Profil koncovej používateľskej stanice Platforma OS Windows

Obsah

1. Účel dokumentu 2
2. Základná úroveň bezpečnosti koncovej stanice 2
3. Odporúčané postupy a nastavenia 2
3.1. Používateľské účty 3
3.2. Inštalácia programov 3
3.3. Tvorba a uchovávanie hesiel 3
3.4. Použitie anti-malwarového riešenia 3
3.5. Použitie brány firewallu 4
3.6. Aktualizácie systému a aplikácií 4
3.7. Používanie počítača 4
3.8. Používanie Internetu 5

1. Účel dokumentu

Tento dokument vznikol za účelom zhrnutia základných odporúčaných postupov a nastavení s cieľom dosiahnuť základné bezpečnostné opatrenia pre počítač s nainštalovaným systémom na platforme Windows v domácom prostredí. Dokument definuje základnú úroveň bezpečnosti koncovej stanice a opatrenia, ktoré je potrebné implementovať na dosiahnutie tejto úrovne.

Súčasne dokument definuje spôsob ochrany detí prostredníctvom rodičovskej kontroly.

2. Základná úroveň bezpečnosti koncovej stanice

Najskôr si zadefinujeme základnú úroveň zabezpečenia počítača na platforme Windows, ktorú sa budeme snažiť v ďalších častiach dokumentu dosiahnuť pomocou konfiguračných nastavení a odporúčaných postupov ako pracovať s počítačom. Základná úroveň bezpečnosti koncovej stanice na platforme Windows musí spĺňať nasledovné body:

- Koncová stanica je chránená pred štandardnými formami škodlivého kódu.
- Koncová stanica umožňuje komunikáciu iba na povolené služby.
- Koncová stanica má aktuálny, výrobcom podporovaný softvér a to najmä:
  - Operačný systém
  - Kancelárske balíky
  - Frameworky Java a .NET
  - Prehliadače PDF
  - Audio a video prehrávače
- V počítači sa nachádza iba legálny softvér a obsah z dôveryhodných zdrojov.
- Používateľ na počítači vykonáva činnosť pod neprivilegovaným účtom.
- Používateľ na počítači obozretne pristupuje k elektronickej pošte, webovým stránkam a obsahu získanému z prostredia Internetu.

V kontexte ochrany maloletého používateľa (dieťaťa) musí ešte základná úroveň bezpečnosti koncovej stanice na platforme Windows spĺňať nasledovný bod:

- Koncová stanica je kontrolovaná administrátorom (rodičom) z hľadiska:
  - Prístupu dieťaťa k počítaču (prihlásenia sa).
  - Prístupu dieťaťa iba k vhodnému obsahu na Internete.
  - Prístupu dieťaťa k vhodným aplikáciám a službám.
  - Kontrola činnosti dieťaťa na počítači.

3. Odporúčané postupy a nastavenia

V tejto časti sa nachádzajú odporúčané postupy pre zníženie pravdepodobnosti výskytu alebo dopadov niektorých štandardných rizík na počítače, ktoré je odporúčané aplikovať a dodržiavať.

3.1. Používateľské účty

1. Je nutné používať výhradne účet pre bežného používateľa a iba v nutnom prípade použiť administrátorsky účet.
2. Používať samostatný používateľský účet na využívanie služieb ako je napr. Internet Banking a podobne.

3.2. Inštalácia programov

1. Je potrebné inštalovať a používať iba legálne aplikácie, ktoré sú získané iba z dôveryhodného zdroja. V prípade, že na stránke výrobcu je aj kontrolný súčet je odporúčané tento kontrolný súčet overiť.
2. Rozšírenia do internetového prehliadača je vhodné inštalovať iba z dôveryhodných zdrojov.

3.3. Tvorba a uchovávanie hesiel

1. Heslá nesmú byť uchovávané v elektronickej alebo papierovej podobe v nechránenom priestore. Ideálne je potrebné ich uchovávať iba v pamäti používateľa alebo v špecializovanom programovom vybavení, určenom pre tento účel.
2. Heslá nesmú byť rovnaké pre rôzne účty.
3. Heslá je potrebné vytvárať dostatočne komplexné, aby sa pravdepodobnosť úspechu útokov hádaním alebo hrubou silou minimalizovala. Treba používať malé a veľké písmená, čísla, diakritika a ostatné tlačiteľné znaky.
4. Dĺžka hesla by mala mať aspoň 9 znakov.
5. Heslá nesmú byť asociovateľné s používateľom, nesmú mať slovníkový význam a nesmú byť vytvorené miernou modifikáciou predchádzajúcich typov.
6. Heslá je potrebné pravidelne meniť.
7. Heslá do dôležitých účtov je potrebné meniť aspoň raz za 12 mesiacov.
8. Heslá do menej dôležitých účtov je potrebné meniť aspoň raz za 2 roky.
9. V prípade, že existuje podozrenie na odhalenie hesla je nutné vykonať zmenu hesla okamžite, teda kontaktovať v tejto veci administrátora počítača a udalosť nahlásiť aj ako bezpečnostný incident správcovi služby, ku ktorej bolo možné odhaleným heslom pristupovať.

3.4. Použitie anti-malwarového riešenia

1. Anti-malwarové riešenie inštalujte hneď po nainštalovaní operačného systému. Ak to nie je možné, je potrebné ho inštalovať v najskoršom možnom čase.
2. Je potrebné aktualizovať pravidelne anti-malwarovú databázu signatúr. Ideálnym intervalom aktualizácie je jeden deň pri počítači pripojenom k Internetu a jeden týždeň pri počítači nepripojenom do Internetu.
3. V anti-malwarovom riešení je potrebné povoliť rezidentnú ochranu.

3.4.1. Kontrola systému

1. Systém je potrebné pravidelne kontrolovať na prítomnosť škodlivého kódu vo forme prehliadky všetkých súborov a aj bootovacej partície. Ak je to možné, tak je treba nastaviť túto kontrolu ako automatizovanú. Odporúčaná frekvencia úplnej kontroly je jeden mesiac.

2. Pred spustením alebo skopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory skontrolovať anti-malwarovým riešením.

3.5. Použitie brány firewallu

1. Firewall je potrebné nainštalovať skôr ako je počítač pripojený k sieti.
2. Je potrebné ho pravidelne aktualizovať, ideálnym intervalom aktualizácie je jeden deň.

3.5.1. Nastavenie

1. Všetko je potrebné zakázať a povoľujú sa iba potrebné služby.
2. Ak počítač neslúži ako server alebo na zdieľanie priečinkov alebo tlačiarní, je vhodné zakázať akúkoľvek iniciáciu spojenia zo siete.
3. V prípade, že firewall umožňuje učenie sa prostredníctvom interakcie s používateľom, je potrebné povoľovať pri tejto interakcii iba také akcie, ktoré používateľ sám spustil a povoľovať spojenie do Internetu iba dôveryhodným aplikáciám.
4. Pre jednotlivé firewally je potrebné si prečítať odporúčanú konfiguráciu firewallu od výrobcu alebo „best practises“ pre daný firewall z dôveryhodného zdroja a na základe týchto zdrojov firewall nastaviť.

3.6. Aktualizácie systému a aplikácií

1. Operačný systém by mal byť podporovaný výrobcom a v aktuálnej verzii.
2. Operačný systém je potrebné pravidelne aktualizovať. Ak to systém umožňuje je potrebné nastaviť automatické aktualizácie operačného systému.
3. Nainštalované aplikácie je potrebné pravidelne aktualizovať. Ak to aplikácia umožňuje je potrebné ju nastaviť na automatické inštalovanie aktualizácie, prípadne nastaviť zobrazovania upozornenia na novú aktualizáciu.
4. Je potrebné pravidelne aktualizovať aj doplnky aplikácií (plugins, kodeky audio a video formátov).

3.7. Používanie počítača

3.7.1. Prihlasovanie sa

1. Do počítača je potrebné vždy nastaviť prístupové heslo.
2. Pri odchode od počítača je potrebné vždy počítač zamknúť alebo odhlásiť sa.
3. Šetrič obrazovky je potrebné nastaviť tak, aby pri jeho vypnutí bolo potrebné heslo.
4. Heslo nesmie byť zapísané nikde v okolí počítača, teda nie na viditeľnom alebo ani menej viditeľnom mieste.

3.7.2. Šifrovanie

1. Všetky citlivé dáta v počítači je potrebné uchovávať iba v šifrovanej podobe.
2. Vhodným riešením je použitie šifrovaného disku, ako napr. softvérové nástroje TrueCrypt a BitLocker.

3.7.3. Zálohovanie

1. Všetky dôležité dáta je potrebné si zálohovať mimo počítača pravidelne v šifrovanej podobe. Odporúčaný interval zálohovania je jeden mesiac pri menej dôležitých dátach, týždeň pri dôležitých dátach a každý deň pri veľmi dôležitých a kritických dátach.
2. Zálohované dáta je potrebné pravidelne kontrolovať, či záloha prebehla v poriadku. Odporúčaný interval kontroly záloh je jeden mesiac.

3.8. Používanie Internetu

1. Svoje heslá a prihlasovacie údaje nikdy nikam neposielajte e-mailom, chatom, ani iným spôsobom. V prípade, že prišla požiadavka aj zo zdanlivo dôveryhodného zdroja je potrebné túto požiadavku odmietnuť a nahlásiť ju zodpovedajúcim miestam ako bezpečnostný incident. Platí to zvlášť pre dôležité účty ako sú Internet Banking alebo účet do pracovnej stanice.
2. Pri prístupe na zabezpečené stránky prostredníctvom protokolu https je potrebné vždy overiť certifikát.
3. Pred registráciou na stránku je potrebné si dôkladne prečítať podmienky používania.
4. Pri odchode zo stránky je vždy potrebné odhlásiť sa z danej stránky.
5. Je vysoko odporúčané nešíriť reťazové e-maily a neoverené varovania prostredníctvom e-mailu.
6. Je vysoko odporúčaná opatrnosť na stránkach, ktoré ohlasujú výhry. Je veľká pravdepodobnosť, že tu existuje snaha o podvod.
7. Nikde na Internete by sa nemalo zadávať číslo platobnej karty, ani ďalšie údaje obsiahnuté na tejto karte, okrem prípadov, keď ňou chce používateľ platiť. Aj v tomto prípade je ale potrebná opatrnosť a využívanie služieb iba dôveryhodných elektronických obchodov.
8. Je vysoko odporúčané zvýšiť opatrnosť pri používaní neznámych anti-malwarových aplikácií. Môže sa jednať o falošný anti-malwarový program s cieľom infiltrovať Vaše zariadenie.
9. Po ukončení práce s prehliadačom je vhodné vymazať históriu, uložené dočasné súbory a *cookies*.