enisa

AGENTÚRA EURÓPSKEJ ÚNIE
PRE KYBERNETICKÚ
BEZPEČNOSŤ

Príručka pre kybernetickú bezpečnosť pre MSP

12 KROKOV NA ZABEZPEČENIE VÁŠHO PODNIKANIA

Kríza spôsobená pandémiou COVID-19 poukázala na to, aký dôležitý je pre MSP internet a počítače vo všeobecnosti. Na to, aby sa počas pandémie darilo v podnikaní, mnohé MSP museli prijať opatrenia na zabezpečenie kontinuity činností, ako napríklad prechod na cloudové služby, zlepšenie svojich internetových služieb, inováciu svojich webových sídiel a umožnenie zamestnancom pracovať na diaľku.

Tento leták poskytuje malým a stredným podnikom 12 praktických krokov na vysokej úrovni, ako lepšie zabezpečiť svoje systémy a podnikanie. Ide o sprievodnú publikáciu k podrobnejšej správe ENISA ***Cybersecurity for SMES – Challenges and Recommendations*** (Kybernetická bezpečnosť pre MSP – Výzvy a odporúčania).

1 VYTVORTE KULTÚRU KYBERNETICKEJ BEZPEČNOSTI

PRIDEĽTE ZODPOVEDNOSŤ ZA RIADENIE

Dobrá kybernetická bezpečnosť je kľúčovým prvkom trvalého úspechu každého MSP. Zodpovednosť za túto kritickú funkciu by mala byť zverená určitej osobe v rámci organizácie, ktorá by mala zabezpečiť, že sa na kybernetickú bezpečnosť vyčlenia primerané zdroje, ako je čas zamestnancov, nákup softvéru, služieb a hardvéru na kybernetickú bezpečnosť, odborná príprava pre zamestnancov a vypracovanie účinných zásad.

ZÍSKAJTE AKTÍVNE ZAPOJENIE ZAMESTNANCOV

Získajte aktívne zapojenie zamestnancov prostredníctvom účinnej komunikácie o kybernetickej bezpečnosti zo strany manažmentu, jeho otvorenou podporou iniciatív v oblasti kybernetickej bezpečnosti, primeranou odbornou prípravou poskytovanou zamestnancom a poskytovaním jasných a konkrétnych pravidiel stanovených v zásadách kybernetickej bezpečnosti pre zamestnancov.

ZVEREJŇUJTE ZÁSADY KYBERNETICKEJ BEZPEČNOSTI

V zásadách kybernetickej bezpečnosti pre zamestnancov by sa mali stanoviť jasné a konkrétne pravidlá týkajúce sa toho, čo sa od nich očakáva, pokiaľ ide o ich správanie pri využívaní prostredia, vybavenia a služieb IKT spoločnosti. V týchto zásadách by sa mali zdôrazniť aj na následky, ktorým by zamestnanec mohol čeliť, ak by tieto zásady nedodržiaval. Tieto zásady je potrebné pravidelne revidovať a aktualizovať.

VYKONÁVAJTE AUDITY KYBERNETICKEJ BEZPEČNOSTI

Pravidelné audity by mali vykonávať osoby s príslušnými znalosťami, zručnosťami a skúsenosťami. Audítori by mali byť nezávislí, či už ide o externého, alebo interného dodávateľa MSP, a mali by pracovať nezávisle od každodenných operácií IT.

PAMÄTAJTE NA OCHRANU ÚDAJOV

Podľa všeobecného nariadenia EÚ o ochrane údajov[1] musia všetky MSP, ktoré spracúvajú alebo uchovávajú osobné údaje obyvateľov EÚ/EHP, zabezpečiť, aby boli zavedené vhodné bezpečnostné kontroly na ochranu týchto údajov. To zahŕňa zabezpečenie toho, aby všetky tretie strany pracujúce v mene MSP mali zavedené primerané bezpečnostné opatrenia.

1 Všeobecné nariadenie o ochrane údajov https://ec.europa.eu/info/law/law-topic/data-protection_sk.

2

POSKYTNITE PRIMERANÚ ODBORNÚ PRÍPRAVU

Zabezpečte pravidelnú odbornú prípravu zameranú na zvyšovanie informovanosti o kybernetickej bezpečnosti pre všetkých zamestnancov, aby ste sa uistili, že sú schopní rozpoznať rôzne kybernetické hrozby a vyrovnať sa s nimi. Táto odborná príprava by mala byť prispôsobená MSP a mala by sa zameriavať na situácie z reálneho života.

Poskytnite špecializovanú odbornú prípravu v oblasti kybernetickej bezpečnosti pre tých, ktorí sú zodpovední za správu kybernetickej bezpečnosti v rámci podniku, s cieľom zabezpečiť, aby mali zručnosti a kompetencie potrebné na výkon svojej práce.

3

ZABEZPEČTE ÚČINNÉ RIADENIE TRETÍCH STRÁN

Zabezpečte, aby všetci dodávatelia, najmä tí, ktorí majú prístup k citlivým údajom a/alebo systémom, boli aktívne riadení a spĺňali dohodnuté úrovne bezpečnosti. Mali by existovať zmluvné dohody, v ktorých sa upravuje, ako môžu dodávatelia splniť tieto bezpečnostné požiadavky.

4

VYPRACUJTE PLÁN REAKCIE NA INCIDENTY

Vypracujte formálny plán reakcie na incidenty, ktorý obsahuje jasné usmernenia, zdokumentované úlohy a zodpovednosti, aby sa zabezpečilo, že na všetky bezpečnostné incidenty sa bude reagovať včas, profesionálne a primeraným spôsobom. reskúmajte nástroje, ktorými by sa mohli monitorovať a vytvárať upozornenia, keď dôjde k podozrivej aktivite alebo narušeniu bezpečnosti, aby sa zabezpečila rýchla reakcia na bezpečnostné hrozby.

5 ZABEZPEČTE PRÍSTUP K SYSTÉMOM

Vyzvite každého, aby používal prístupovú frázu, kombináciu najmenej troch náhodných bežných slov spojených do frázy, ktorá je veľmi ľahko zapamätateľná a bezpečná. Ak sa rozhodnete pre klasické heslo:

- vytvorte dlhé heslo obsahujúce malé a veľké písmená, prípadne aj čísla a špeciálne znaky,
- vyhnite sa slabým heslám, ako je napríklad „heslo“, postupnostiam písmen ako „abc“ alebo postupnostiam čísiel ako „123“,
- vyhnite sa používaniu osobných údajov, ktoré možno nájsť online.

Či už používate prístupové frázy, alebo heslá

- nepoužívajte ich nikde inde,
- neprezrádzajte ich kolegom,
- umožnite dvojstupňovú autentifikáciu,
- použite špecializovaného správcu hesiel.

6

ZABEZPEČTE ZARIADENIA

Zabezpečenie zariadení, ktoré zamestnanci používajú, či už ide o ich stolové počítače, notebooky, tablety, alebo smartfóny, je kľúčovým krokom v programe kybernetickej bezpečnosti.

ZABEZPEČTE OPRAVY A AKTUALIZÁCIE SOFTVÉRU

Najlepšie pomocou centralizovanej platformy na správu opráv. Malým a stredným podnikom sa dôrazne odporúča, aby:

- pravidelne aktualizovali všetok softvér,
- zapli automatické aktualizácie vždy, keď je to možné,
- identifikovali softvér a hardvér, ktorý si vyžaduje manuálne aktualizácie,
- brali do úvahy mobilné zariadenia a zariadenia internetu vecí.

ANTIVÍRUS

Centrálne spravované antivírusové riešenie by sa malo zaviesť na všetkých typoch zariadení a malo by sa neprestajne aktualizovať, aby sa zabezpečila jeho nepretržitá účinnosť. Neinštalujte softvér porušujúci autorské práva, pretože môže obsahovať malvér.

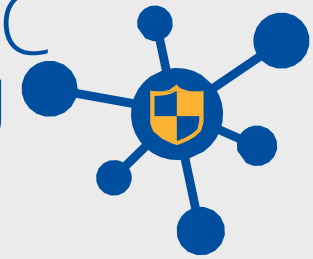
ZAVEĎTE NÁSTROJE NA OCHRANU E-MAILU A WEBU

Využívajte riešenia na blokovanie nevyžiadanej elektronickej pošty, e-mailov obsahujúcich odkazy na škodlivé webové sídla, e-mailov obsahujúcich škodlivé prílohy, ako sú vírusy, a e-mailov so zámerom neoprávneného získania údajov.

ŠIFROVANIE

Chráňte údaje ich šifrovaním. MSP by mali zabezpečiť, aby údaje uložené v mobilných zariadeniach, ako sú notebooky, smartfóny a tablety, boli šifrované. V prípade údajov prenášaných cez verejné siete, ako sú bezdrôtové siete v hoteloch alebo na letiskách, zabezpečte, aby boli údaje šifrované, a to buď použitím virtuálnej súkromnej siete (VPN) alebo prístupom na webové sídla cez zabezpečené pripojenie prostredníctvom protokolu SSL/TLS. Zabezpečte, aby ich vlastné webové sídla využívali vhodnú technológiu šifrovania na ochranu údajov klientov pri ich prenose cez internet.

7 ZABEZPEČTE SVOJU SIEŤ



ZAVEĎTE SPRÁVU MOBILNÝCH ZARIADENÍ

Pri uľahčovaní práce zamestnancov na diaľku mnohé MSP umožňujú zamestnancom používať ich vlastné notebooky, tablety a/alebo smartfóny. S tým súvisí viacero problémov so zabezpečením citlivých obchodných údajov uložených na týchto zariadeniach. Jedným zo spôsobov, ako zvládnuť toto riziko, je použiť riešenie Správa mobilných zariadení (MDM), ktoré umožňuje MSP:

- mať pod kontrolou, ktoré zariadenia majú povolený prístup k ich systémom a službám,
- uistiť sa, že v zariadení je nainštalovaný aktuálny antivírusový softvér,
- zistiť, či je zariadenie šifrované,
- potvrdiť, či má zariadenie nainštalované aktuálne softvérovéopravy,
- dbať na to, aby bolo zariadenie chránené kódom PIN a/alebo heslom,
- na diaľku vymazať všetky údaje MSP zo zariadenia, ak vlastník zariadenia nahlási ich stratu alebo krádež, alebo ak by sa mal skončiť pracovný pomer vlastníka zariadenia v MSP.

POUŽÍVAJTE FIREWALL

Firewall riadi prenos údajov, ktoré vstupujú do siete a opúšťajú ju, a je rozhodujúcim nástrojom pri ochrane systémov MSP. Firewall by mal byť nasadený na ochranu všetkých dôležitých systémov a mal by sa použiť najmä na ochranu siete MSP pred internetom.

KONTROLUJTE MOŽNOSTI VZDIALENÉHO PRÍSTUPU

MSP by mali pravidelne kontrolovať všetky nástroje na vzdialený prístup, aby zaistili ich bezpečnosť, a najmä by mali:

- zabezpečiť, že sú nainštalované opravy a aktualizácie všetkého softvéru na vzdialený prístup,
- obmedziť vzdialený prístup z podozrivých zemepisných polôh alebo určitých IP adries,
- obmedziť vzdialený prístup zamestnancov len na systémy a počítače, ktoré potrebujú na svoju prácu,
- dbať na silné heslá pre vzdialený prístup, a ak je to možné, umožniť dvojstupňovú autentifikáciu,
- zabezpečiť, aby bolo povolené monitorovanie a upozornenia, aby vás upozornili na podozrivé útoky alebo nezvyčajnú podozrivú aktivitu.

8 ZLEPŠITE FYZICKÚ BEZPEČNOSŤ

Všade tam, kde sa nachádzajú dôležité informácie, by sa mali zaviesť primerané fyzické kontroly. Podnikový notebook alebo smartfón by ste napríklad nemali nechať bez dozoru na zadnom sedadle auta. Kedykoľvek používateľ odíde od svojho počítača, mal by ho uzamknúť. V opačnom prípade povoľte funkciu automatického uzamknutia na akomkoľvek zariadení používanom na obchodné účely. Citlivé tlačené dokumenty by ste takisto nemali nechávať bez dozoru, a keď sa nepoužívajú, odložte ich na bezpečnom mieste.

9 ZABEZPEČTE ZÁLOHOVANIE

Aby bolo možné obnoviť kľúčové informácie, mali by sa udržiavať zálohy, pretože predstavujú účinný spôsob obnovy po závažných zlyhaniach, ako je útok ransomvérom. Mali by sa uplatňovať tieto pravidlá zálohovania:

- pokiaľ je to možné, zálohovanie sa vykonáva pravidelne a automatizovane,
- záloha sa uchováva oddelene od produkčného prostredia MSP,
- zálohy sú šifrované, najmä ak sa budú presúvať medzi rôznymi miestami,
- testuje sa schopnosť pravidelne obnovovať údaje zo záloh. V ideálnom prípade by sa mal vykonávať pravidelný test úplnej obnovy od začiatku do konca.

10 VYUŽÍVAJTE SLUŽBY CLOUDU

Hoci cloudové riešenia ponúkajú množstvo výhod, predstavujú určité jedinečné riziká, ktoré by MSP mali zvážiť pred tým, než sa spoja s poskytovateľom cloudu. Agentúra ENISA vydala príručku zabezpečenia cloudu pre MSP *Cloud Security Guide for SMEs*[2], ktorú by MSP mali používať pri migrácii do cloudu.

Pri výbere poskytovateľa cloudu by mal MSP zabezpečiť, aby neporušil žiadne zákony alebo nariadenia ukladaním údajov, najmä osobných údajov, mimo EÚ/EHP. Napríklad vo všeobecnom nariadení EÚ o ochrane údajov sa vyžaduje, aby sa osobné údaje obyvateľov v rámci EÚ/EHP neukladali ani neprenášali mimo EÚ/EHP, pokiaľ to nie je za veľmi osobitných podmienok.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

11 ZABEZPEČTE WEBOVÉ SÍDLA

Je nevyhnutné, aby MSP zabezpečili, že ich webové sídla sú nakonfigurované a udržiavané bezpečným spôsobom a že všetky osobné údaje alebo finančné údaje, ako sú údaje o kreditných kartách, sú primerane chránené. Bude si to vyžadovať vykonávanie pravidelných bezpečnostných testov na webových sídlach s cieľom identifikovať prípadné slabé stránky zabezpečenia a vykonávať pravidelné kontroly, aby sa zabezpečila správna údržba a aktualizácia webových sídel.

12 VYHĽADÁVAJTE A ZDIEĽAJTE INFORMÁCIE

Účinným nástrojom v boji proti počítačovej kriminalite je zdieľanie informácií. Zdieľanie informácií v súvislosti s počítačovou kriminalitou je kľúčom k tomu, aby MSP lepšie pochopili riziká, ktorým čelia. Podniky, ktoré sa od iných spoločností dozvedia o výzvach v oblasti kybernetickej bezpečnosti a o tom, ako tieto výzvy prekonali, s väčšou pravdepodobnosťou podniknú kroky na zabezpečenie svojich systémov, ako keby sa podobné informácie dozvedeli zo správ odvetvia alebo z prieskumov kybernetickej bezpečnosti.

AGENTÚRA EURÓPSKEJ ÚNIE
PRE KYBERNETICKÚ
BEZPEČNOSŤ

O AGENTÚRE ENISA
Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúra Únie, ktorej úlohou je zabezpečovať vysokú spoločnú úroveň kybernetickej bezpečnosti v Európe. Agentúra EÚ, ktorá bola zriadená v roku 2004 a ktorej postavenie posilnil akt EÚ o kybernetickej bezpečnosti, prispieva k vytváraniu kybernetickej politiky EÚ a pomocou systémov certifikácie kybernetickej bezpečnosti zvyšuje dôveryhodnosť produktov, služieb a procesov IKT, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy v budúcnosti. Agentúra prostredníctvom spoločného využívania vedomostí, budovania kapacít a zvyšovania informovanosti spolupracuje s kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v prepojenú ekonomiku, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zachovať digitálnu bezpečnosť európskej spoločnosti a občanov Európy. Viac informácií nájdete na stránke www.enisa.europa.eu.

ENISA
Agentúra Európskej únie pre kybernetickú bezpečnosť

Kancelária v Aténach
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Grécko

Kancelária v Irakliu
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Iraklio, Grécko

enisa.europa.eu