IBA a bezpečnost

Zásady pro bezpečnou práci s IT na IBA/ÚZIS
dle metodiky ISMS

Přístupová hesla

Zásady:

- Do služeb mimo IBA nepoužívat heslo používané ke zdrojům IBA/ÚZIS, všude používat **unikátní přístupové údaje**
- Platí i pro heslo pro email. Při vyzrazení hackeři začnou využívat váš e-mail k šíření spamu a virů, hrozí zablokování všeho emailu.
- I obráceně platí – nepoužívat soukromá hesla do žádných služeb IBA
- Pokud máme hesel mnoho, používat **softwarového správce hesel**
- **Osobní HESLA zásadně nesdílíme s jinými osobami**
- **Hesla zásadně neposíláme v nezašifrované podobě**
- **Lze poslat formou SMS, ale bez doprovodné informace (login, služba)**
- **Hesla nezapisuji do nešifrovaných dokumentů, na papír pouze krátkodobě pro účely předání**
- **Žádná hesla nesmí být vylepována na monitor, nástěnku apod.**

Správce hesel – užitečný a jednoduchý pomocník pro bezpečnou práci s hesly

Je třeba si pamatovat pouze jedno hlavní heslo, ostatní hesla jsou bezpečně a přehledně uloženy v programu. Heslo musí být netriviální, lze použít stejné jako máte do systémů IBA.

Mezi nejznámější, zdarma dostupný software této kategorie patří:

KeePass Password Safe – přehledný správce hesel, zdarma i pro komerční použití, existuje i verze pro mobilní telefony. Obsahuje i generátor hesel.

Předávání hesel a citlivých informací

Jak správně předat citlivé informace?

Pokud potřebuji poslat někomu jakékoli citlivé informace, je třeba to provést **bezpečně**. Mezi bezpečné způsoby patří:

- **šifrovaný email** – pokud mám adresátův veřejný klíč a obě strany umějí šifrování použít
- **šifrovaný archiv** – pokud jsem se s adresátem předem dohodl na společném netriviálním hesle, mohu tímto heslem zašifrovat archiv a poslat jako přílohu emailem, nebo přes sdílená úložiště (Ulož.to, Uschovna.cz, FileSender) či cloudové služby
- **Interní OwnCloud a souborové servery –** pro předávání dat uvnitř IBA

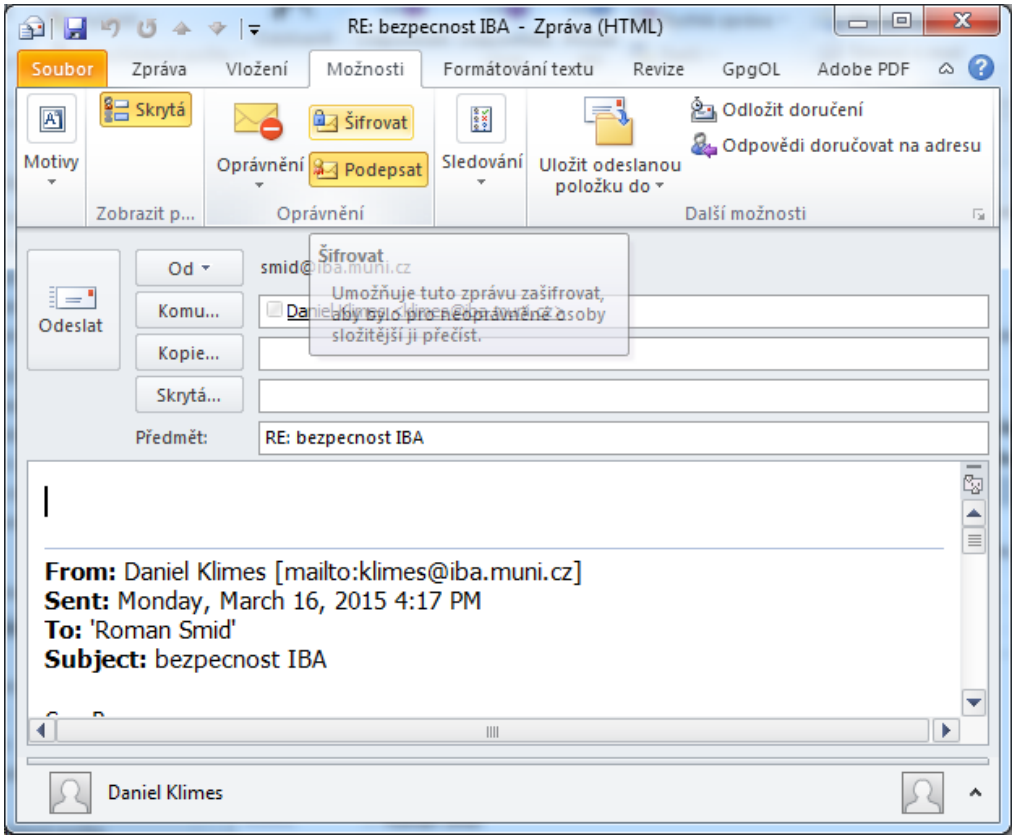
Pokud nemohu zajistit bezpečnost informace při přenosu, raději nepředám informaci vůbec.

Šifrovaný e-mail

Abych mohl někomu poslat šifrovaný e-mail, musím mít jeho veřejný klíč.

Veřejný klíč je ke každému emailu připojen při podepsání dokumentu. Zaměstnanci IBA MU implicitně podepisují všechny e-maily, odesílané z Outlooku, vlastním elektronickým podpisem.

Pokud vám adresát poslal podepsaný e-mail, stačí v odpovědi na email zatrhnout možnost Šifrovat.



Platnost elektronických podpisů na IBA MU je 1 rok, poté je třeba podpis obnovit. Zaměstnanec je povinen ohlásit končící platnost podpisu na IT oddělení.

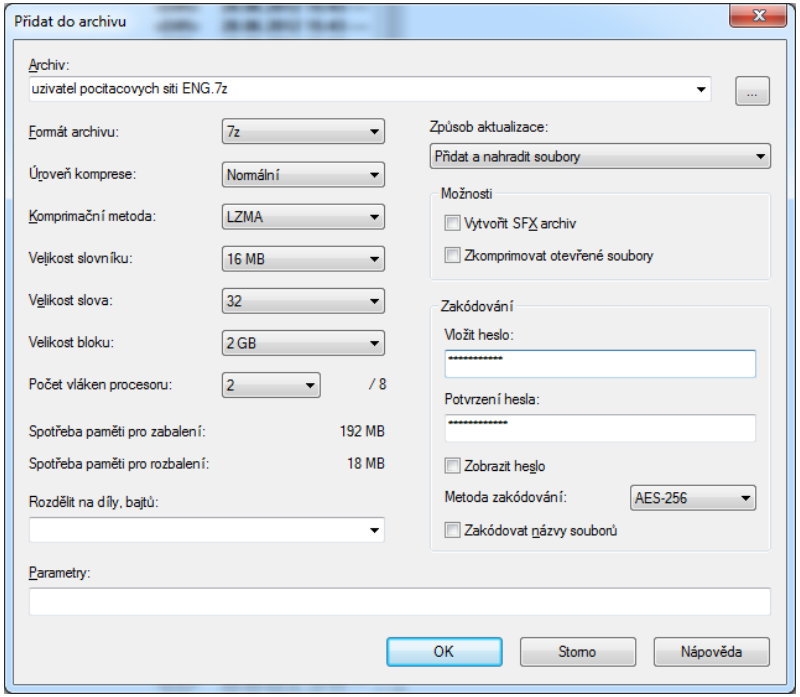
Šifrovaný archiv

Co když nemám adresátův veřejný klíč?

Informace lze poslat nešifrovaným e-mailem jako **šifrovanou přílohu.** Je nutné se předem s adresátem dohodnout (nejlépe osobně) na **netriviálním** hesle, kterým bude příloha zašifrována.

Použijeme zdarma dostupný program 7-Zip (nutno instalovat z :

Na soubor nebo adresář, který chceme poslat, klikneme v průzkumníku pravým tlačítkem a vybereme X64---->7-ZIP---->Přidat do archivu. Zadáme heslo. Ostatní volby necháme jak jsou. Vytvořený archiv s příponou .7z odešleme emailem, adresátovi řekneme, aby k rozbalení použil 7-Zip. Pokud je archiv větší než 8 MB, použijeme služby jako uschovna.cz, uloz.to apod.



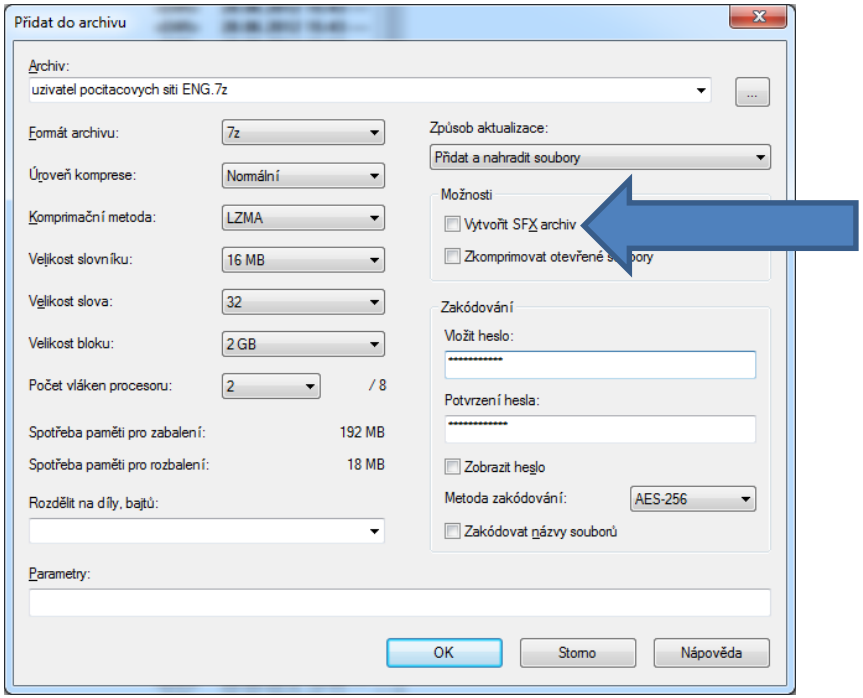
Šifrovaný samorozbalovací archiv

Vhodný pro případy, kdy posíláme soubor někomu méně počítačově zdatnému nebo někomu, kdo nemá 7zip.

Je nutné se předem s adresátem dohodnout (nejlépe osobně) na **netriviálním** hesle, kterým bude příloha zašifrována.

Použijeme zdarma dostupný program 7-Zip (nutno instalovat z :

Na soubor nebo adresář, který chceme poslat, klikneme v průzkumníku pravým tlačítkem a vybereme X64---->7-ZIP---->Přidat do archivu. Zadáme heslo a **zatrhneme Vytvořit SFX archiv**. Ostatní volby necháme jak jsou. Vytvořený archiv s příponou .**exe** odešleme na uloz.to, uschovna.cz apod. a adresátovi pošleme pouze odkaz. **Neposíláme emailem**, soubory s příponou .exe bývají poštovními klienty blokovány.



Šifrování PC a USB disků

Šifrováním disku PC zabráníme nechtěnému vyzrazení dat v případě ztráty nebo odcizení PC.

Ideální je šifrovat celý disk. K šifrování můžeme použít open-source program TrueCrypt (pro Windows 7), nebo v případě Windows 8 Pro vestavěný BitLocker.

Notebooky v majetku IBA a ÚZIS jsou implicitně zašifrovány.

Při šifrování čehokoliv je nutné používat netriviální heslo.

Zákaz svévolného dešifrování NTB.

Pro šifrování USB flash disku se opět skvěle hodí TrueCrypt. Na USB disku lze vytvořit šifrovaný virtuální disk v souboru, do kterého můžeme následně ukládat data. Současně lze na disk nahrát soubory potřebné k otevření šifrovaného disku na kterémkoli počítači. Návod krok za krokem je popsán na http://www.howtogeek.com/61810/how-to-protect-your-flash-drive-data-with-truecrypt/

Pokud máte o nastavení vašeho USB disku zájem, kontaktujte naše IT oddělení.

Přenášení jakýchkoliv dat IBA/ÚZIS na nešifrovaných médiích je zakázáno.

E-mail a viry

- Hrozby:
  - SPAM – nevyžádané zprávy posílané za účelem:
  - Phishing – nevyžádaná zpráva, hromadně rozesílaná za účelem:
    - Vylákání přístupových údajů k různým službám
    - Vylákání soukromých informací
  - Spear Phishing – nevyžádaná zpráva cílená a upravená pro konkrétního uživatele
    - Jde o velmi zákeřný útok, na který se mohou nachytat i zkušení uživatelé
- Pravidla:
  - **Neklikat na odkazy** v neznámých zprávách (nebezpečí podvržení adresy, nasměrování na stránku se škodlivým kódem
  - **Neotvírat přílohy** v neznámých a podezřelých zprávách
  - **Nezobrazovat obrázky a vzdálený obsah v podezřelých zprávách!!**
  - Nikam nezadávat ani **neposílat loginy** a hesla, čísla kreditních karet
  - Všímat si **podezřelých rysů ve zprávách** (strojově přeložený text, **odkazy** vedou jinam než jejich popis, zprávy předstírající že pocházejí od masově používaných služeb a sociálních sítí (Facebook, banky atd…), podezřelá adresa odesílatele
  - Neignorovat případná **varování antivirových programů**
  - Nenechat se **zastrašit** (Pokud nenainstalujete software X.Y., váš počítač bude ohrožen…)

Sociální sítě, IM

- **Facebook** – zneužíván pro šíření spamu, hoaxů, škodlivého kódu
  - **Nebezpečná je důvěra v přátele**: kliknu na cokoli, co postne někdo z mých přátel
  - Obtížná orientace v prostředí, které se často mění – pasti na neznalé uživatele
  - Clickjacking – kombinace sociálního inženýrství a tlačítek To se mi líbí
    - Příklad: Klikněte postupně na všechna tlačítka To se mi líbí pro zobrazení videa apod.
    - Na konci často pouze webová stránka se škodlivým kódem, stránka tahající z lidí peníze nebo zvyšující si uměle návštěvnost
- **Twitter** – šíření adres stránek obsahujících škodlivý kód

Základní pravidlo – neklikat na cokoli, přemýšlet. I počítače vašich přátel mohou být napadeny škodlivým kódem, který na jejich FB profilu posílá zavirované příspěvky…

Neinstalovat neznámé doplňky, např. vyžadované pro přehrání videa apod., často jde o viry.

To samé platí pro Skype a ostatní komunikátory.

Cloudové služby a torrenty

- **Dropbox, Box.net, OneDrive** aj.
- Jsou to služby cizích firem, jejichž používáním souhlasíme s jejich licenčními podmínkami. V podmínkách bývá téměř vždy uvedeno, že **cokoliv tam nahrajete, stává se jejich majetkem** a mohou s tím volně disponovat.
- **Z toho plyne zákaz nahrávání jakýchkoli nešifrovaných dat IBA/ÚZIS do těchto služeb**
- **Ve Windows 10 pozor na OneDrive, vypnout pokud je aktivní**
- Pokud dodržíte bezpečnostní zásady pro šifrování, lze služby použít

- Pro torrenty platí to samé – lze využívat pouze při dodržení bezpečnostních zásad šifrování sdílených souborů
- Instalaci klientů těchto služeb může provádět pouze IT oddělení

Freemail

- **Seznam.cz, Gmail, Email.cz, Volny.cz, Hotmail.com a podobní poskytovatelé**
- Jsou to služby cizích firem, jejichž používáním souhlasíme s jejich licenčními podmínkami. V podmínkách bývá téměř vždy uvedeno, že **cokoliv tam nahrajete, stává se jejich majetkem** a mohou s tím volně disponovat.

- Platí to samé, co pro cloudové služby, **zákaz posílání jakýchkoli nešifrovaných dat IBA/ÚZIS do těchto služeb a na adresy vedené u těchto poskytovatelů, včetně přeposílání vlastní pošty IBA/ÚZIS na tyto adresy.**
- Pokud dodržíte bezpečnostní zásady pro šifrování, lze služby použít (poslat tam někomu něco šifrovaně).

- Výjimka – Protonmail.com – má implementováno end-to-end šifrování, tedy ani nemají přístup k Vašim emailům u nich uložených.

Web

- **Používat intranet**
- Důležité a často používané stránky služeb IBA/ÚZIS nepublikovat na svých vlastních stránkách kdesi v internetu (nevytvářet si svoje vlastní, volně přístupné stránky s odkazy)
- To samé platí pro emaily, telefonní čísla, aliasy…

Notebooky

- Notebooky IBA a ÚZIS nejsou zaměstnaneckým benefitem, slouží výhradně k plnění pracovních povinností. Je zakázáno je používat k jiným účelům.
- **Je zakázáno zejména:**
  - **Dešifrovat notebook nebo měnit heslo**
  - **Půjčovat notebook jiným osobám**
  - **Sdělovat komukoli heslo k notebooku**
  - **Instalovat na notebook jakýkoli neschválený software**
  - **Ukládat na notebook data nesouvisející s pracovními povinnostmi**
  - **Měnit nastavení notebooku, včetně parametrů zamykání obrazovky**
  - **Nechávat notebook s neuzamčenou obrazovkou bez dozoru**
- **Další pravidla najdete v SOP 16 – Provozní řád ICT**
- **Nerespektování těchto pravidel může být bezpečnostním incidentem se všemi důsledky**

Mobilní telefony

- Zařízení často obsahují důvěrná data uživatelů nebo přístupy k různým službám (email, bankovnictví apod.).
- Adekvátně zabezpečena pro případ ztráty zařízení.
- **PIN ani odemčení gestem nestačí!!**
- **šifrování celého zařízení včetně SD karty**. Tuto možnost dnes nabízejí všechny současné mobilní OS.
- Vhodná je i aktivace možnosti **vzdáleného vymazání zařízení** v případě ztráty.
- Zaměstnanci IBA jsou povinni **dodržovat zásady bezpečnosti** dle zavedených ISO norem. Pokud chtějí soukromý mobilní telefon využívat ke čtení pošty IBA nebo jinou práci s citlivými daty IBA, **je nutné šifrování celého zařízení a aktivovaná možnost vzdáleného vymazání zařízení.** Mobilní telefony, které z technologických důvodů šifrování neumožňují, nelze k těmto činnostem využít.

Zálohování

- Data jsou často důležitější než samotný hardware – je důležité **zálohovat**:
  - Vím, co se z mého PC zálohuje, kam a v jakých intervalech?
  - Umím si zkontrolovat, zda zálohování funguje?
  - Umím si zálohovaná data v případě potřeby obnovit?
- **Windows 7 –** vestavěné zálohování je nepohodlné – neumí mazat staré zálohy, nutno dělat ručně. Řešením je použít jiný zálohovací software, např. Cobian Backup
- **Windows 8, 10 –** vestavěné zálohování (Historie souborů) lze nastavit do rozumného automatického režimu
- Problém ve všech verzích Windows zálohování **– neumí zálohovat otevřené soubory.** Tedy například poštu lze zazálohovat pouze pokud je zavřený Outlook. **Řešením je speciální úloha v Cobian Backup.**
- Každý zaměstnanec má na pracovním počítači nastaveno základní zálohování, není tedy zálohováno vše na jeho počítači, ale vybrané složky. V úložišti záloh je pouze omezené místo, proto je třeba **udržovat zálohované složky v počítači v rozumné velikosti** – nedávat tam objemné soubory (instalačky, videa apod…)
- Pokud zálohování hlásí chybu, je zaměstnanec povinen ji nahlásit IT oddělení.

Bezpečnostní incident

- Jakékoliv narušení či podezření z narušení či bezpečnosti
- Ztráta mobilu, notebooku
- Zavirování počítače
- Požáry, záplavy, zatékání vody
- Výpadek elektřiny, sítě
- Porucha hardware
- Nerespektování těchto pravidel
- Může to být i hláška v počítači, které nerozumíte
- **Co dělat:**
- Hlásit (přímému nadřízenému, IT oddělení + HELPDESK)

Dodržování předpisů

- Všichni zaměstnanci jsou povinni znát a dodržovat pravidla stanovená v SOP IBA, zejména SOP 16 – Provozní řád ICT a další dokumenty, včetně této prezentace.
- SOP jsou v rámci IBA pravidelně školeny, zaměstnanec stvrzuje podpisem, že byl proškolen (četl SOP)
- Dodržování pravidel je kontrolováno při auditech, a také namátkově IT oddělením. Při zjištění bezpečnostního incidentu bude situace zdokumentována, založen incident do EP a dotyčnému zaměstnanci může hrozit pracovněprávní postih.