ZÁKLADNÍ BEZPEČNOSTNÍ OPATŘENÍ PRO VRCHOLOVÉ VEDENÍ ORGANIZACE

Tento dokument je určen vrcholovému vedení organizací a čelným představitelům institucí – osobám, které mají největší vliv na směřování dané organizace a mají významné rozhodovací pravomoci. Důležitost těchto osob je však zároveň staví do pozice, kdy jsou lákavým cílem pro útočníky snažící se narušit kybernetickou bezpečnost organizace. Z tohoto důvodu je pro tyto osoby doporučeno dodržovat níže uvedená opatření ke snížení rizika ohrožení fungování organizace a naplňování povinnosti péče řádného hospodáře. Zároveň je potřeba mít vždy na paměti, že chování vrcholového vedení má odraz v chování běžných zaměstnanců – pokud vrcholové vedení pravidla nerespektuje, lze těžko vyžadovat plnění pravidel i po řadových zaměstnancích.

Tento dokument je doporučením a nenahrazuje žádné právní předpisy, tedy zejm. právní úpravu kybernetické bezpečnosti. Tento dokument nemůže nikdy pokrýt veškerá opatření, která lze aplikovat. Další opatření nad rámec tohoto dokumentu, vhodná pro danou organizaci, mohou navrhnout bezpečnostní specialisté v dané organizaci.

HLAVNÍ BEZPEČNOSTNÍ PRAVIDLO

RESPEKTOVAT BEZPEČNOSTNÍ POKYNY SPECIALISTŮ V DANÉ ORGANIZACI.
Každá organizace by se měla snažit dosahovat bezpečného prostředí a nakládání s daty. Za tímto účelem organizace také obvykle zaměstnává specialisty, kteří mají zabezpečení organizace na starosti. Jejich doporučeními, pokyny a návrhy je nutné se řídit a dodržovat je, jinak nemůže být bezpečnost nikdy na přijatelné úrovni. Neváhejte se na ně obrátit v případě dotazů nebo potřeby upřesnění těchto základních opatření.

PRÁCE S FIREMNÍM POČÍTAČEM NEBO SMARTPHONEM

NEPOUŽÍVAT SOUKROMÁ ZAŘÍZENÍ PRO PRACOVNÍ ÚČELY.
Soukromá zařízení nejsou pod správou organizace. S používáním soukromých zařízení je obvykle spojeno jejich neustálé přenášení, snížený dohled či sdílení se členy rodiny. Dále obsahují aplikace, které nejsou nutné k pracovním účelům. To vše přináší zvýšené riziko pro bezpečnost uživatele i celé organizace. Pokud jsou v organizaci soukromá zařízení přesto používána, obraťte se na bezpečnostní specialisty v organizaci a řiďte se jejich pokyny.

OMEZIT PŘÍSTUP K PRACOVNÍM ZAŘÍZENÍM A UZAMKNOUT JE POKAŽDÉ, KDYŽ JE POTŘEBA SE OD NICH VZDÁLIT.
Nehlídané zařízení dává prostor útočníkovi. Odemknuté zařízení bez dozoru dává komukoliv prostor k manipulaci s ním i jeho obsahem. To je potřeba mít na paměti nejen v kanceláři, ale především na veřejných místech (např. na konferenci, ve vlaku, apod.).

U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L.

U MAC počítače je nejjednodušší způsob rychlého zamknutí klávesová zkratka COMMAND + CONTROL + Q.

U mobilního zařízení stisknutí zamykacího tlačítka.

NEPŘIPOJOVAT NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Neznámá zařízení mohou obsahovat škodlivý kód, který se ihned po připojení dostane do zařízení. V případě nevyhnutelné nutnosti připojit neznámé médium je potřeba provést alespoň antivirovou kontrolu tohoto zařízení.

POUŽÍVAT HESLA, ČÍSELNÉ KÓDY NEBO JINÉ ZPŮSOBY ZABEZPEČENÍ TAK, JAK JE MÁ ORGANIZACE ZAVEDENÉ.
V případě ztráty nebo odcizení je zařízení podstatně lépe chráněno.

VOLIT DLOUHÉ, ZAPAMATOVATELNÉ FRÁZE PRO HESLA, PŘÍPADNĚ POUŽÍVAT SPRÁVCE HESEL.
Šifrovaný správce hesel umožňuje jednoduchou a bezpečnou správu všech potřebných přihlašovacích údajů a hesel na jednom místě.

PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ A HESEL SE UJISTIT, ŽE JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.
Především v případě pohybu na veřejném místě s větším počtem lidí, kamer nebo fotoaparátů (např. na konferenci, ve vlaku apod.), je zvýšené riziko, že útočník jednoduše zjistí a následně použije tyto údaje. V případě mobilních telefonů preferovat odemykání zařízení pomocí otisku prstu nebo skenu obličeje.

PROVÁDĚT AKTUALIZACI ZAŘÍZENÍ A NEVYPÍNAT PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU A PROGRAMŮ.
Aktualizace zařízení je způsob, jakým výrobce zařízení opravuje nově známé zranitelnosti, které by mohly toto zařízení ohrozit. Pokud má být aktualizace provedena, je potřeba jí nebránit a neodsouvat termín jejího provedení. Termín pravidelných automatických aktualizací je obvykle možno v zařízení nastavit. Stejně jako je tomu v případě aktualizací systému, také programy je potřeba aktualizovat. Program, který doposud fungoval bez problému, může být bez aktualizace téměř nepoužitelný a nebezpečný.

VYUŽÍVAT MOŽNOSTI ŠIFROVÁNÍ DAT NA INTERNÍCH I EXTERNÍCH ZAŘÍZENÍCH.
Šifrování zabezpečí data především při ztrátě nebo odcizení zařízení. Data na pracovním počítači by měla být šifrována, ale je nutno mít na paměti také ostatní zařízení, na kterých se tato data vyskytují.

PRAVIDELNĚ ZÁLOHOVAT DATA.
Vždy existuje riziko ztráty dat. Může se jednat o poruchu zařízení, jejich ztrátu nebo cílený útok, který data nenávratně zašifruje. Je proto vhodné myslet na zálohu důležitých dat a tuto zálohu uchovávat na jiném místě než v zařízení samotném, šifrovat a připojovat ji k zařízení pouze v okamžiku zálohování. Nezálohujte pracovní data na jiná než organizací určená zařízení.

VYVAROVAT SE POUŽITÍ VEŘEJNÉ WI-FI A DALŠÍCH VEŘEJNĚ NEBO ZDARMA POSKYTOVANÝCH SLUŽEB.
Veřejně poskytovaná Wi-Fi a další služby jsou jednoduchým způsobem, jak může útočník proniknout do zařízení a mít přehled o všech činnostech, především o použití přihlašovacích údajů a hesel. Problémem jsou zejména veřejné a nezabezpečené Wi-Fi (např. bez hesla, ale také s veřejně dostupným heslem – např. restaurace, konference apod.), a pokud to není nutné, je vhodné se k nim vůbec nepřipojovat. Tento problém je možné snížit použitím zabezpečeného spojení (tzv. VPN), nejvhodnější je pak používat VPN v kombinaci s mobilním internetem.

VĚNOVAT ZVÝŠENOU POZORNOST BEZDRÁTOVÝM TECHNOLOGIÍM, JAKO JE WI-FI, BLUETOOTH, NFC A DALŠÍ.
Bezdrátové technologie v zařízení je vhodné zapnout jen tehdy, pokud jsou využívány – představují potenciální cestu, jak proniknout do zařízení.

KONTROLOVAT, ZDA WEBOVÉ STRÁNKY PODPORUJÍ PROTOKOL HTTPS.
V případě internetových stránek, které vyžadují přihlášení (zejm. internetové bankovnictví, e-mail apod.), je potřeba věnovat pozornost, zda je taková stránka zabezpečena HTTPS protokolem. Pokud tomu tak není, nejsou zadané údaje vhodně zabezpečeny a jsou jednoduše zneužitelné.

Zobrazení HTTPS protokolu v internetovém prohlížeči

Zobrazení v internetovém prohlížeči bez protokolu HTTPS (přes tyto stránky nezadávat hesla)

NA INTERNETOVÉ ODKAZY KLIKAT OBEZŘETNĚ.
Je-li to možné, zkontrolovat, že odkaz nevede na podezřelou URL adresu. Skutečná URL adresa se po umístění kurzoru myši na odkaz bez rozkliknutí zobrazí vedle kurzoru (viz ilustrační obrázek), případně v okénku v levém dolním rohu stránky. Pokud nelze ověřit, kam odkaz vede, neklikat na něj.

Další informace o námi poskytované službě naleznete na našich internetových stránkách www.poskytovane-sluzby.cz.

http://adminmicrosofupda.wxisite.com/mys...
Kliknutím nebo klepnutím přejdete na odkaz.

SPRÁVNÁ A BEZPEČNÁ KOMUNIKACE

PŘISTUPOVAT K INFORMACÍM NA INTERNETU KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Je potřeba ověřovat, zda jsou informace skutečně pravdivé a zda jsou uvedeny v patřičném kontextu.

NEZVEŘEJŇOVAT OSOBNÍ ANI JINÉ CITLIVÉ INFORMACE.
Je potřeba zvážit, zda je skutečně nutné určité informace zveřejňovat. Data narození, náboženské vyznání nebo například fotografie mohou být následně zneužity, a to ať už proti konkrétním osobám, tak i proti organizaci, kterou tyto osoby zastupují.

OVĚŘIT IDENTITU PROTISTRANY PŘI KOMUNIKACI.
Je potřeba mít na paměti, že osoba, se kterou je komunikováno, se může vydávat za někoho jiného, což je zvláště důležité při prvotní komunikaci. Pokud existuje podezření, že osoba není tou, za kterou se vydává, je možné např. zavěsit a zavolat zpátky na telefonní číslo z oficiálního seznamu.

VĚNOVAT OBSAHU E-MAILŮ ZVÝŠENOU POZORNOST A V PŘÍPADĚ PODEZŘELÉHO E-MAILU NEBO PŘÍLOHY INFORMOVAT IT/BEZPEČNOSTNÍ ODDĚLENÍ ORGANIZACE.
Prostřednictvím příloh e-mailové zprávy se může jednoduše šířit škodlivý kód, který se po otevření přílohy aktivuje. Z tohoto důvodu je potřeba otevírat jen takové e-maily a jejich přílohy, které jsou důvěryhodné, a o těch podezřelých informovat IT oddělení.

CO JE TO PHISHING?
Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat uživatele na podvodnou stránku, nebo zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí. Neváhejte se obrátit na bezpečnostní specialisty v organizaci s dotazy, jak phishing poznat, případně využijte doporučení zveřejněná na stránkách NÚKIB, v sekci Infoservis – Doporučení – Spear-phishing a jak se před ním chránit.

NESDÍLET INFORMACE, KTERÉ JDOU NAD RÁMEC POTŘEBY AKTUÁLNÍ SITUACE.
Vše, co je obsahem komunikace, může být v budoucnu zneužito.

MÍT NA PAMĚTI, ŽE NIC NENÍ ZADARMO.
Nabídky a on-line služby zdarma, které jsou jindy placené, je potřeba důkladně zvažovat.

POKUD PROBÍHÁ KOMUNIKACE V ČASOVÉ TÍSNI, JE POTŘEBA O TO VÍCE UVAŽOVAT O JEJÍM OBSAHU A SDĚLOVÁNÍ POŽADOVANÝCH INFORMACÍ.
Útočníci rádi pracují s časovou tísní – teď je třeba něco vykonat, napravit, sdělit. Je potřeba to mít na paměti. Škoda z prodlení bývá menší než důsledky neuvážených činů.

ZABEZPEČENÍ ON-LINE ÚČTŮ

NEPOUŽÍVAT SOUKROMÉ ÚČTY PRO PRACOVNÍ ÚČELY A OBRÁCENĚ.
Soukromé účty (e-mailové schránky, cloudové služby, apod.) uživatele nejsou pod dohledem organizace a jsou tak pro organizaci zvýšeným rizikem např. z důvodu zvýšeného rizika infikování firemní sítě škodlivým kódem. Platí to i obráceně; pracovní účty není žádoucí používat pro soukromé účely.

PŘÍSTUPY K PRACOVNÍM ÚČTŮM CHRÁNIT HESLY. PRO KAŽDOU SLUŽBU POUŽÍVAT JINÉ UNIKÁTNÍ HESLO.
V případě používání slabého hesla je jeho prolomení útočníkem otázkou okamžiku. Pokud dojde k vyzrazení hesla k jednomu účtu, má útočník možnost použít stejné heslo i u jiných účtů.

NESDĚLOVAT JINÝM OSOBÁM PŘIHLAŠOVACÍ ÚDAJE A HESLA K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu nebo hesla do počítače může mít takové jednání závažné následky.

V PŘÍPADĚ, ŽE JE TO MOŽNÉ, VYUŽÍVAT VÍCEFAKTOROVOU AUTENTIZACI, A TO PŘEDEVŠÍM U SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL A DALŠÍ.
Běžným způsobem realizace vícefaktorové autentizace je obdržení kontrolní SMS po zadání přístupových údajů. V organizaci však mohou existovat i jiné způsoby vícefaktorové autentizace uživatelů.

PRO BĚŽNOU ČINNOST VYUŽÍVAT BĚŽNÝ UŽIVATELSKÝ ÚČET. ADMINISTRÁTORSKÝ ÚČET JE URČEN PRO TY, KDO VYKONÁVAJÍ SPRÁVU SYSTÉMŮ A ZAŘÍZENÍ V ORGANIZACI.
Administrátorský účet s vyššími oprávněními je určen výhradně pro správu systému, typicky prostřednictvím IT oddělení.

NEPOUŽÍVAT KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nikdy není vhodnou alternativou k obnovení hesla zadávat kontrolní otázky typu „nejmenší planeta sluneční soustavy" či „rodné jméno manželky". Podobné informace jsou či mohou být dohledatelné z veřejných zdrojů. Je-li taková kontrolní otázka povinná, je potřeba k ní přistupovat jako k heslu a volit ji tak, aby nebyla dohledatelná.