Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

AGENTÚRA EURÓPSKEJ ÚNIE PRE KYBERNETICKÚ BEZPEČNOSŤ ENISA

12 KROKOV AKO OCHRÁNIŤ SVOJU FIRMU

KYBERNETICKÁ BEZPEČNOSŤ PRE MALÉ A STREDNÉ PODNIKY

Kríza spojená s pandémiou a vojnou na našich východných hraniciach ukazuje, aká dôležitá a zároveň zraniteľná je IT infraštruktúra vo všetkých malých a stredných podnikoch.

Leták predstavuje dvanásť praktických krokov pre zabezpečenie systémov a procesov malých a stredných podnikov (MSP). Je inšpirovaný letákom agentúry ENISA, ktorý vznikol ako poradenský materiál k správe Kybernetická bezpečnosť pre malé a stredné podniky: Výzvy a odporúčania.

1 *https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes*

1. BUDUJTE KULTÚRU KYBERNETICKEJ BEZPEČNOSTI

MANAŽÉRSKE ZODPOVEDNOSTI

Kybernetická bezpečnosť je kľúčovým prvkom pre úspešnú existenciu firmy bez ohľadu na veľkosť. Zodpovednosť za túto kritickú funkciu musí mať konkrétny zamestnanec alebo kontraktor a v jeho kompetencii je aj zabezpečenie primeraných zdrojov. Pod zdrojmi rozumieme zapojenie a školenia zamestnancov, nákup softvéru, služieb a hardvéru a vývoj efektívnych postupov v kyberbezpečnosti.

ZAMESTNANCI NA VAŠEJ STRANE

Vedenie spoločnosti by malo otvorene podporovať iniciatívy, ktoré presadzujú kybernetickú bezpečnosť vo všetkých firemných aktivitách. Súčasťou je aj komunikácia so zamestnancami na všetkých úrovniach, školenia v tejto oblasti podľa kvalifikácie a jasné a špecifické pravidlá bezpečnosti.

BEZPEČNOSTNÉ POLITIKY

Jasné a špecifické pravidlá bezpečnostnej politiky by mal byť popísané v politikách kyberbezpečnosti pre zamestnancov. Každý by mal vedieť, ako bezpečne používať IKT prostriedky, zariadenia a služby vo firme. Zároveň by mal byť každý zamestnanec oboznámený s dôsledkami, ak tieto zásady nedodrží. Pravidlá bezpečnostnej politiky je potrebné pravidelne kontrolovať a aktualizovať.

AUDIT KYBERNETICKEJ BEZPEČNOSTI

Pravidelné audity kyberbezpečnosti vykonávajú profesionáli s príslušnými znalosťami, zručnosťami a skúsenosťami. Audítor, či už interný, alebo externý by mal byť v nezávislej pozícii, najmä od prevádzky a vývoja IT.

OCHRANA ÚDAJOV

Ak malé a stredné podniky spracúvajú alebo uchovávajú osobné údaje obyvateľov Európskej únie respektíve Európskeho hospodárskeho spoločenstva, musia zabezpečiť, aby boli implementované dostatočné bezpečnostné opatrenia na ochranu týchto údajov. Túto povinnosť im ukladá Všeobecné nariadenie EÚ o ochrane údajov (GDPR). Zahŕňa to aj zodpovednosť tretích strán mať zavedené vhodné bezpečnostné opatrenia.

https://ec.europa.eu/info/law/law-topic/data-protection_sk

2. POSKYTNITE ŠKOLENIA

Pravidelné školenia o kybernetickej bezpečnosti pomáhajú zamestnancom rozoznať hrozby kybernetickej bezpečnosti a vysporiadať sa s nimi. Aby boli školenia užitočné a dôveryhodné, mali by byť prispôsobené potrebám každej firmy a zameriavať sa na situácie v reálnom živote. Zamestnanci zodpovední za riadenie kybernetickej bezpečnosti v podniku by rozhodne mali absolvovať aj špecializované školenia.

3. PAMÄTAJTE NA EFEKTÍVNE RIADENIE DODÁVATEĽOV

Kybernetická bezpečnosť je komplexná oblasť a preto je nevyhnutné, aby aj dodávatelia spĺňali dohodnuté požiadavky na bezpečnosť. Najmä tí, ktorí majú prístup k vašim citlivým údajom alebo kritickým systémom. Zmluvy a dohody by mali obsahovať konkrétne ustanovenia o spôsobe plnenia bezpečnostných požiadaviek.

4. VYPRACUJTE PLÁNY REAKCIE NA UDALOSTI

Formálny plán reakcie na incidenty, ktorý obsahuje jasné usmernenia, úlohy a zodpovednosti, by už dnes mal byť bežnou súčasťou firemných štandardov. Cieľom je zaistiť, že všetky bezpečnostné incidenty sa budú riešiť včas, profesionálne a vhodným spôsobom. V prípade bezpečnostných hrozieb je nevyhnutné reagovať rýchlo a preto využívajte nástroje na monitorovanie siete. Ak dôjde k podozrivej aktivite alebo narušeniu bezpečnosti, budú vás varovať automatické upozornenia.

5. ZABEZPEČTE PRÍSTUPY

Na vytvorenie prístupových hesiel do siete alebo do systémov používajte komplexné frázy. Aby to bola dobrá kombinácia na zapamätateľnosť a bezpečnosť, zložte si frázu aspoň z troch náhodných bežných slov.

Ak použijete prístupové frázy alebo heslá

- *Nepoužívajte ich na prístup do viacerých služieb*
- *Nezdieľajte ich s kolegami*
- *Používajte viacfaktorové overenie*
- *Použite aplikáciu na manažment hesiel*

Ak sa rozhodnete pre typické heslo, dodržujte nasledovné odporúčania

- *Vytvorte dlhé heslo, zložené z malých a veľkých písmen, prípadne aj z číslic a špeciálnych znakov.*
- *Vyhnite sa jednoduchým heslám, akými sú „heslo" či sekvencie písmen „abc", alebo číslic „123".*
- *Nepoužívajte osobné informácie, ktoré sa dajú vyhľadať online.*

6. UDRŽUJTE ZARIADENIA ZABEZPEČENÉ

Či už ide o servery, počítače, notebooky, tablety, smartfóny alebo iné komponenty, kľúčovým krokom kyberbezpečnosti je ich udržiavanie v súlade s bezpečnostnými pravidlami.

AKTUALIZOVANÝ SOFTVÉR

V ideálnom prípade používajte centralizovanú platformu na správu aktualizácií.

ANTIMALVÉROVÁ OCHRANA

Centrálne spravované antivírusové riešenie by malo byť implementované na všetkých typoch zariadení. Zároveň ho treba neustále aktualizovať, aby bolo nepretržito efektívne. Rozhodne si neinštalujte pirátsky softvér, pretože môže obsahovať malvér.

Dôrazne odporúčame

- *Pravidelne aktualizovať všetok softvér.*
- *Zapnúť automatické aktualizácie všade, kde je to možné.*
- *Identifikovať softvér a hardvér, ktorý vyžaduje manuálne aktualizácie.*
- *Nezabúdať na mobilné a IoT zariadenia.*

NÁSTROJE NA OCHRANU EMAILOV A WEBOVEJ STRÁNKY

Využite štandardné riešenia, ktoré blokujú nevyžiadanú poštu, odkazy obsahujúce prepojenie na škodlivé webové stránky, e-maily so škodlivými prílohami a phishingové e-maily.

ŠIFROVANIE

Podniky všetkých veľkostí by mali zabezpečiť, aby boli údaje v počítačoch aj smartfónoch šifrované. Ochránite tak dáta.

Pri prenose dát vo verejných sieťach je nutné zabezpečiť šifrovaný prenos použitím virtuálnej súkromnej siete (VPN) alebo prístupom na webové stránky cez zabezpečené pripojenia pomocou protokolu SSL/TLS.

Ak vaši zákazníci pristupujú cez internet, aj webové stránky musia používať vhodnú šifrovaciu technológiu na ochranu údajov.

7. CHRÁŇTE SVOJU SIEŤ

SPRÁVA MOBILNÝCH ZARIADENÍ

Pri využívaní práce na diaľku veľa firiem umožňuje zamestnancom používať vlastné notebooky, tablety alebo smartfóny. Takto však vznikajú bezpečnostné riziká pre citlivé obchodné údaje v týchto zariadeniach. Jedným zo spôsobov, ako spravovať toto riziko, je použiť riešenia na správu mobilných zariadení (MDM – Mobile Device Management).

MDM riešenie umožňuje

- Kontrolovať, ktoré zariadenia majú povolený prístup do systémov a služieb
- Verifikovať, či má zariadenie nainštalovaný a aktualizovaný antivírusový softvér.
- Uistiť sa, či je zariadenie šifrované.
- Overiť si, či má zariadenie nainštalované aktuálne softvérové záplaty
- Vyžadovať ochranu zariadenia pomocou PIN alebo hesla, či oboje súčasne
- Možnosť na diaľku vymazať údaje firmy, ak vlastník nahlásil stratu či krádež zariadenia, alebo sa skončil jeho pracovný pomer

FIREWALLY

Firewally sú kritickým nástrojom pri ochrane systémov malých a stredných podnikov. Kontrolujú prevádzku, ktorá vstupuje a vystupuje zo siete. Mali by byť implementované na ochranu všetkých kritických systémov a najmä chrániť firemnú sieť v prípade komunikácie cez internet.

VZDIALENÝ PRÍSTUP

Podniky by mali pravidelne overovať každý vzdialený prístup do podnikovej siete.

Preto pri riadení vzdialených prístupov uplatňujte tieto princípy

- *Uistite sa, že každý systém je aktualizovaný.*
- *Zakážte vzdialený prístup z podozrivých geografických miest alebo určitých IP adries.*
- *Vzdialený prístup pre používateľov obmedzte iba do tých systémov a počítačov, ktoré potrebujú k svojej práci.*
- *Vynucujte silné heslá pre vzdialený prístup a tam, kde je to možné, používajte viacfaktorové overenie.*
- *Implementujte monitorovanie a nastavte upozornenia v prípade podozrenia útoku alebo nezvyčajných aktivít.*

8. ZLEPŠITE FYZICKÚ BEZPEČNOSŤ

Primerané opatrenia fyzickej bezpečnosti by mali byť implementované všade, kde sa nachádzajú citlivé informácie. Kedykoľvek keď používateľ odíde od svojho počítača, mal by uzamknúť pracovnú plochu. Ani firemný notebook či smartfón nesmú byť voľne pohodené na zadnom sedadle auta.

Na všetky IKT zariadenia aplikujte automatické uzamknutie po nečinnosti. Citlivé tlačené dokumenty by ste nemali nechávať voľne pohodené a keď ich nepoužívate, bezpečne ich uložte.

9. ZÁLOHUJTE ÚDAJE

Zálohujte údaje, pretože to predstavuje efektívny spôsob obnovy po haváriách alebo kyberútokoch.

Pamätajte na kľúčové pravidlá zálohovania

- *pravidelne a automatizovane zálohujte vždy, keď je to možné*
- *zálohovanie prebieha oddelene od produkčného prostredia*
- *zálohy šifrujte, najmä ak sa presúvajú na iné miesto*
- *pravidelne testujte schopnosť obnovovať dáta zo záloh. V ideálnom prípade by sa mal vykonávať pravidelný test úplného obnovenia.*

10. VYUŽITE CLOUDOVÉ RIEŠENIA

Hoci cloudové riešenia ponúkajú množstvo výhod, existujú aj riziká, ktoré by mali malé a stredné podniky zvážiť. Agentúra ENISA vydala publikáciu *Sprievodca zabezpečením cloudu pre malé a stredné podniky,* ktorá vám pomôže pri migrácii.

Pri výbere poskytovateľa by sa mal každý podnik uistiť, či uchovávaním údajov, najmä osobných, neporušuje zákony a nariadenia, najmä pri ich umiesťovaní mimo Európskej únie respektíve Európskeho hospodárskeho spoločenstva (EÚ/EHP). Napríklad GDPR vyžaduje, aby sa osobné údaje obyvateľov EÚ/EHP neukladali ani neprenášali mimo EÚ/EHP, pokiaľ nie sú splnené veľmi špecifické podmienky.

11. NEZABÚDAJTE NA SVOJU WEBOVÚ STRÁNKU

Pre každý podnik je existenčne dôležité, aby jeho webové stránky boli konfigurované a udržiavané bezpečne. Akékoľvek osobné alebo finančné údaje, napríklad údaje o platobných kartách, musia byť primerane chránené. Aby sa identifikovali akékoľvek zraniteľnosti, na webových stránkach treba nevyhnutne robiť opakovane bezpečnostné testy. Pravidelné kontroly sa zas starajú o správnu údržbu a aktualizáciu všetkých komponentov.

12. VYHĽADÁVAJTE INFORMÁCIE

Účinným nástrojom v boji proti počítačovej kriminalite je zdieľanie informácií medzi manažmentom, bezpečnostnými profesionálmi aj zamestnancami. Dôležité je vedieť, ako sa iné firmy postavili ohrozeniam, alebo riešili reálny incident. Často je to spôsob, kedy pochopia zmysel bezpečnostných opatrení.

Malé a stredné podniky chcú vedieť, čo sa deje v ich segmente a tak zdieľanie skúsenosti prispieva k akceptácii konkrétnych krokov na zabezpečenie systémov. Ak budete vedieť viac, lepšie pochopíte riziká, ktorým čelíte.

Spolufinancovaný Európskou úniou

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

www.cybercompetence.sk