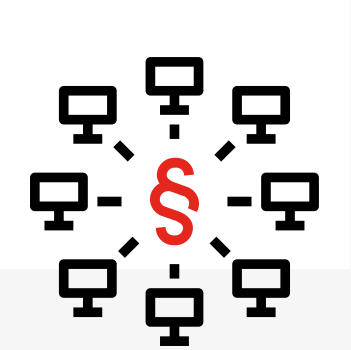
Aké bezpečnostné opatrenia priniesol zákon o kybernetickej bezpečnosti? Koho sa týkajú?



1. apríl 2020 bol dátumom, do ktorého mal každý prevádzkovateľ základných a poskytovateľ digitálnych služieb povinnosť zabezpečiť súlad svojej organizácie s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. To znamená, že vybrané firmy a orgány verejnej moci by mali mať do tohto dátumu okrem iného splnené požiadavky a prijaté bezpečnostné opatrenia uvedené najmä vo vyhláške č. 362/2018 Z. z., ako aj sektorové bezpečnostné opatrenia, ak pre daný sektor boli prijaté.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej iba „ZoKB“) nadobudol účinnosť pred dvoma rokmi 1. apríla 2018 a upravuje organizáciu, pôsobnosť a povinnosti v oblasti kybernetickej bezpečnosti a ustanovuje aj minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti. Tento zákon sa týka všetkých prevádzkovateľov základných služieb, ktorými sú okrem orgánov verejnej moci aj organizácie, ktoré poskytujú služby napr. v oblastiach bankovníctva (úverové inštitúcie), dopravy (cestná, letecká, železničná a vodná), energetiky (baníctvo, plynárenstvo, tepelná energetika a pod.), poštových služieb, zdravotnej starostlivosti, priemyslu (farmaceutický, hutnícky, chemický, inteligentný), kritickej infraštruktúry, ako aj poskytovateľov digitálnych služieb ktorými sú napr. online trhoviská, internetové vyhľadávače alebo poskytovatelia cloud computingových služieb. Uvedený zákon komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti a zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Okrem základných oznamovacích povinností a povinností spolupracovať s príslušnými orgánmi pri riešení vzniknutých kybernetických bezpečnostných incidentoch vyžaduje aj ďalšie povinnosti, ako sú:

- **povinnosť detegovať a riešiť kybernetické incidenty,**
- **zabezpečiť dôkazy o vzniknutých kybernetických bezpečnostných incidentoch,**
- **zaviesť bezpečnostné opatrenia s cieľom zabezpečenia kybernetickej bezpečnosti prevádzkovaných informačných systémov a sietí.**

Aké bezpečnostné opatrenia je nevyhnutné zaviesť?

Rozsah bezpečnostných opatrení je závislý od klasifikácie informácií a kategorizácie sietí a informačných systémov (ďalej iba „IS“) a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti. Opatrenia musia byť aplikované pre všetky siete a IS (vo všeobecnosti aktíva), od ktorých závisí poskytovanie základných služieb. Preto je veľmi dôležité hneď na začiatku mať jasne zadefinované, aké základné služby organizácia poskytuje a ktoré IS a siete tieto základné služby podporujú.

Implementácia bezpečnostných opatrení je vykonávaná s ohľadom na významnosť, funkcie a účely informácií a IS s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu poskytovaných základných služieb a kontrolnú činnosť. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. Prijímané bezpečnostné opatrenia majú zvyčajne charakter organizačných, resp. procesných, personálnych alebo technických opatrení.

Tempest
IT makes sense

Medzi základnú bezpečnostnú dokumentáciu, ktorú je potrebné mať vypracovanú patrí najmä:

- bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
- klasifikácia informácií a kategorizácia sietí a IS,
- analýza rizík kybernetickej bezpečnosti,
- procesy a procedúry pre manažment kybernetických bezpečnostných incidentov,
- stratégia a krízové plány na zabezpečenie dostupnosti siete a IS vrátane havarijných plánov.
- politiky, resp. predpisy pre jednotlivé oblasti bezpečnosti

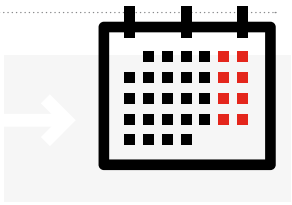
Súčasne je potrebné určiť manažéra kybernetickej bezpečnosti, ktorý bude niesť v organizácii zodpovednosť za riadenie kybernetickej bezpečnosti.

Okrem organizačných a personálnych opatrení je potrebné implementovať aj technické opatrenia akými sú napr.:

- nástroje na detegovanie existujúcich zraniteľností (nástroje na manažment zraniteľností, penetračné testy / skeny zraniteľností),
- nástroje na bezpečné mobilné pripojenie do siete a IS a na vzdialený prístup využívajúce dvojfaktorovú autentizáciu alebo kryptografické opatrenia,
- nástroje na ochranu integrity sietí a IS (segmentácia siete, firewally, IDS/IPS...),
- centrálny nástroj na zaznamenávanie činnosti sietí, IS a ich používateľov (sieťový a bezpečnostný monitoring, LOG manažment...),
- nástroje na správu a overovanie identity používateľov (IDM, AM, PIM...),
- nástroje na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí (SIEM, SOC...).

Veľa organizácií využíva na zabezpečenie prevádzky svojich sietí a IS aj služby externých spoločností. Dodávateľov, ktorí vykonávajú činnosti priamo súvisiace s prevádzkou sietí a IS, je nevyhnutné identifikovať a uzavrieť s nimi zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa ZoKB. Obdobná povinnosť platí aj v prípade podnikov poskytujúcich elektronické komunikačné služby alebo siete (ISP, resp. TELCO operátori).

Do kedy je potrebné jednotlivé opatrenia prijať?



Prevádzkovateľ základnej služby ako aj poskytovateľ digitálnej služby je povinný:

- **do dvoch rokov** odo dňa účinnosti ZoKB (**do 1. 4. 2020**):
  - **prijať bezpečnostné opatrenia**, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov,
  - **zosúladiť zmluvy** o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľmi na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov, so ZoKB.

Prevádzkovateľ základnej služby je ďalej povinný:

- **informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí** ku ktorému je sieť alebo IS základnej služby pripojená o skutočnosti, že organizácia bola zaradená do registra prevádzkovateľov základných služieb,
- **podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu** o výsledkoch auditu Národnému bezpečnostnému úradu najneskôr **do 9. 11. 2021**.

Ako na to?

Značnú výhodu majú tie organizácie, ktoré majú zavedený systém riadenia informačnej bezpečnosti, napr. podľa normy ISO 27001 alebo systém riadenia poskytovaných služieb v IT podľa normy ISO 20000-1. V prípade, ak patríte medzi túto skupinu organizácií, máte čiastočne vyhraté, pretože požiadavky právnych predpisov v oblasti kybernetickej bezpečnosti a spomínaných noriem sa vo viacerých oblastiach prekrývajú.

Bez ohľadu na to, či máte zavedený niektorý z manažérskych systémov alebo nie, je vhodné, ako prvý krok, vykonať analýzu aktuálneho stavu za účelom identifikácie oblastí, ktoré je potrebné zosúladiť s požiadavkami právnych predpisov v oblasti kybernetickej bezpečnosti.

Až následne je možné pristúpiť k samotnému zosúladeniu organizácie s požiadavkami platných právnych predpisov, t. j. implementácii bezpečnostných požiadaviek (technických, organizačných a personálnych), tvorbe dokumentácie a pod.

ZHRNUTIE

Vývoj v oblasti informačných technológií beží závratnou rýchlosťou. Informačné technológie sa stali súčasťou nášho každodenného života. Spracúvanie presných a správnych informácií ako aj dostupnosť informačných technológií sú nevyhnutné na fungovanie organizácie. Viac ako kedykoľvek predtým vzniká potreba chrániť informácie. Počet útokov sa z roka na rok zvyšuje. A otázka už nestojí, či na organizáciu niekto zaútočí, ale kedy sa to stane a či bude organizácia schopná tomuto útoku odolať.

Je dobré si uvedomiť, že napadnutie vašich systémov nesie vysoké reputačné riziko a môže spôsobiť obrovské škody. Nemalé sankcie vyplývajú aj z nezabezpečenia súladu so ZoKB, a to do výšky až 300.000 €, pričom táto sankcia môže byť aj zdvojnásobená v prípade opätovného porušenia povinností. Čiže je potrebné konať!

Prečo TEMPEST?

Ak je pre vás naplnenie legislatívy v oblasti kybernetickej bezpečnosti, ako aj samotná oblasť kybernetickej bezpečnosti veľkou neznámou, neviete kde a ako začať, nerobte si z toho ťažkú hlavu. Nemusíte sa s tým trápiť sami, ale môžete využiť služby externých spoločností, ktoré majú bohaté skúsenosti v tejto oblasti. Pri výbere vhodného partnera sa zamerajte na spoločnosti, ktoré majú všestranné skúsenosti v oblasti informačnej a kybernetickej bezpečnosti a vedia vám nielen identifikovať čo nemáte v súlade s legislatívnymi požiadavkami a navrhnúť spôsob zosúladenia sa s jednotlivými požiadavkami ZoKB, ale majú skúsenosti aj s návrhom optimálnych technológií na zabezpečenie kybernetickej bezpečnosti a v neposlednom rade aj s ich implementáciou. **V spoločnosti TEMPEST disponujeme špecialistami s dlhoročnými skúsenosťami v oblasti aplikačnej i analytickej bezpečnosti. V našich radoch máme odborníkov na súlad s príslušnou legislatívou, normami a nariadeniami ako aj držiteľov certifikátov CEH-Certified Ethical Hacker, CISSP-Certified Information Systems Security Professional, CRISC-Certified Risk and Information Systems Control a ďalších.**

Viac informácií nájdete na www.tempest.sk.

TEMPEST a.s.
EBC, Krasovského 14
851 01 Bratislava 5
Slovenská republika

Tel.: +421 2 502 67 111
Fax: +421 2 502 67 129
E-mail: info@tempest.sk
Web: www.tempest.sk

Tempest
IT makes sense