MINISTERSTVO ZDRAVOTNÍCTVA SLOVENSKEJ REPUBLIKY

Informačná bezpečnosť a ochrana údajov

Vážení poskytovatelia zdravotnej starostlivosti

Bezpečnosť je pre nás prvoradá, preto by sme Vás radi upozornili, že pred dvoma rokmi ukončila spoločnosť Microsoft podporu a aktualizáciu systému Windows XP. Počítače s Windows XP sú tak vo zvýšenej miere ohrozené vírusmi a škodlivým softvérom. Zároveň s ukončením podpory Windows XP prestávajú aktualizácie svojich aplikácií pre tento systém vydávať i nezávislí dodávatelia. Z tohto dôvodu je ďalšie používanie operačného systému Windows XP bezpečnostným rizikom, ktoré by ste mali zvážiť, pokiaľ ho budete používať na prihlasovanie sa do Národného zdravotníckeho informačného systému (NZIS). **Aj špecializovaný útvar CSIRT.SK používanie operačného systému Windows XP neodporúča.** Jeho používanie znamená pre poskytovateľov zdravotnej starostlivosti podľa CSIRT.SK bezpečnostné i legislatívne riziká. Od 8. apríla 2014, kedy spoločnosť Microsoft pre tento operačný systém ukončila podporu, nie sú preň už naďalej vydávané aktualizácie, bezpečnostné záplaty a hotfixy. Používanie tohto systému predstavuje riziko nákazy pracovnej stanice viacerými druhmi škodlivého softvéru s veľmi negatívnymi potenciálnymi dôsledkami. Patrí k nim predovšetkým únik citlivých informácií, ich modifikácia alebo zničenie. Pre poskytovateľov zdravotnej starostlivosti to znamená priame ohrozenie osobitných kategórií osobných údajov a podľa názoru CSIRT.SK je spracúvanie týchto údajov na takto zraniteľnom systéme porušením povinnosti *„chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením"* ustanovenej zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v platnom znení. Prevádzkovateľ, ktorým je každý poskytovateľ zdravotnej starostlivosti je povinný prijať bezpečnostné opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, pričom musí vziať do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov a rozsah možných rizík spôsobilých narušiť bezpečnosť a funkčnosť informačného systému. **Medzi opatrenia**, ktoré ustanovuje vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v platnom znení, okrem iného, **patrí aj „aktualizácia operačného systému a programového aplikačného vybavenia".**

Rovnako zodpovedne ako Ministerstvo zdravotníctva SR a Národné centrum zdravotníckych informácií (NCZI) na problém s používaním Windows XP nazerajú aj bankové inštitúcie, ktoré tiež z bezpečnostných dôvodov nepodporujú prihlásenie sa do ich internetbankingu z počítačov s operačným systémom Windows XP a upozorňujú, že každý užívateľ, ktorý Windows XP naďalej používa, tak koná na svoju vlastnú zodpovednosť. Podobne aj Finančná správa SR informuje verejnosť, že vzhľadom na ukončenie podpory operačného systému Windows XP zo strany výrobcu nie je možné garantovať plnú podporu pri aplikáciách finančnej správy v tomto prostredí.

NCZI ako správca a prevádzkovateľ NZIS teda neodporúča používanie operačného systému Windows XP na prihlasovanie sa do NZIS a každý poskytovateľ zdravotnej starostlivosti, ktorý ho naďalej používa, tak koná na vlastnú zodpovednosť. Odporúčame aktualizáciu na novšiu verziu systému Windows s funkčnou podporou výrobcu. Viac informácií nájdete na oficiálnych stránkach spoločnosti Microsoft http://windows.microsoft.com/sk-sk/windows/end-support-help Jedine pravidelne aktualizovaný softvér podporovaný výrobcom daného systému zaručuje dostatočnú bezpečnosť.

Je potrebné mať na pamäti dodržiavanie bezpečnostných štandardov kladených na Vaše počítačové systémy, ktorými sa prihlasujete do NZIS. V rámci verejnej správy, ale aj v rámci súkromného sektora sú na podporu rozvoja všeobecnej informačnej bezpečnosti špecializovaným útvarom CSIRT.SK sformulované tieto bezpečnostné štandardy a zásady, ktoré je potrebné dodržiavať:

CSIRT.SK sa odvoláva na dodržiavanie bezpečnostných štandardov uvedených vo výnose Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v platnom znení a na aplikáciu bezpečnostných opatrení ustanovených vyhláškou č. 164/2013 Z. z. Okrem splnenia legislatívnych požiadaviek CSIRT.SK odporúča nasledovné opatrenia:

Použitie antivírusového softvéru:

1. Inštalácia:

- Antivírusový systém inštalujte hneď po nainštalovaní operačného systému. (Ak to nie je možné, je potrebné ho inštalovať v najskoršom možnom čase.)

2. Aktualizácia:

- Je potrebné pravidelne aktualizovať antivírusovú databázu škodlivého kódu. (Ideálnym intervalom aktualizácie je menej ako jeden deň pri počítači pripojenom k Internetu a jeden týždeň pri počítači nepripojenom do Internetu.)

3. Rezidentná ochrana:

- V antivírusovom riešení je potrebné povoliť rezidentnú ochranu systému (ochrana počítača počas bežnej prevádzky).

4. Prehliadka systému:

- Systém je potrebné pravidelne prehliadať na prítomnosť škodlivého kódu vo forme prehliadky všetkých súborov a aj bootovacej partície. Ak je to možné, tak je potrebné nastaviť túto kontrolu ako automatizovanú. Odporúčaná frekvencia úplnej kontroly je jeden mesiac.
- Pred spustením alebo kopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory prehliadnuť antivírusovým systémom. (Uvedená voľba sa najčastejšie nachádza v kontextovom menu súborov.)

5. Antivírusové riešenia (najčastejšie používané):

- Platforma Windows
  - o Freeware: AVG Personal, Avast, ...
  - o Komerčné riešenia: NOD, AVG, Symantec, ...
- Platforma Linux
  - o Freeware: ClamAV, ...
  - o Komerčné riešenia: Panda, Symantec, ...

Použitie bezpečnostnej brány (firewall):

1. Inštalácia:

- Osobný firewall je potrebné nainštalovať skôr ako je počítač pripojený k sieti.

2. Aktualizácia:

- Osobný firewall je potrebné pravidelne aktualizovať.
- (Ideálnym intervalom aktualizácie je jeden deň)

3. Nastavenie:

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

4. Firewall a „personal security" riešenia (najčastejšie používané):

- Platforma Windows
  - o Freeware riešenia: Windows Firewall, Comodo Personal ,...
  - o Komerčné riešenia: Eset Smart Security, Symantec, ...
- Platforma Linux
  - o Freeware riešenia: iptables

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, tak je potrebné nastaviť automatické aktualizácie operačného systému.

3. Nainštalované aplikácie je potrebné pravidelne aktualizovať.

Použitie antispyware riešenia (ochrana pred škodlivým kódom nevírusového charakteru):

1. Inštalácia:

- Antispyware riešenie je potrebné nainštalovať pred pripojením do Internetu.

2. Aktualizácia:

- Antispyware riešenie je potrebné aktualizovať pravidelne. Ideálne každý deň.

3. Prehliadka systému:

- Systém je potrebné pravidelne prehliadať na prítomnosť škodlivého kódu vo forme prehliadky všetkých súborov. Ak je to možné, tak je potrebné nastaviť túto kontrolu ako automatizovanú. Odporúčaná frekvencia úplnej kontroly je jeden mesiac.
- Pred spustením alebo kopírovaním súboru (súborov) z neznámeho média je potrebné tieto súbory prehliadnuť antispyware systémom (Uvedená voľba sa najčastejšie nachádza v kontextovom menu súborov).

4. Antispyware riešenia (najčastejšie používané):

- Platforma Windows
  o Freeware: AVG Personal, Ad-aware, Spybot, ...
  o Komerčné riešenia: AVG, Microsoft Windows AntiSpyware, ...

Tvorba a uchovávanie hesiel:

1. Heslá nesmú byť uchovávané v elektronickej alebo papierovej podobe v nechránenom priestore. Ideálne je ich potrebné uchovávať iba v pamäti používateľa alebo v špecializovanom, na to určenom programovom vybavení.

2. Heslá nesmú byť rovnaké pre rôzne účty.

3. Heslá je potrebné vytvárať dostatočne komplexné, aby sa zabránilo útokmi hádaním alebo hrubou silou (malé a veľké písmená, čísla, diakritika, ostatné tlačiteľné znaky). Dĺžka hesla by mala byť aspoň 12 znakov.

4. Heslá nesmú byť asociovateľné s používateľom, mať slovníkový význam alebo byť vytvorené miernou modifikáciou predchádzajúcich typov.

5. Heslá je potrebné pravidelne meniť.

6. Heslá do dôležitých účtov je potrebné meniť aspoň raz za 2-3 mesiace.

7. Heslá do menej dôležitých účtov je potrebné meniť aspoň raz za rok.

8. V prípade, že existuje podozrenie na kompromitáciu hesla je nutné vykonať zmenu hesla okamžite a udalosť nahlásiť ako bezpečnostný incident správcovi počítača/siete.

Inštalácia programov:

1. Je potrebné inštalovať a používať iba legálne aplikácie, ktoré sú získané iba z dôveryhodného zdroja. V prípade, že je na stránke výrobcu aj kontrolný súčet, odporúča sa tento kontrolný súčet overiť.

2. Rozšírenia do Internetového prehliadača je vhodné inštalovať iba z dôveryhodných zdrojov.

Používanie Internetu:

1. Svoje heslá a prihlasovacie údaje nikdy nikam neposielajte 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, účet do pracovnej stanice alebo intranetu organizácie.

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 potrebné sa vždy odhlásiť" z danej stránky.

5. Je vysoko odporúčané nešíriť reťazové maily a neoverené varovania prostredníctvom emailu.

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 potrebná opatrnosť a využívanie služieb iba dôveryhodných elektronických obchodov.

8. Je vysoko odporúčaná opatrnosť pri používaní neznámych antivírových aplikácií. Môže sa jednať o falošný antivírový program s cieľom infiltrovať Vaše zariadenie.

9. Po ukončení práce s prehliadačom je vhodné vymazať históriu a uložené dočasné súbory a „cookies".

10. Vo webovom prehliadači sa odporúča využívať rozšírenia: Adblock, NoScript a Ghostery.

Používanie počítača:

1. ***Prihlasovanie:***

- Do počítača je potrebné vždy nastaviť prístupové heslo.
- Pri odchode od počítača je potrebné vždy počítač zamknúť alebo odhlásiť" sa.
- Šetrič obrazovky je potrebné nastaviť tak, aby pre jeho vypnutie bolo potrebné heslo.
- Heslo nesmie byť zapísané nikde v okolí počítača na viditeľnom ani menej viditeľnom mieste.

2. ***Šifrovanie:***

- Všetky citlivé dáta v počítači je potrebné uchovávať iba v šifrovanej podobe.
- Vhodným riešením je použitie šifrovaného disku (Napríklad softvérové nástroje Truecrypt a Bitlocker) alebo šifrovanie celého disku (v prípade, že to interné smernice povoľujú).

3. ***Zálohovanie:***

- 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.
- Zálohované dáta je potrebné pravidelne kontrolovať, či záloha prebehla v poriadku. Odporúčaný interval kontroly záloh je jeden mesiac.

CSIRT.SK vypracoval viaceré návody pre zaistenie bezpečnosti koncových staníc a zverejnil ich na svojom webovom portáli
(www.csirt.gov.sk).