Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ZÁKLADNÉ BEZPEČNOSTNÉ OPATRENIA PRE VRCHOLOVÝ MANAŽMENT

Tento dokument je určený vrcholovému manažmentu a štatutárnym predstaviteľom organizácií, teda osobám, ktoré majú významné rozhodovacie právomoci a najväčší vplyv na smerovanie danej organizácie. Dôležitosť týchto osôb ich však zároveň stavia do pozície, kedy sú lákavým cieľom pre útočníkov snažiacich sa narušiť kybernetickú bezpečnosť organizácie. V zmysle Obchodného zákonníka je štatutárny orgán spoločnosti povinný konať s odbornou starostlivosťou, v súlade so záujmami spoločnosti, pričom zodpovedá za porušenie týchto povinností.

Členom vrcholového manažmentu a štatutárnym predstaviteľom sa preto odporúča dodržiavať nižšie uvedené opatrenia týkajúce sa zníženia rizika ohrozenia činnosti organizácie a plnenia povinnosti konať v súlade s jej záujmami. Zároveň je potrebné mať na pamäti, že správanie vrcholového manažmentu sa vždy odráža aj v správaní zamestnancov. Pokiaľ nerešpektuje pravidlá vrcholový manažment, môže byť zložité vyžadovať plnenie pravidiel od ostatných zamestnancov.

Dokument má odporúčací charakter a nenahrádza žiadne právne predpisy, konkrétne ani právnu úpravu vyplývajúcu zo zákona o kybernetickej bezpečnosti. Odporúčania vyplývajúce z tohto dokumentu zároveň nemôžu obsiahnuť všetky aplikovateľné bezpečnostné opatrenia, preto ďalšie opatrenia vhodné pre danú organizáciu, musia byť odborníkmi navrhnuté a prispôsobené na mieste.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Vydané v spolupráci s: Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

www.cybercompetence.sk

ZÁKLADNÉ BEZPEČNOSTNÉ PRAVIDLO

Rešpektujte bezpečnostné pokyny

Každá organizácia by sa mala snažiť zaručiť bezpečné prostredie a bezpečné narábanie s informačnými aktívami. Za týmto účelom organizácia zvyčajne zamestnáva odborníkov, ktorí sú zodpovední za informačnú a kybernetickú bezpečnosť. Je potrebné riadiť sa ich odporúčaniami a návrhmi a dodržiavať ich, v opačnom prípade bezpečnosť nikdy nemôže byť udržateľná na úrovni požadovanej bezpečnostnou stratégiou organizácie. Neváhajte sa na nich obrátiť v prípade potreby upresnenia týchto základných bezpečnostných pravidiel a opatrení.

PRÁCA S FIREMNÝM POČÍTAČOM A SMARTFÓNOM

Nepoužívajte súkromné zariadenia na pracovné účely

Súkromné zariadenia nie sú spravované a udržiavané organizáciou. S používaním súkromných zariadení je obyčajne spätá nižšia miera dohľadu, a bežne aj zdieľanie s členmi rodiny. V súkromných zariadeniach sú bežne tiež nainštalované aplikácie, ktoré nie sú potrebné na pracovné účely. To všetko prináša zvýšené riziko pre bezpečnosť používateľa, ale aj celej organizácie. Pokiaľ je v organizácii používanie súkromných zariadení aj napriek tomu povolené, obráťte sa na bezpečnostných odborníkov vo Vašej organizácií a riaďte sa ich pokynmi.

Obmedzte prístup k zariadeniam a uzamykajte ich obrazovky počas vašej neprítomnosti

Zariadenie, ktoré nie je pod vašou fyzickou kontrolou, dáva priestor útočníkovi. Odomknuté zariadenie bez dozoru umožňuje komukoľvek manipulovať so zariadením a s jeho obsahom. Je to potrebné uvedomiť si nielen v kancelárii, ale predovšetkým na verejných miestach (napr. na konferencii, vo vlaku a pod.).

- *Pri počítačoch s operačným systémom Windows je najjednoduchší spôsob rýchleho uzamknutia klávesová skratka WIN+L*
- *Pri počítačoch s operačným systémom MacOS je najjednoduchší spôsob rýchleho zamknutia klávesnicová skratka COMMAND+CONTROL+Q*
- *Na mobilnom zariadení stlačenie tlačidla uzamknutia*

Nepripájajte neznáme externé disky a iné pamäťové médiá

Neznáme pamäťové médiá môžu obsahovať škodlivý kód, ktorý sa zvyčajne ihneď po pripojení automaticky nahrá do zariadenia. V prípade, že je nevyhnutné pripojiť neznáme médium, vykonajte aspoň základnú antivírovú kontrolu jeho obsahu.

Používajte heslá, kódy alebo iné spôsoby zabezpečenia v súlade s bezpečnostnou politikou organizácie

V prípade straty alebo odcudzenia je zariadenie výrazne lepšie chránené.

Zvoľte si dlhé, zapamätateľné frázy pre heslá, prípadne používajte správcu hesiel

Aplikácia „správca hesiel" (Password Manager) umožňuje jednoduchú a bezpečnú správu všetkých potrebných prihlasovacích údajov a hesiel na jednom mieste.

Pri zadávaní prihlasovacích údajov a hesiel sa ubezpečte, že ich nikto cudzí nevidí, napríklad pohľadom cez rameno

Predovšetkým počas prítomnosti na verejných miestach, kde je väčší pohyb ľudí, vyšší počet kamier alebo fotoaparátov (napr. na konferencii, vo vlaku a pod.), je zvýšené riziko, že útočník jednoducho odčíta a následne použije Vaše údaje. V prípade mobilných telefónov odomykajte zariadenie pomocou odtlačku prsta alebo scanu tváre.

Pravidelne aktualizujte zariadenie a nevypínajte automatické aktualizácie systémov a aplikácií

Aktualizácia zariadení je spôsob, ktorým výrobca zariadenia opravuje nové identifikované zraniteľnosti, ktoré by mohli toto zariadenie ohroziť. Pokiaľ systém vyžaduje vykonanie aktualizácie, je potrebné jej nebrániť a neodsúvať ju. Termín automatických pravidelných aktualizácií je obvykle možné nastaviť priamo v zariadení. Rovnako ako je to v prípade aktualizácie systémov, je potrebné aktualizovať aj aplikácie. Program, ktorý doteraz fungoval bez problémov, môže byť bez aktualizácie takmer nepoužiteľný alebo až nebezpečný.

Využívajte možnosti šifrovania údajov na interných a externých médiách

Šifrovanie zabezpečí dáta predovšetkým pri strate alebo odcudzení zariadenia. Dáta na pracovnom počítači by mali byť zásadne chránené kryptografickými opatreniami. Je však potrebné myslieť aj na ostatné zariadenia, na ktorých sa dáta nachádzajú, vrátane pamäťových médií.

Pravidelne zálohujte dáta

Riziko straty údajov existuje vždy. Môže ísť o poruchu zariadenia, jeho stratu, odcudzenie alebo o cielený útok škodlivým kódom, ktorý dáta na disku nenávratne zašifruje. Je preto vhodné myslieť na zálohu dôležitých dát a túto zálohu uchovávať na inom mieste ako v samotnom zariadení. Pripájať záložné médium k zariadeniu je potrebné iba počas zálohovania. Nezálohujte pracovné dáta na iné, ako na organizáciou určené zariadenia.

Vyhýbajte sa používaniu verejných wi-fi sietí

Verejne poskytované wi-fi služby sú jednoduchým spôsobom, ako môže útočník preniknúť do zariadenia a mať prehľad o všetkých vašich činnostiach, predovšetkým o použití prihlasovacích údajov a hesiel. Problémom sú najmä verejné a nezabezpečené wi-fi (napr. bez hesla alebo s verejne dostupným heslom – napr. reštaurácie, konferencie, a pod.). Pokiaľ to nie je nutné, je vhodné sa k nim vôbec nepripájať. Riziko je možné znížiť použitím zabezpečeného spojenia (tzv. VPN), najvhodnejšie je potom používať VPN v kombinácii s mobilným internetom.

Venujte zvýšenú pozornosť bezdrôtovým technológiám, ako je Wi-Fi, Bluetooth, NFC a ďalšie

Bezdrôtové technológie je vhodné v zariadení zapínať iba vtedy, pokiaľ sú využívané - predstavujú potencionálnu cestu, ako môže útočník preniknúť do zariadenia.

Kontrolujte, či webové stránky podporujú protokol HTTPS

V prípade internetových stránok, ktoré vyžadujú prihlásenie (najmä internetové bankovníctvo, e-mail a podobne), je potrebné sa ubezpečiť že webstránka je zabezpečená HTTPS protokolom. Pokiaľ to tak nie je, údaje nie sú dostatočne chránené a sú veľmi ľahko zneužiteľné.

- *Zobrazenie HTTPS protokolu v internetovom prehliadači*

  https://www...

- *Zobrazenie v internetovom prehliadači bez protokolu HTTPS (cez tieto stránky nezadávať heslá)*

  www...

Na internetové odkazy klikajte obozretne

Ak je to možné, skontrolujte, či odkaz nevedie na podozrivú URL adresu. Skutočná URL adresa sa po umiestnení kurzora na odkaz bez rozkliknutia zobrazí vedľa kurzora, prípadne v okienku v ľavom dolnom rohu stránky. Pokiaľ nie je možné zistiť kam odkaz smeruje, neotvárajte ho.

BEZPEČNÁ KOMUNIKÁCIA

Overujte identitu protistrany pri komunikácii

Je potrebné myslieť na to, že osoba s ktorou komunikujete sa môže vydávať za niekoho iného. Overovať identitu protistrany je vhodné najmä pri prvotnej komunikácii. Pokiaľ existuje podozrenie, že osoba nie je tá, za ktorú sa vydáva, je možné hovor ukončiť a zavolať späť na dané telefónne číslo z oficiálneho zoznamu.

Nezverejňujte osobné a ani iné citlivé informácie

Je potrebné zvážiť, či je skutočne potrebné zverejňovať niektoré údaje. Dátum narodenia, náboženské presvedčenie alebo napríklad aj súkromné fotografie môžu byť následne zneužité, a to či už voči konkrétnym osobám alebo voči organizácii, ktorú tieto osoby zastupujú.

K informáciám na internete pristupujte kriticky, nemusia byť pravdivé

Je potrebné vždy overovať, či sú informácie skutočne pravdivé a či sú uvedené v príslušnom kontexte. Kritické myslenie a obozretnosť sú v čase falošných správ, hybridných hrozieb a cielených útokov sú základom bezpečnej komunikácie na internete.

Venujte zvýšenú pozornosť obsahu v správach elektronickej pošty a v prípade podozrivého e-mailu alebo prílohy informujte zodpovedných zamestnancov

Prostredníctvom príloh v e-mailovej správe sa môže ľahko šíriť škodlivý kód, ktorý sa po otvorení prílohy aktivuje. Z tohto dôvodu je vhodné otvárať len tie e-maily a ich prílohy, ktoré sú dôveryhodné a o podozrivých správach informovať IT oddelenie, alebo manažéra kybernetickej bezpečnosti.

Čo je to phishing?

Phishing je podvodná technika, prostredníctvom ktorej sa útočníci snažia napríklad získať osobné údaje, alebo rôzne iné citlivé informácie (prihlasovacie údaje, dátum narodenia, číslo platobnej karty atď.), nasmerovať používateľa na podvodnú stránku alebo zaslať škodlivú prílohu. Phishing sa najčastejšie šíri formou e-mailových správ, ktoré vyzerajú ako keby boli odoslané z dôveryhodnej inštitúcie. Neváhajte sa obrátiť na bezpečnostných odborníkov s otázkami, ako rozpoznať phishing. Prípadne využite odporúčania publikované na odborných portáloch.

Zbytočne nezdieľajte viac informácií, než si vyžaduje daná situácia

Všetko, čo je obsahom komunikácie, môže byť v budúcnosti zneužité.

Majte na pamäti, že nič nie je zadarmo

Ponuky na on-line služby zadarmo, ktoré sú za bežných okolností platené, je potrebné dôkladne zvážiť.

Ak vediete komunikáciu v časovej tiesni, je oveľa dôležitejšie premýšľať nad obsahom a minimalizovať objem zdieľaných informácií

Útočníci používajú manipulatívne techniky a jednou z nich je vyvolanie pocitu časovej tiesne. Tlačia na používateľa, že bezodkladne, alebo čo najskôr je potrebné niečo vykonať, niečo opraviť, niečo zdieľať. Je potrebné si vždy uvedomiť, že škoda spôsobená omeškaním býva menšia, ako dôsledky neuvážených činov.

ZABEZPEČENIE ON-LINE ÚČTOV

Nepoužívajte súkromné účty na pracovné účely

Súkromné účty (e-mailové schránky, cloudové služby a podobne) používateľa nie sú pod dohľadom organizácie a sú tak pre organizáciu zvýšeným rizikom napr. z dôvodu hrozby infikovania škodlivým kódom. Platí to však aj naopak - pracovné účty nie je vhodné používať na súkromné účely.

Chráňte prístupy k pracovným účtom a pre každú službu používajte iné unikátne heslo

V prípade používania slabého hesla je jeho prelomenie útočníkom otázkou času. Pokiaľ dôjde k prezradeniu hesla k jednému účtu, má útočník možnosť vyskúšať použitie rovnakého hesla aj do množstva ďalších Vašich účtov.

Nezdieľajte s inými ľuďmi prihlasovacie údaje k účtom a službám

V prípade kompromitácie vašich prístupových práv k pracovným zdrojom môže mať takéto konanie závažné následky pre organizáciu.

V prípade, že je to možné, využívajte viacfaktorovú autentifikáciu, a to predovšetkým pri kritických službách

Bežným spôsobom realizácie viacfaktorovej autentifikácie je obdržanie kontrolnej SMS po zadaní prístupových údajov. V organizácii však môžu existovať aj iné spôsoby viacfaktorovej autentifikácie užívateľov.

Pre bežnú činnosť používajte účet bežného používateľa - administrátorský účet je určený pre tých, ktorí vykonávajú správu systémov a zariadení v organizácii

Administrátorský účet s vyššími oprávneniami je určený výhradne pre správu systému, typicky prostredníctvom IT oddelení. Útočník, ktorý má k dispozícii administrátorské práva, spôsobí väčšiu škodu s menšou námahou.

Nepoužívajte kontrolné otázky pre obnovenie hesla

Na obnovenie hesla nie je vhodnou alternatívou používať kontrolné otázky typu „najmenšia planéta slnečnej sústavy", či „rodné meno manželky". Podobné informácie môžu byť dohľadateľné z verejných zdrojov. Pokiaľ sa takáto kontrolná otázka vyžaduje, je potrebné k nej pristúpiť pri zadávaní hesla a voliť ju tak, aby ju nebolo možné uhádnuť.

Vydané v spolupráci s: Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) | **www.cybercompetence.sk**

ISBN 978-80-69011-23-6
Verzia V.1