Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Smernica pre nahlasovanie a riešenie kybernetických bezpečnostných incidentov

Obec Lomnička

Verzia:	01.43
Platné od:	
Stav dokumentu:	Finálny
Dôvernosť dokumentu:	Interný
Typ dokumentu:	Interná Smernica pre nahlasovanie a riešenie kybernetických bezpečnostných incidentov
Priorita:	Štandardná

Autor dokumentu	e-mail	telefonický kontakt
CUBS plus, s.r.o.	kyber@cubsplus.sk oou@cubsplus.sk	0918/43 43 74 0903/608-164
Vlastník dokumentu	**e-mail**	**telefonický kontakt**
Obec Lomnička	obec@obeclomnicka.sk	0908 310 654 0948 164 202

Po zverejnení tohto dokumentu už nie sú všetky predchádzajúce verzie platné!
Po vytlačení a vytvorení lokálnych kópií sa dokument vyradí zo skupiny kontrolovaných dokumentov!

Obsah

1 Účel

1. **Obec Lomnička, IČO: 00330027, adresa: Obecný úrad Lomnička, Lomnička 66, 065 03 Podolínec** (ďalej len „PZS") – vydáva túto smernicu za účelom stanovenia postupu pre nahlasovanie a riešenie bezpečnostných incidentov.
2. V Slovenskej republike problematiku bezpečnostných incidentov a kybernetickej bezpečnosti upravuje zákon NR SR č. 69/2018 Z. z. o kybernetickej bezpečnosti, zákon NR SR č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a vyhláška NBÚ č. 362/2018 Z. z.

2 Rozsah

Smernica je záväzná pre všetkých zamestnancov PZS v rozsahu zodpovednosti vyplývajúcej z ich pracovného zaradenia alebo poverenia, pracovnej zmluvy, pracovnej náplne ako aj pre všetkých externých spolupracovníkov vykonávajúcich činnosť u prevádzkovateľa na základe iných právnych skutočností a zmlúv.

3 Definícia a vymedzenie základných pojmov

Z dôvodu lepšieho pochopenia princípov a postupov spojených s nahlasovaním a riešením kybernetických bezpečnostných incidentov je nevyhnutné vymedziť si niekoľko základných pojmov, bez ktorých by táto problematika v podmienkach PZS nebola správne pochopená.

Bezpečnostný správca (manažér kybernetickej bezpečnosti) – je nezávislá zodpovedná osoba, ktorá riadi oblasť kybernetickej bezpečnosti, taktiež sa zaoberá riešením kybernetického bezpečnostného incidentu a má za úlohu zabezpečiť všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident.
Správca aktíva – je zamestnanec prevádzkovateľa, ktorému bol pridelený súbor aktív (mobilné telefóny, počítače, kamerový systém, aplikačné vybavenie a podobne) a ktorý je v prípade kybernetického bezpečnostného incidentu zodpovedný za pridelené aktívum a taktiež za definovanie nápravných opatrení v súčinnosti s manažérom kybernetickej bezpečnosti.

V zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti sú základné pojmy vymedzené nasledovne:

Sieť - elektronická komunikačná sieť podľa § 2 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.
Informačný systém - funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov.

Kybernetický priestor - globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.

Kontinuita - strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni.

Dôvernosť - záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom.

Dostupnosť - záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná.

Integrita - záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené.

Kybernetická bezpečnosť - stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.

Riziko - miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami.

Hrozba - každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť.

Kybernetický bezpečnostný incident - akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií.

Prevádzkovateľ základnej služby - orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena l) zákona o kybernetickej bezpečnosti.

Riešenie kybernetického bezpečnostného incidentu - všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

4 Príklady kybernetických bezpečnostných incidentov

4.1 Únik prihlasovacích údajov

Popis: získanie prihlasovacích údajov používateľa útokom zvonka alebo prezradením zamestnanca.

Dôsledky: získanie prístupu k údajom a ich možný únik

Preventívne opatrenia: chrániť prístup do lokálnej počítačovej siete overením firewallom.

4.2 Neúmyselné prezradenie prihlasovacích údajov

Popis: neúmyselné prezradenie prihlasovacích údajov kolegom alebo osobe mimo organizáciu. Zverejnenie osobných údajov ich zaznamenaním v papierovej podobe a umiestnenie prístupu k nim.

Dôsledky: získanie prístupu k údajom a ich možný únik.
Preventívne opatrenia: poučenie zamestnancov o ochrane ich prihlasovacích údajov a zakázanie ich zverejňovania. Kontrolovať dodržiavanie týchto pravidiel.

4.3 Modifikácia údajov

Popis: neúmyselná alebo úmyselná zmena údajov v informačnom systéme.
Dôsledky: nesprávne údaje a prípadná ich strata.
Preventívne opatrenia: poučenie zamestnancov, logovanie vstupov do informačných systémov, pravidelná záloha.

4.4 Strata údajov

Popis: neúmyselné (pri poruche alebo havárii) alebo úmyselné (činnosť zamestnanca) vymazanie údajov.
Dôsledky: strata údajov.
Preventívne opatrenia: poučenie zamestnancov, logovanie vstupov do Informačných systémov, pravidelná záloha.

4.5 Strata alebo krádež USB kľúča

Popis: strata alebo krádež USB kľúča alebo USB zariadenia s citlivými údajmi
Dôsledky: získanie dokumentov s citlivými údajmi
Preventívne opatrenia: šifrovanie prenosných USB zariadení.

4.6 Strata alebo krádež notebooku

Popis: strata alebo krádež notebooku s citlivými údajmi.
Dôsledky: získanie dokumentov s citlivými údajmi, získanie prístupu k mailovej komunikácie, prípadne získanie vzdialeného prístupu do lokálnej počítačovej siete.
Preventívne opatrenia: šifrovanie diskov, zakázanie zapamätania si hesla do kľúčových aplikácii a mailovej schránky.

4.7 Nesprávne adresovanie mailu

Popis: odoslanie mailu s citlivými údajmi na nesprávnu mailovú adresu.
Dôsledky: získanie dokumentov s citlivými údajmi nepovolanou osobou.
Preventívne opatrenia: zákaz používania pracovných mailov na súkromné účely, šifrovanie dokumentov v mailoch.

4.8 Prístup k obsahu mailu pri jeho prenose

Popis: neoprávnený prístup (napr. administrátora mailového serveru) k mailom pri jeho prenose.
Dôsledky: získanie dokumentov s citlivými údajmi nepovolanou osobou.
Preventívne opatrenia: šifrovanie dokumentov v mailoch.

4.9 Napadnutie škodlivým softvérom

Popis: Zavírenie počítača alebo servera škodlivým softvérom — vírusy, malware, trójske kone a podobne.

Dôsledky: prístup k dokumentom na zariadení, ovládnutie zariadenia útočníkom, strata údajov.

Preventívne opatrenia: pravidelná aktualizácia antivírového programu a ochrana proti SPAMU. Kontrola prenosných USB zariadení. Kontrola prístupu zamestnancov na škodlivé webové stránky prostredníctvom PROXY servera.

4.10 Zneužitie zverejnených zraniteľností

Popis: Zverejnené bezpečnostné zraniteľnosti tvoria riziko pre každý systém.

Dôsledky: požadované služby nie sú dostupné, prístup k dokumentom na zariadení, ovládnutie zariadenia útočníkom.

Preventívne opatrenia: pravidelná aktualizácia operačných systémov firmvarov.

4.11 DoS alebo DDoS útoky na služby a infraštruktúru

Popis: útok, ktorého cieľom je akýmkoľvek spôsobom narušiť plynulý priebeh služby alebo infraštruktúru.

Dôsledky: požadované služby nie sú dostupné.

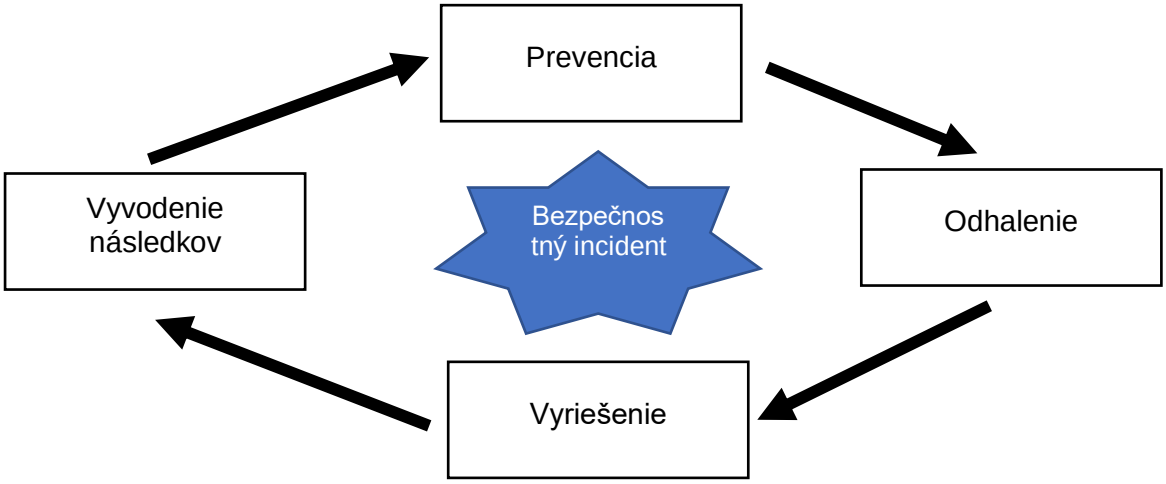
Preventívne opatrenia: správna konfigurácia zariadení pristupujúcich na Internet.

5 Riešenie kybernetických bezpečnostných incidentov

1) Zamestnanec PZS, ktorý zistí kybernetický bezpečnostný incident ho musí bezodkladne ohlásiť kontaktnej osobe.
2) Kontaktná osoba PZS pre nahlasovanie kybernetických bezpečnostných incidentov (ďalej len „kontaktná osoba"): Mária Oračková, Starostka.
    a. kontaktný mail: obec@obeclomnicka.sk
    b. telefonický kontakt: 0908 310 654
3) Hlásenie kybernetického bezpečnostného incidentu je možné urobiť osobne, mailom alebo telefonicky kontaktnej osobe, prípadne pomocou internej platformy na hlásenie incidentov.
4) Kontaktná osoba je povinná obratom potvrdiť prijatie mailu o nahlásenom kybernetickom bezpečnostnom incidente. Pokiaľ nahlasujúci nedostane do jednej hodiny odpoveď na mail, je povinný nahlásiť kybernetický bezpečnostný incident iným kanálom osobne alebo telefonicky, prípadne pomocou internej platformy na hlásenie incidentov.
5) Kontaktná osoba je povinná informovať o kybernetickom bezpečnostnom incidente bezpečnostného správcu (manažéra kybernetickej bezpečnosti), ktorým je: spoločnosť CUBS plus, s.r.o., Mudroňova 29, 040 01 Košice a všetkých správcov dotknutých aktív, ktorými sú vlastníci aktíva (v prípade, že sa ich kybernetický bezpečnostný incident týka).

6) Po zistení kybernetického bezpečnostného incidentu sa vykoná diagnostika a hľadá sa jeho riešenie. Vykonanie diagnostiky koordinuje bezpečnostný správca (manažér kybernetickej bezpečnosti) s príslušným správcom aktíva, ktorého sa incident týka.
7) Pokiaľ spôsobí kybernetický bezpečnostný incident havarijný stav, tak prevádzkovateľ postupuje podľa **Smernice pre riadenie bezpečnostnej politiky článok 15 „Havarijné plánovanie".**
8) Po prijatí opatrení na obnovu po kybernetickom bezpečnostnom incidente bezpečnostný správca zistí v súčinnosti s prevádzkovateľom veľkosť vzniknutých škôd a konzultuje spôsob ich nahradenia v súčinnosti s prevádzkovateľom.
9) O kybernetickom bezpečnostnom incidente urobí správca aktíva záznam do formulára, ktorý je prílohou číslo 1 tejto Smernice ako aj záznam do evidencie kybernetických bezpečnostných incidentov. Tento zápis sa predloží vedeniu PZS a manažérovi kybernetickej bezpečnosti.
10) Bezpečnostný správca spolu so správcom dotknutého aktíva určí podstatné nedostatky, ktoré by mohli zapríčiniť alebo prispievať k výskytu kybernetických bezpečnostných incidentov. Na základe zistení PZS prijme preventívne a nápravne opatrenia.

Proces kybernetického bezpečnostného incidentu:



Obecný úrad Lomnička
Lomnička 66
065 03 Podolínec

Príloha č. 1 ku Smernici pre nahlasovanie a riešenie kybernetických bezpečnostných incidentov

Por. č.	Dátum a čas zistenia	Zdroj incidentu (kto zistil incident)	Dátum a čas zmeny režimu	Dátum a čas začiatku	Dátum a čas skončenia
Opis kybernetického bezpečnostného incidentu (čo sa stalo):					
Opis vlastníka incidentu (vyjadrenie vlastníka aktíva):					
Zoznam dotknutých aktív:					
Porovnanie s rizikovou analýzou (ak bola urobená):					
Prijaté opatrenia:					
Opatrenia na zamedzenie opätovného kyber. bezpečnostného incidentu:					
Opatrenia a nariadenia, ktoré boli porušené :					

---------- ----------

Dátum a podpis správcu aktíva Dátum a podpis bezpečnostného správcu

---

Dátum a podpis štatutára

Zoznam osôb, ktoré boli oboznámené so Smernicou pre nahlasovanie a riešenie kybernetických bezpečnostných incidentov

p. č.	Meno a priezvisko	Dátum	Podpis