Metodické pokyny

o ďalších podrobnostiach a detailoch k spracovaniu minimálnych bezpečnostných opatrení v podniku.

Minimálne bezpečnostné opatrenia sa stanovujú s cieľom zjednotiť, určiť a zaručiť základnú úroveň ochrany bezpečnosti sietí a služieb vo všetkých podnikoch poskytujúcich verejné elektronické komunikačné siete alebo služby. Podnik pritom môže ďalej rozvíjať a zdokonaľovať bezpečnostný systém na ochranu bezpečnosti sietí a služieb nad túto základnú úroveň podľa svojich možností a potrieb.

Úrad využíva stanovené minimálne bezpečnostné opatrenia na kontrolu toho, či ochrana bezpečnosti sietí a služieb podniku je aspoň na základnej úrovni. Rozsiahlosť a podrobnosť postupov, ktorými podnik preukazuje plnenie minimálnych bezpečnostných požiadaviek má byť primeraná veľkosti a dôležitosti sietí alebo služieb podniku.

Tieto metodické pokyny obsahujú odporúčania pre podniky na detailnejší obsah minimálnych bezpečnostných opatrení.

(1) V oblasti riadenia bezpečnosti a manažmentu rizík, ktorá pokrýva riadenie sieťovej a informačnej bezpečnosti a manažmentu rizík je strategickým opatrením vypracovanie a udržiavanie bezpečnostnej politiky, ktorá rámcovým spôsobom určuje postoj a správanie podniku pri zabezpečovaní ochrany bezpečnosti sietí a služieb. Bezpečnostná politika podniku má určiť najmä:

a) bezpečnostné ciele podniku, spôsoby a kritériá ich vyhodnocovania a spôsoby kontroly postupov využívaných na ich dosahovanie,

b) úlohy vedenia podniku pri zaisťovaní bezpečnosti a integrity a vyhlásenie vedenia o podpore bezpečnostnej politiky podniku,

c) všeobecné a špecifické zodpovednosti a povinnosti v oblasti bezpečnosti,

d) povinnosti na zaistenie nenarušenia bezpečnosti a integrity,

e) súlad bezpečnostnej politiky podniku so všeobecne záväznými právnymi predpismi, s vnútornými predpismi podniku a jeho zmluvnými záväzkami,

f) rozsah a úroveň ochrany sietí alebo služieb,

g) rozsah a periodicitu vnútorného bezpečnostného auditu podniku,

h) dokumenty, ktoré podnik na zaistenie bezpečnosti a integrity vypracuje,

i) postupy pri revízii bezpečnostnej politiky podniku vrátane periodicity pravidelných revízií a dôvodov mimoriadnych revízií bezpečnostnej politiky.

Rámec na riadenie bezpečnosti a manažmentu rizík má stanoviť riziká ohrozenia sietí a služieb podniku, identifikovať slabé miesta, kritické aktíva podniku a určiť zásady ich ochrany.

Podniková štruktúra bezpečnostných úloh a zodpovedností zamestnancov podniku, ako aj postavenie a zodpovednosť tretích osôb v oblasti bezpečnosti sa má definovať a dokumentovať v súlade s bezpečnostnou politikou podniku.

Bezpečnostné požiadavky na siete alebo služby, dodávané podniku tretími osobami majú byť stanovené tak, aby zabezpečovanie prostriedkov a činností tretími osobami nezničovalo bezpečnosť podnikových aktív a procesov.

(2) Personálna bezpečnosť sa týka zamestnancov podniku ako aj tretích osôb. Rozsah oboznámenia s bezpečnostnou politikou podniku sa má stanoviť na základe toho, do akej miery alebo k akým aktívam podniku bude mať zamestnanec alebo tretia osoba prístup. Odporúča sa, aby sa zamestnanci a tretie osoby oboznámili s bezpečnostnou politikou a s povinnosťami z nej vyplývajúcimi predtým, ako začnú pre podnik vykonávať požadované úlohy a činnosti. Podnik má zabezpečiť aj oboznamovanie týchto subjektov o zmenách, ktoré v bezpečnostnej politike podniku nastanú v dobe platnosti ich vzťahu s podnikom.

Školenia pre zamestnancov podniku na udržanie a zdokonaľovanie ich bezpečnostných návykov, znalostí a zručností sa odporúča vykonávať pravidelne s periódami, ktoré si podnik zvolí primerane k bezpečnostným úlohám a zodpovednosti zamestnancov.

Bezpečnostné postupy pri personálnych zmenách, ako sú ukončenie pracovného pomeru, zmena pozície a zodpovednosti zamestnancov podniku alebo ukončenie a zmeny zmluvných vzťahov s tretími osobami sa majú týkať najmä riadenia prístupových práv, účtov, držby zariadení, údajov, dokumentov a pod.

Odporúča sa, aby si podnik vypracoval formálne postupy na právne vysporiadanie sa s porušením bezpečnostných opatrení zo strany zamestnancov, ako aj tretích osôb (disciplinárne konania, sankcie v zmluvách a pod.).

(3) Oblasť bezpečnosti systémov a zariadení obsahuje sieťové a informačné systémy a zariadenia, v ktorých sú tieto systémy umiestnené.

Na zaistenie fyzickej bezpečnosti a bezpečnosti prostredia pre zariadenia a infraštruktúru sietí a služieb sa odporúča umiestnenie dôležitých aktív podniku v priestoroch chránených pred poškodením vplyvom prírodných katastrof alebo človekom zapríčinených havárií a pred fyzickým vstupom nepovolaných osôb. Rozsah opatrení má byť primeraný identifikovaným rizikám ohrozenia.

Bezpečnosť sietí a služieb sa netýka len hlavných sieťových systémov a zariadení, ale aj od podporných prostriedkov, od ktorých závisí ich prevádzka ako sú napájacie zdroje, pohonné hmoty, klimatizácia a pod, preto má podnik venovať dostatočnú pozornosť aj vytváraniu vhodných záloh pre podporné systémy (napr. náhradné zdroje energie v prípade výpadku energetickej siete).

Zavedenie a udržiavanie riadenia prístupu pri vstupe do sieťových a informačných systémov sa týka identifikácie a autentizácie užívateľov, pravidiel a postupov na prístup k rôznym kategóriám údajov, bezpečnostných zásad využívania systémov, evidencie prístupov a pod.

(4) Oblasť riadenia prevádzky pokrýva riadenie a prevádzku sieťových systémov a informačných systémov zviazaných s poskytovaním sietí a služieb. Vypracovanie prevádzkových postupov a stanovenie zodpovednosti pre manažment aj obsluhu prispieva k znižovaniu možných ohrození bezpečnosti vplyvom chybných prevádzkových postupov a reakcií personálu. Odporúča sa zamerať najmä na riadenie zmien a aktualizácií sieťových a informačných systémov tak, aby sa minimalizovala pravdepodobnosť ich narušenia alebo chýb v dôsledku týchto činností. Pre možný návrat do stavu pred zmenou si má podnik uchovať pôvodné konfigurácie a nastavenia.

Postupy na riadenie konfigurácie a manažment aktív podniku majú jednoznačne identifikovať aktíva, spôsoby overenia ich dostupnosti a stavu.

(5) Manažment bezpečnostných incidentov sa týka detekcie a reakcie na bezpečnostné incidenty a s nimi súvisiacich komunikačných plánov na ohlasovanie a informovanie, vrátane určenia úloh a zodpovednosti.

Podnikové štandardy a postupy manažmentu bezpečnostných incidentov sa majú týkať zisťovania bezpečnostných incidentov a reakcií na vzniknuté incidenty, ako aj zabezpečenia prevencie pred vznikom alebo opakovaním bezpečnostných incidentov.

Monitorovacie a kontrolné postupy majú byť schopné odhaliť nielen zrealizované narušenia, ale aj pokusy o narušenie bezpečnosti.

Postupy reakcie na jednotlivé druhy bezpečnostných incidentov majú obsahovať analýzu bezpečnostných incidentov, stratégiu reakcie v technickej, riadiacej a legislatívnej oblasti, opatrenia a činnosti na obnovu alebo náhradu postihnutých aktív podniku.

Od všetkých zamestnancov podniku aj tretích osôb sa má vyžadovať, aby si všímali a hlásili informácie a okolnosti o možnom ohrození bezpečnosti a zraniteľnosti sietí a služieb.

(6) Riadenie kontinuity podniku sa týka ochrany sietí a služieb pred účinkami vážnych porúch systémov alebo katastrof a zabezpečenia ich rýchlej obnovy po takýchto udalostiach.

Stratégia a krízové plány na zabezpečenie kontinuity sietí a služieb majú obsahovať postupy na obnovenie prevádzky sietí a dostupnosti služieb v stanovených časových intervaloch po narušení alebo zlyhaní kritických procesov podniku.

Prostriedky na obnovu sietí alebo služieb bezprostredne po katastrofe majú zabezpečiť užívateľom poskytovanie aspoň základných komunikačných možností.

(7) Monitorovanie, skúšanie a vykonávanie auditov sa týka prevádzky a bezpečnosti sieťových a informačných systémov, zariadení a bezpečnostných opatrení.

Postupy na monitorovanie a na zaznamenávanie činností obsluhy sieťových a informačných systémov majú zabezpečiť podklady na identifikáciu možných chybných krokov obsluhy pri ohrození bezpečnosti.

Odporúča sa, aby podnik pravidelne preskúšaval záložné prostriedky a precvičoval krízové plány v prípade, ak je to vhodné aj v spolupráci s tretími stranami (napríklad s účasťou prevádzkovateľov sietí, ktoré využíva podnik na poskytovanie svojich služieb), a tým posilňoval svoju pripravenosť na možné ohrozenia bezpečnosti.

Pri skúšaní sieťových a informačných systémov, predovšetkým pri zavádzaní nových sietí, služieb, zariadení a pod sa odporúča tieto nové funkcie skúšať na systémoch oddelených od bežne využívaných sietí a služieb a do prevádzky ich uvádzať až po dôkladnom odskúšaní.

Politika posudzovania zraniteľnosti a skúšania bezpečnosti aktív podniku sa má zaoberať charakterom, rozsahom a časovým plánom vykonávania skúšok, ktoré majú preveriť ochranu bezpečnosti aktív podniku pred možnými ohrozeniami. Výkon takýchto skúšok bezpečnosti si podnik môže zabezpečiť nielen vlastnými prostriedkami, ale aj nezávislými expertmi.

Odporúča sa, aby si podnik pripravil aj plány na uskutočňovanie interných auditov bezpečnosti, ako aj postupy na nápravu auditom zistených bezpečnostných nedostatkov. Súčasťou môžu byť aj postupy na monitorovanie zhody podnikových bezpečnostných opatrení s internými predpismi podniku a s externými právnymi, regulačnými a zmluvnými požiadavkami a na odstraňovanie zistených nezhôd.