# KYBERNETICKÁ BEZPEČNOSŤ

## VO SVETLE ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

S RASTOM ZÁVISLOSTI JEDNOTLIVÝCH ORGANIZÁCIÍ A CELEJ SPOLOČNOSTI OD INFORMAČNÝCH SYSTÉMOV SA STÁVA NUTNÝM ZAISTENIE ICH BEZPEČNOSTI VO VZŤAHU NIELEN KU KYBERNETICKÝM HROZBÁM.

So zvyšujúcim sa počtom nasadení informačných a komunikačných systémov na podporu každodenných činností sa zvyšuje závislosť celej spoločnosti od správnej funkcie týchto systémov, a preto sa zvyšuje aj potreba dostatočnej ochrany systémov a dát v nich uložených. Z tohto dôvodu sa jednotlivé subjekty (najmä organizácie) v rámci zaisťovania informačnej bezpečnosti začínajú chrániť aj pred kybernetickými útokmi a z kybernetickej bezpečnosti sa stáva samostatná oblasť v rámci bezpečnosti informácií.

### [ ZÁKON ]

Na tento vývoj reagovala aj štátna správa zastúpená národným bezpečnostným úradom, ktorý pripravil a v roku 2014 vydal zákon o kybernetickej bezpečnosti č. 181/2014 Zb. a nadväzujúce právne predpisy. Zákon pokrýva tri oblasti (v niektorých dokumentoch označované ako „piliere"), ktoré majú za úlohu zvýšiť odolnosť informačných a komunikačných <adj11159></adj11159systémov proti kybernetickým hrozbám a zefektívniť a zrýchliť komunikáciu a reakciu v prípade výskytu závažnej kybernetickej hrozby:

- hlásenie bezpečnostných incidentov CERT-om (vládnemu a národnému CERT-u – Computer Emergency Respose Team) a spätné odovzdávanie informácií o zraniteľnostiach a prebiehajúcich útokoch,
- zavedenie bezpečnostných opatrení na ochranu významných informačných systémov a komunikačných alebo informačných systémov kritickej infraštruktúry a
- vykonávanie reaktívnych opatrení a vytvorenie legislatívneho rámca pre ich presadzovanie zo strany NBÚ.

### VLASTNOSTI A VÝHODY

- Splnenie požiadaviek zákona a nadväzujúcej vyhlášky
- Zvýšenie pripravenosti organizácie v prípade vzniku kybernetickej bezpečnostnej udalosti alebo kybernetického bezpečnostného incidentu
- Zníženie rizík súvisiacich s ne dostupnosťou, únikom či stratou informácií v informačnom alebo komunikačnom systéme
- Optimalizácia nákladov na zaistenie bezpečnosti informácií na základe výsledkov analýzy rizík

Povinnosti uvedené v zákone sa týkajú najmä nasledujúcich skupín subjektov (typicky organizácií) zoradených podľa ich odhadovanej častosti:

- správcovia významného informačného systému,
- správcovia komunikačného alebo informačného systému kritickej infraštruktúry,
- subjekty zaisťujúce významnú sieť elektronických komunikácií.

Z uvedenej definície vidieť, že dopad zákona na subjekt určuje charakter ním prevádzkovaných informačných alebo komunikačných systémov. Konkrétne ide o:

- významné informačné systémy – teda systémy, ktoré splnia kritériá uvedené vo vyhláške (podľa návrhu vyhlášky pôjde o základné registre, agendové informačné systémy editorov základných registrov, ISDS, IS podporujúce prvky kritickej infraštruktúry, ktoré nie sú kritickou informačnou infraštruktúrou, IS kľúčových správnych agend, IS poskytujúce služby a informácie obyvateľstvu a pod.)
- komunikačné alebo informačné systémy kritickej infraštruktúry – teda systémy takto určené.

Vyššie uvedeným subjektom zákon ukladá najmä nasledujúce povinnosti:

- určiť osoby zodpovedné za hlásenie kybernetických udalostí na CERT a za príjem informácií od CERT-ov a za vykonávanie reaktívnych opatrení (lokálna CERT/CSIRT organizácia; CSIRT – Cyber Security Response Team),
- odovzdať kontaktné údaje CERT-om,
- nastaviť systém riadenia bezpečnosti informácií,
- implementovať bezpečnostné opatrenia v minimálnom rozsahu danom vyhláškou, doplnené o opatrenia vychádzajúce z výsledkov analýzy rizík.

Zákon aj nadväzujúce právne predpisy vstúpil do platnosti od 1. 1. 2015 s prechodným obdobím 1 rok.

## [ PONÚKANÉ SLUŽBY ]

S cieľom zaistiť pripravenosť organizácie a splniť požiadavky zákona ponúka ICZ nasledujúce skupiny služieb.

### Analýza

V rámci tejto skupiny služieb ICZ ponúka službu klasifikácie IS z pohľadu zákona o kybernetickej bezpečnosti (či je IS významným informačným systémom, komunikačným alebo informačným systémom kritickej informačnej infraštruktúry) a službu zhodnotenia stavu bezpečnosti IS – gap analýza (identifikácia, ktoré požiadavky pripravovaného zákona a vyhlášky IS spĺňa, a ktoré nie).

### Organizácia lokálnych CERT/CSIRT

ICZ ponúka vytvorenie pravidiel a pre lokálny tím CERT/CSIRT (pravidlá, komunikačné matice, obsadenie požadovaných rolí, ...)

### Zavedenie/revízia systému riadenia bezpečnosti

V oblasti systému riadenia bezpečnosti ICZ ponúka služby vypracovania, resp. revízie existujúceho systému riadenia informačnej bezpečnosti a vykonanie, resp. aktualizáciu analýzy rizík. Pri realizácii ponúkanej služby budú aplikované požiadavky zákona a vyhlášky a zohľadnené požiadavky normy ISO/IEC 27001:2013.

### Návrh bezpečnostných opatrení

V rámci tejto služby ICZ ponúka na základe zisteného aktuálneho stavu bezpečnostných opatrení, požiadaviek vyhlášky a výsledkov analýzy rizík návrh nových, resp. revíziu súčasných bezpečnostných opatrení. Pri návrhu bude maximálne vychádzať z existujúceho stavu a bude maximálne využívať už existujúce opatrenia.

### Implementácia bezpečnostných opatrení

V tejto oblasti ICZ ponúka tak služby vlastnej implementácie opatrenia (organizačné alebo technické), ako aj konzultačné služby v rámci implementácie opatrení tradičnými dodávateľmi zákazníka.

Jednotlivé opatrenia môžu nadobúdať rôzne formy podľa možností a požiadaviek zákazníka – od čisto organizačnej formy, cez formu opensource nástroja, až po komerčné enterprise riešenia. Tu je ICZ pripravená v maximálnej miere zohľadniť možnosti a potreby zákazníka a ponúknuť zodpovedajúcu formu opatrení.

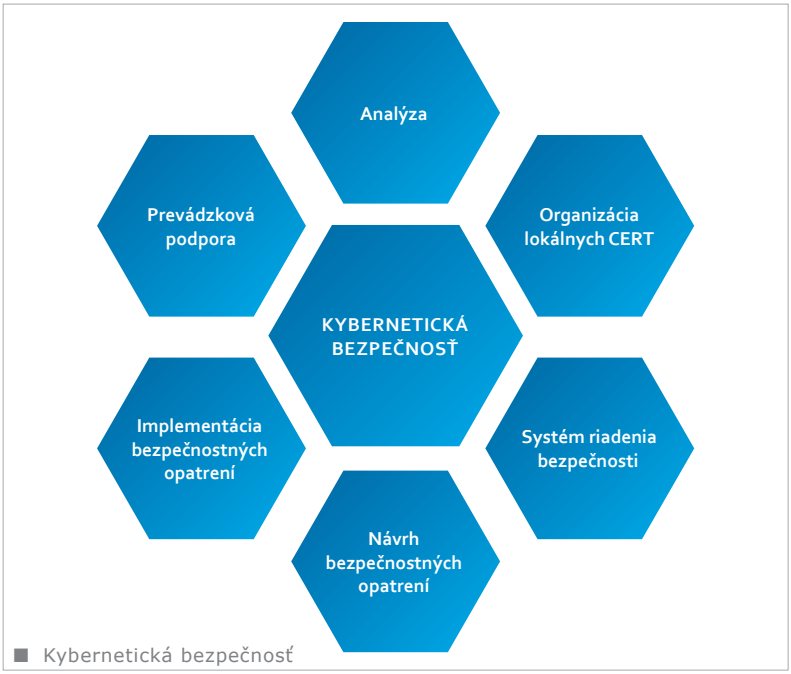
### Prevádzková podpora

Pretože žiadna bezpečnosť, a teda ani kybernetická, nie je statická, musí byť jej úroveň udržiavaná množinou činností a procesov, ktoré dohromady tvoria systém riadenia bezpečnosti.

V prípade, že zákazník nemá dostatok kvalifikovaného personálu, je ICZ pripravená ponúknuť služby školenia, outsourcingu vybraných rolí požadovaných vyhláškou, hodnotenia stavu bezpečnosti IS (interný audit IS) a zverené správy alebo prevádzkové podpory implementovaných technológií.

## [ PRUŽNOSŤ ]

Vyššie uvedené služby je ICZ pripravená kombinovať podľa aktuálnych potrieb zákazníka.



Kybernetická bezpečnosť

**OBCHODNÝ 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