Prevádzkovateľ: Obec Čaňa

INTERNÝ POKYN

RIEŠENIE BEZPEČNOSTNÝCH INCIDENTOV

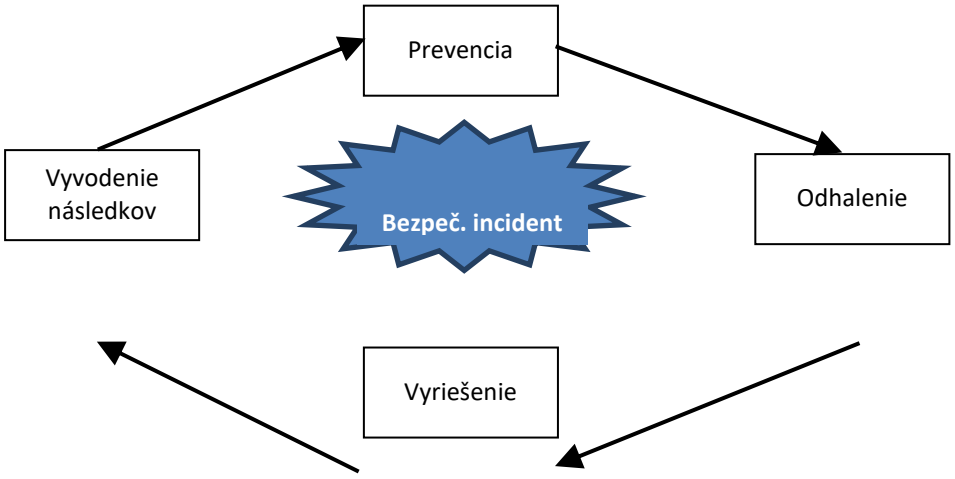
Schválil: Michal Rečka

Dátum: 25.5.2018

Riešenie bezpečnostných incidentov

1) Kontaktný mail pre nahlasovanie bezpečnostných incidentov (ďalej len kontaktný mail) obeccana@centrum.sk.
2) Kontaktná osoba pre nahlasovanie bezpečnostných incidentov (ďalej len kontaktná osoba) MVDr. Otília Tomčová, prednostka.
3) Zamestnanec, ktorý zistí bezpečnostný incident toto bezodkladne hlási kontaktnej osobe.
4) Hlásenie bezpečnostného incidentu je možné urobiť osobne, alebo telefonicky kontaktnej osobe alebo na kontaktný mail.
5) Kontaktná osoba je povinná obratom potvrdiť prijatie nahláseného incidentu. Pokiaľ nahlasujúci nedostane do jednej hodiny odpoveď na mail, je povinný nahlásiť incident iným kanálom, osobne alebo telefonicky.
6) Kontaktná osoba je povinná informovať o bezpečnostnom incidente bezpečnostného správcu a všetkých správcov dotknutých aktív.
7) O bezpečnostnom incidente sa vykoná diagnostika a hľadá sa jeho riešenie. Vykonanie diagnostiky koordinuje bezpečnostný správca s príslušným správcom aktíva, ktorého sa incident týka.
8) Pokiaľ spôsobí bezpečnostný incident havarijný stav, tak bezpečnostný správca postupuje podľa Smernici pre riadenie bezpečnostnej politiky článok 13 až 16.
9) Po prijatí opatrení na obnovu po incidente bezpečnostný správca zistí veľkosť vzniknutých škôd a riešiť spôsob ich nahradenia.
10) O bezpečnostnom incidente urobí bezpečnostný správca záznam do formulára, ktorý je prílohou číslo 1. Smernice pre riešenie bezpečnostných incidentov ako aj záznam do evidencie bezpečnostných incidentov. Tento zápis sa predloží vedeniu Prevádzkovateľa.
11) Bezpečnostný správca spolu so správcom dotknutého aktíva určí podstatné nedostatky, ktoré by mohli zapríčiniť alebo prispievať k výskytu incidentov. Na základe zistení sa príjmu preventívne a nápravné opatrenia.

Životný cyklus bezpečnostného incidentu



Možnosti bezpečnostných incidentov

Únik prihlasovacích údajov

Popis: získanie prihlasovacích údajov používateľa útokom z vonka alebo prezradením zamestnanca.
Dôsledky: získanie prístupu k údajom a ich možný únik.
Preventívne opatrenia: chrániť prístup do lokálnej počítačovej siete overeným firewallom.

Neúmyselné prezradenie prihlasovacích údajov

Popis: neúmyselné prezradenie prihlasovacích údajov kolegom alebo osobe mimo organizáciu. Zverejnenie osobných údajov ich zaznamenaním v papierovej podobe a umožnenie prístupu k ním.
Dôsledky: získanie prístupu k údajom a ich možný únik.
Preventívne opatrenia: poučenie zamestnancov o ochrane ich prihlasovacích údajov a zakázať ich zverejňovanie. Kontrolovať dodržiavanie týchto pravidiel.

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.

Strata údajov

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

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.

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 aplikácií a mailovej schránky.

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.

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.

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 webové stránky prostredníctvom PROXY servera.

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 firmvérov.

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.