



ČIMIB

Český institut manažerů informační bezpečnosti

Zásady vzdělávání zaměstnanců v oblasti bezpečnosti ICT a jejich aktivní přístup

Praha, 11.5.2010

Ing. Jan Bukovský, jan.bukovsky@ceb.cz



- **„Best practices“ – ISO / IEC 27001**
- **5.2.2 Školení, vědomí závažnosti a odborná způsobilost**
- Organizace musí zajistit, aby zaměstnanci, kterých se týkají povinnosti určené v Systému řízení bezpečnosti informací (ISMS), **byli kompetentní k výkonu požadovaných úkolů**. Zajišťuje to pomocí:
 - určení nezbytných kompetencí personálu vykonávajícího práci ovlivňující ISMS;
 - **zajištění odpovídajícího školení** nebo podniknutí jiných kroků (např. zaměstnání kvalifikovaného personálu);
 - **vyhodnocení efektivnosti zajištěného školení** a provedených činností;
 - udržování záznamů o vzdělávání, školení, dovednostech, zkušenostech a kvalifikačních předpokladech (viz 4.3.3).
- Organizace musí také zajistit, aby si byl veškerý příslušný personál **vědom závažnosti a významu svých činností** v rámci bezpečnosti informací a svého přínosu k dosažení cílů ISMS.



- Organizace musí provést následující:
- **Formulovat ... a zavést ...plán zvládnutí rizik**, který vymezí odpovídající řídicí činnosti, zdroje, odpovědnosti a priority pro řízení rizik bezpečnosti informací (viz kapitola 5).
- **Zavést bezpečnostní opatření**
- **Určit jakým způsobem bude měřit účinnost vybraných opatření** a stanovit jakým způsobem budou tato měření použita k vyhodnocení účinnosti opatření tak, aby závěry hodnocení byly porovnatelné a opakovatelné. Měření účinnosti opatření poskytuje vedení organizace a zaměstnancům informaci o tom, jak jednotlivá opatření naplňují plánované cíle.
- **Zavést programy školení a programy zvyšování bezpečnostního povědomí (viz 5.2.2).**
- **Řídit provoz ISMS.**
- **Řídit zdroje ISMS (viz 5.2).**
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní události a postupy **reakce na bezpečnostní incidenty**

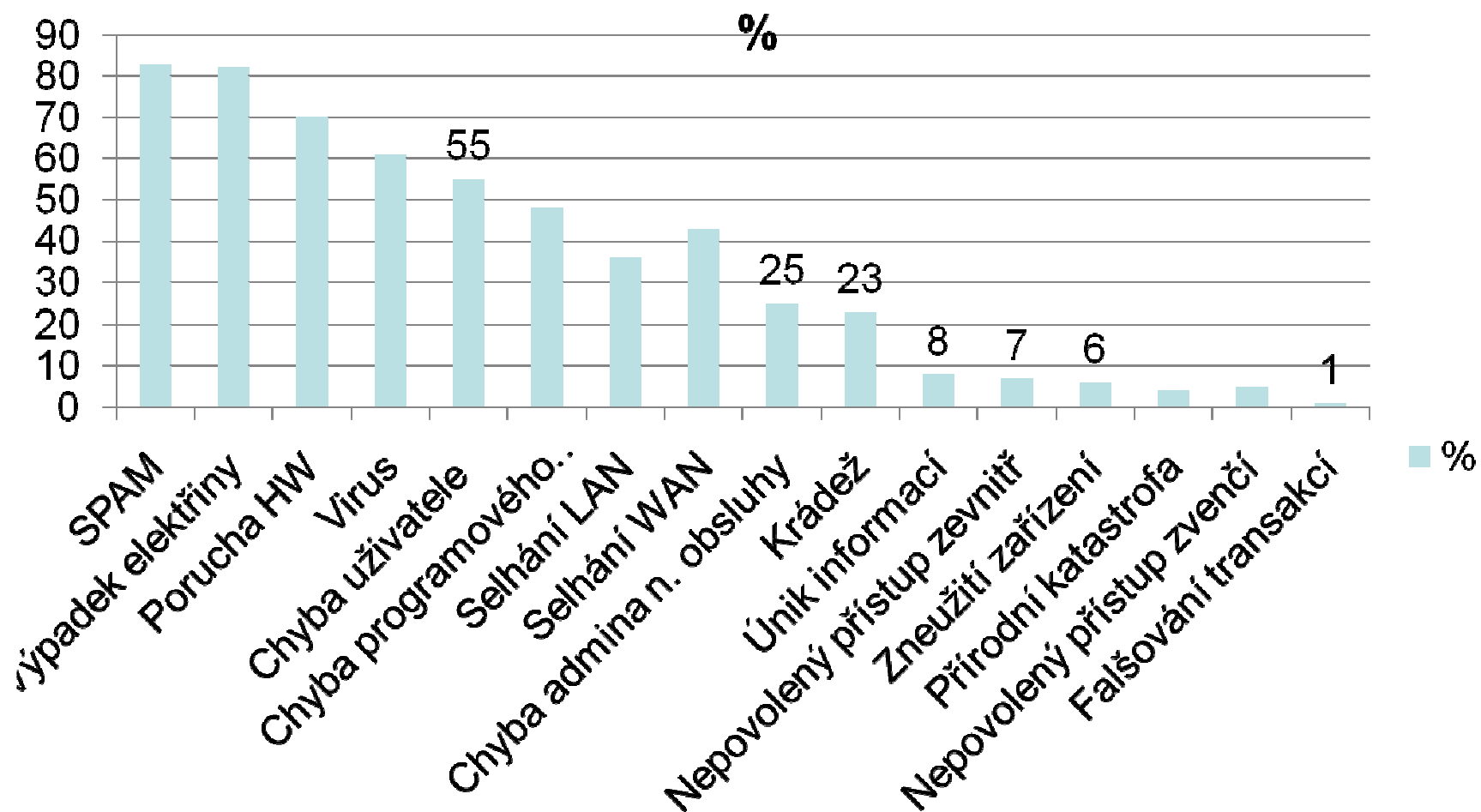


- A.8.2.2
- Povědomí, vzdělávání a školení v oblasti bezpečnosti informací
- *Opatření*
- Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran musí, s ohledem na svoji pracovní náplň, projít odpovídajícím a pravidelně se opakujícím školením v oblasti bezpečnosti informací, bezpečnostní politiky a směrnic organizace.



- Z best practices se požadavek na pravidelná bezpečnostní školení přenáší do
 - Bezpečnostních politik
 - Vnitřních směrnic
 - I některých vyhlášek, metodických pokynů apod.
- Požadavek byl vyvolán situací v devadesátých letech, kdy se ukázalo, že nasazení technických ochranných mechanismů v sítích nestačí .
- Není dobré soustředit se pouze na technická opatření. Pokud potenciální útočník zjistí, že se přes ně nedostane, zvolí jednodušší cestu zevnitř organizace.
- Hlavní cíl: zvýšení bezpečnostního povědomí
- Zajišťování pravidelných školení je součástí opatření personální bezpečnosti





- Cílem hackera je získat přístup do vnitřní sítě (půjčení klíčů, „změna“ hesla telefonem, získání informací o síti) nebo do databáze (platby, účty, partneři...)
- Hacker v podstatě nepotřebuje žádné technické znalosti nebo je použije až následně po získání klíčových informací
- **PHISHING** – k získání informací hacker použije vlastní e-mail nebo WWW stránku obdobného vzhledu nebo vlastností jako známá společnost (výzvy k zadání hesel, změně účtů apod.)
- Měla by omezit vhodná personální politika a znalost tohoto nebezpečí ze strany zaměstnanců (osvěta)

- Prozrazování hesel a dalších autentizačních údajů
- Přílišná důvěra k informacím od nedůvěryhodných zdrojů, náchylnost k podlehnutí sociálním technikám
- Slepá důvěra v pracovníky IT
- Podcenění nebezpečí z Internetu, surfování po podezřelých stránkách
- Zasílání důvěrných údajů e-mailem
- Vynášení nezabezpečených informací
- Ukládání důvěrných údajů mimo bezpečná úložiště
- Hrubá neznalost práce s počítačem - vede např. k ztrátám dat
- Zneužívání prostředků zaměstnavatele pro soukromé účely
- Nezabezpečení prostředků IT (nezamčené kanceláře, neodhlášený počítač, nevypínání na noc)
- Porušení autorského zákona, licenční politiky (pokud k tomu mají možnost)
- Zrušení zabezpečení, nevhodná konfigurace (-"-)



- Školení provede:
 - Specializovaná firma
 - Vlastní zaměstnanec (IT, specialita ICT bezpečnosti...)
 - Přímý nadřízený
- Režim:
 - Každý nový pracovník + Všichni např. 1x za 2 roky
 - Všichni např. 1x ročně
 - Spojit s jinými školeními
 - Bezpečnost práce a PO (1x za 2 roky, vedoucí 1x za 3 roky)
 - Jiné pravidelné školení IT, je-li předepsáno
 - Ad hoc s jiným školením IT (např. při přechodu na Windows 7, nový Office, novou význačnou aplikaci)
 - Až v případě napadení auditem nebo kontrolou
- Koho školit
 - Všechny uživatele stejně
 - IT školit samostatně (třeba ještě členit provoz / vývoj / bezpečnost)
 - Management školit samostatně



A. Kompletní obsah všech platných politik a směrnic.

- Včetně vysvětlení potřebné teorie týkající se sítí a jejich zabezpečení

B. Pouze vybrané nejpotřebnější údaje z politik a směrnic

- Pouze vybrané údaje, např. o šifrování a virech



- Bezpečnostní politika - včetně informace, kde je uložena
- Seznam dalších norem v oblasti IT a bezpečnosti IT
- Zásady užívání hesel – včetně toho, jak často se mění, jak musí být složena, že nesmí být nikomu zpřístupněna apod.
- Užívání certifikátů
- Ukončení práce večer, ukončení práce během dne, jak se přihlásit večer/ v sobotu / neděli
- Jak se projevuje vir / spyware, jak postupovat při podezření, jak spustit ručně antivir / antispyware
- Co je zakázáno na Internetu a v e-mailu (viz dále)
- Klasifikace informací v organizaci a její návaznost na IT (sestavy, obrazovky, zákaz rozesílání a kopírování důvěrných informací)
- Tiskárny a zabezpečení tisků
- Šifrování v organizaci
- Zakázáno instalovat programy



- Fyzické zabezpečení – zóny, zamykání, úklid médií
- Připojení USB, jiných periférií, vypalování apod.
- Obecný zákaz pokusů o prolomení zabezpečení
- Seznámení s existencí sociálního hackingu a phishingu
- Řízení kontinuity – kde je umístěn seznam kontaktů, kdo je v havarijním štábu, kde je záložní pracoviště, kde je shromaždiště apod.



- Je zakázáno navštěvovat pornografické stránky, stránky propagující terorismus, fašismus, násilí.
- Je zakázáno používat Internet k poslechu TV nebo rozhlasu.
- Je zakázáno stahovat soubory nesouvisející s pracovní činností (P2P sítě, rapidshare – např. filmy, počítačové hry, hudba a jiné programy...)
- Je omezeno též hraní her přes Internet a provoz sociálních sítí.
- Uživatel nesmí měnit bezpečnostní nastavení prohlížečů (MSIE, FIREFOX).
- Zablokované stránky je možno předat k dalšímu řešení oddělení IT (jsou-li však skutečně podezřelé, odblokovány být nemohou).
- Pokud možno neotevírat přílohu emailu od neznámého odesílatele (viry)
- Je zakázáno používat mail k rozesílání produktů vlastní výdělečné činnosti (nabídky aj.)
- Je zakázáno zneužívat systém elektronické pošty (včetně freemailů dostupných přes internet) k neoprávněnému rozesílání dat majících důvěrný charakter
- Je zakázáno rozesílat „hoax“ zprávy (tj. falešné poplašné zprávy apod.), řetězové dopisy a nevyžádanou poštu (tzv. spam).



- Základní myšlenky školení je vhodné podtrhnout v krátkém resumé, např. s obsahem
 - Užívání hesel
 - Odhlášení uživatele
 - Instalace aplikací
 - Užívání Internetu a e-mailu
 - Klasifikace informací a označování dokumentů (včetně reportů a obrazovek)
 - Tisk
 - Zásada čistého stolu
 - Monitorování aktivit
 - Znalost havarijního plánu
- Resumé by měli uživatelé např. potvrdit podpisem, mělo by být zveřejněno na Intranetu apod.
- Mělo by obsahovat to, co považuje manažer bezpečnosti za nejdůležitější
- Může být součástí bezpečnostní politika, ta je ale často pro běžné uživatele příliš komplikovaná..., nebo samostatný dokument



- Hlavní bezpečnostní chyby při správě systémů
- Hlavní druhy útoků z vnitřní sítě
- Připojení do veřejných sítí
- Zneužívání Internetu vnitřními uživateli k neslužebným účelům
- Antivir vs. antispysware, možnosti ochrany
- Možnosti monitorování
- Nasazení patchů
- Prosazení zásad IT bezpečnosti do systémů při vývoji
- Ochrana vývojového prostředí – vhodnost a možné způsoby oddělení
- Bezpečnost vývoje webových aplikací(OWASP „Top 10“)
- Snižování rizik



Základy bezpečnosti ICT	<ul style="list-style-type: none"> - Bezpečnostní politika - Analýza rizik - Řízení kontinuity
Řízení přístupů	<ul style="list-style-type: none"> - Doména, trust, forest - Lokální a doménová skupina - Zásady pro přidělování práv k aplikacím a složkám - Nastavení group policy – politika hesel - Kdo smí v organizaci rozhodovat o právech a kdo je smí přidělovat
Chyby při správě sítě	<ul style="list-style-type: none"> - Chyby systémové - Chyby „osobní“ (ve správě) - Chyby v konfiguraci - Chyby v „uvědomění“ - Chyby v architektuře - Chyby technologické (exploity)
Hlavní druhy útoků z Internetu	<ul style="list-style-type: none"> - DOS / DDOS - Zneužití otevřených portů - VPN



Hlavní druhy útoků z vnitřní sítě	<ul style="list-style-type: none"> - Zneužití fyzického přístupu (boot) - Sniffing - Password guessing - Útoky na služby - ARP poisoning - Man in the middle
Obrana	<ul style="list-style-type: none"> - Vyznam patchů a aktualizací - IDS a IPS - Nastavení firewallů - Nastavení mailu a internetu - Nastavení stanic a serverů - ACL na aktivních prvcích
Audit a monitoring	<ul style="list-style-type: none"> - Vyhodnocování logů - Vulnerability scanery



- Doba školení od 30 min. až po několik dní (časová dotace)
- Závěrečný test ?
- Motivace ?
- „Originální“ školení nebo video?
- Co působí PROTI získání bezpečnostního povědomí ?
 - Příliš detailní a uživatelům nesrozumitelné podání problematiky
 - Pohodlnost, staré návyky
 - Okolní prostředí, včetně např. hoaxů a spamů obdržených Internetem
- Školení samo nestačí, je třeba:
 - Kontrolovat plnění politik
 - Vynucovat politiky



- Jde o ideální stav
- Možnost získání aktivního přístupu uživatelů
 - Školení
 - Získání důvěry uživatelů při řešení konkrétních situací
 - Motivace (často bohužel spíše negativní – hrozba odebrání notebooku, VPN, práv...)
 - Přesvědčení uživatele, že spolupráce má smysl (bezpečnostní povědomí)
 - Strach z následků
 - Obtěžující chování systému
- Projevy aktivního přístupu
 - Hlášení podezřelého chování WWW stránek a mailů
 - Hlášení podezřelého chování aplikací
 - Iniciativní návrhy řešení v oblasti přístupových práv
 - Seznamování s novinkami, které našel např. na Internetu (často ale hoax)



Děkuji Vám za pozornost...

Ing. Jan Bukovský, jan.bukovsky@ceb.cz

