při návrhu bude maximálně vycházet ze stávajícího stavu a bude využívat již existující opatření.

Implementace bezpečnostních opatření

V této oblasti ICZ nabízí jak služby vlastní implementace opatření (organizačních nebo technických), tak i konzultační služby v rámci implementace opatření tradičními dodavateli zákazníka.

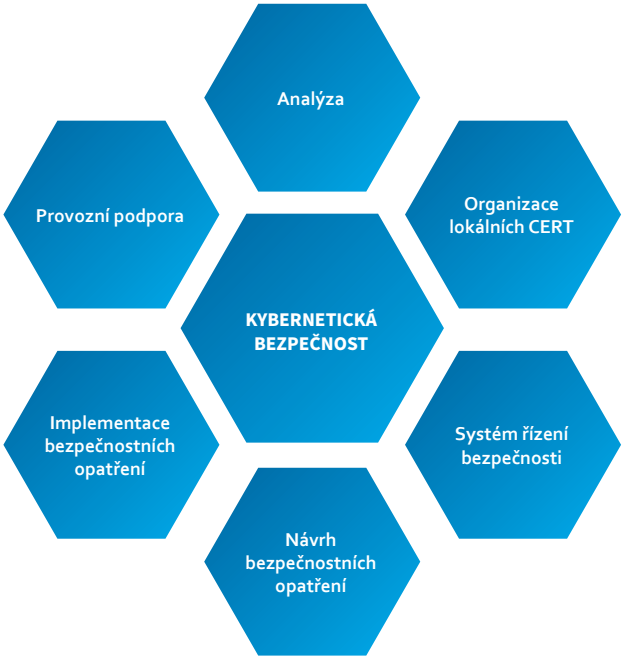
Jednotlivá opatření mohou nabývat různých forem dle možností a požadavků zákazníka – od čistě organizační formy, přes formu opensource nástroje, až po komerční enterprise řešení. Zde je ICZ připravena zohlednit možnosti a potřeby zákazníka a nabídnout odpovídající formu opatření.

Provozní podpora

Protože žádná bezpečnost, a tedy ani kybernetická, není statická, musí být její úroveň udržována množinou činností a procesů, které dohromady tvoří systém řízení bezpečnosti. V případě, že zákazník nemá dostatek kvalifikovaného personálu, je ICZ připravena nabídnout služby školení, outsourcingu vybraných rolí požadovaných vyhláškou, hodnocení stavu bezpečnosti IS (interní audit IS) a svěřené správy nebo provozní podpory implementovaných technologií.

[PRUŽNOST]

Výše uvedené služby je ICZ připravena kombinovat podle aktuálních potřeb zákazníka.



■ Kybernetická bezpečnost

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz