Označení dokumentu:	**ISMS-006**
Název dokumentu:	**Antivirová ochrana počítačů JU**
Typ dokumentu:	Interní dokument- typ B - směrnice
Určeno pro:	Všechny zaměstnance, studenty a účastníky CŽV JU
Prvek normy ISO:	27001
Datum vydání:	29.4.2010
Datum účinnosti:	3.5.2010
Platnost do:	odvolání
Počet stran + příloh:	13 + 3
Verze:	3.0 – aktualizace 07/2019
Účel:	Určuje zásady ochrany počítačů a dat na JU proti napadení parazitními programovými kódy, popisuje funkci antivirového programového vybavení používaného na JU, personální zajištění antivirové ochrany a preventivní kroky proti infiltraci PC
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	verze 2.0 tohoto dokumentu
Zpracovatel:	Ing. Jana Kolářová - MIB, Josef Jann – HS AVO
Přezkoumal:	IT manažeři součástí JU
Schválil:	RNDr. Josef Milota – ředitel CIT a ISMS

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Tato směrnice popisuje pravidla a principy řízení ochrany počítačů a dat na JU proti napadení parazitními programovými kódy, poskytuje výčet nejběžnějších typů malware, vysvětluje činnost antivirového SW provozovaného na JU a popisuje preventivní opatření. Obsahuje též personální zajištění AVO na JU, určuje zásady prevence a definuje pravidla jak postupovat v případě infiltrace PC.

POJMY, DEFINICE A ZKRATKY

1. POJMY A DEFINICE

- **Adware** (advertising-supported software) - je SW produkt znepříjemňující práci s nějakou aplikací vnucenou reklamou. Podrobněji viz odstavec 8.1.
- **Antivirová ochrana (AVO)** – soubor organizačních a softwarových opatření, jehož účelem je ochrana počítačů a počítačové sítě JU před průnikem a šířením parazitních kódů. Bližší informace o běžných typech jsou uvedeny v kapitole 8. této směrnice a další lze nalézt na http://www.viry.cz/.
- **Backdoor** – škodlivý kód, který umožňuje převzít vzdáleně (např. přes Internet) kontrolu nad takto infikovaným PC na principu obcházení běžné autentizace při vstupu do aplikace nebo systému. Dále viz odstavec 8.2.
- **Freeware** – software, který je distribuován bezplatně. Jedná se tedy o volně šiřitelný program, bez placení autorského honoráře. Nedodává se k němu zdrojový kód a je zakázáno jej vnitřně upravovat. To je výhradně v kompetenci autora freeware.
- **Hacker** - počítačový specialista či programátor s detailními znalostmi fungování systému, je schopen ho plně využívat a dokáže si ho také upravit podle svých potřeb.
- **Hoax** – poplašná zpráva, která varuje před neexistujícím nebezpečným virem s výzvou k dalšímu rozesílání - dále viz odstavec 8.4.
- **ID karta** – plastová identifikační karta k ověření identity uživatele, sloužící pro docházkové, přístupové či jiné systémy ke zvýšení bezpečnosti pracovního prostředí. Umožňuje ukládání různých identifikačních údajů uživatele v závislosti na typu karty a účelu jejího použití.
- **Infiltrace PC** – jakýkoli neoprávněný vstup do počítačového systému.
- **Malware** (Malicious software) - souhrnný výraz pro jakýkoliv škodlivý program. Tento pojem zahrnuje počítačové viry, adware, spyware, červy, trojské koně a několik dalších. Seznam nejnovějšího malware lze nalézt např. na http://www.hoax.cz/malware/.
- **Phishing** - viz odstavec 8.5.
- **Ping** (Packet InterNet Groper) – program, který umožňuje prověřit funkčnost spojení přes protokol TCP/IP mezi dvěma síťovými rozhraními (PC, síťová zařízení) v počítačové síti.
- **Plugin** – zásuvný modul – SW třetích stran, který nepracuje samostatně, ale jako doplňkový modul jiné aplikace a rozšiřuje tak její funkčnost.
- **Rootkit** – sada počítačových programů, které maskují přítomnost zákeřných programů na PC skrýváním adresářů, v nichž jsou instalovány – dále viz odstavec 8.6.
- **Spam** – nevyžádané sdělení, obvykle e-mailová zpráva. Více viz odstavec 8.7.
- **Správce počítačů** – zaměstnanec JU pověřený údržbou operačních systémů a dalšího software na osobních počítačích (PC nebo NB) JU. Každá součást má jednoho či více správců počítačů.
- **Spyware** - program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Odcizuje pouze "statistická" data jako např. přehled navštívených stránek či nainstalovaných programů a šíří se často společně s řadou sharewarových programů. Dále viz odstavec 8.8.
- **Trojský kůň** – škodlivý program vydávající se za jiný neškodný SW, více viz odstavec 8.9.
- **USB token** – hardwarové zařízení velikosti flash disku pro bezpečnou autentizaci uživatele. Je určen pro zabezpečení přístupu do počítačových sítí, VPN, intranetu nebo extranetu, pro uložení digitálních certifikátů, pro nasazení v aplikacích e-business, elektronického podpisu a PKI.
- **Uživatel** – je zaměstnanec, student nebo účastník CŽV JU.
- **Virus** - v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele, blíže viz odstavec 8.10.
- **Worm = počítačový červ** - je v informatice specifický počítačový program, který je schopen automaticky rozesílat kopie sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření. Podrobněji viz odstavec 8.3.

2. ZKRATKY

- **ADNM** (avast! Distributed Network Manager) – SW nástroj pro správce AVO k instalaci a konfiguraci AV SW v síti.
- **AMS** (avast! Management Server) – server pro stažení nejnovějších nastavení, s připojenou administrační konzolí, založený na SQL databázi.
- **AV SW** – antivirový software, který chrání počítačový systém proti případnému útoku, odhaluje a odstraňuje počítačové viry infiltrované do počítače. Aby splňoval svoji funkci, musí být antivirový program aktuální a musí být zajištěna pravidelná aktualizace databáze virů.
- **AVO –** antivirová ochrana počítače pomocí AV SW.
- **BS –** bezpečnostní správce součásti JU (funkce popsaná v dokumentu *ISMS-002_Celková bezpečnostní politika JU)*.
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV –** celoživotní vzdělávání.
- **FD** (Floppy Disk) – disketa – přenosné datové médium.
- **HS AVO –** hlavní správce antivirové ochrany na JU.
- **HW** (HardWare) - technické prostředky ICT.
- **ICQ –** internetová aplikace ke komunikační mezi uživateli.
- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IM** (Instant Messaging) – internetová služba umožňující uživateli sledovat, zda jsou dostupní/připojeni konkrétní uživatelé a komunikovat s nimi v reálném čase (např. prostřednictvím Skype, ICQ a dalšími).
- **ISMS** (Information Security Management System) – Systém řízení bezpečnosti informací.
- **IT** – Informační technologie.
- **ITM** – IT manažer, který zajišťuje IT služby na své součásti.
- **JU** – Jihočeská univerzita v Českých Budějovicích.
- **LAN** (Local Access Network) – lokální počítačová síť.
- **LS AVO –** lokální správce antivirové ochrany na každé součásti JU (fakulty, ústavy).
- **MIB –** manažer informační bezpečnosti JU.
- **MP –** metodický pokyn HS AVO.
- **MS (**MicroSoft) - zkratka firmy Microsoft, který obvykle předchází názvu SW produktu.
- **NB** (NoteBook) - přenosný počítač.
- **OS** – operační systém počítače - Windows, Linux, UNIX, Mac, atd.
- **PC** (Personal Computer) – osobní počítač uživatele.
- **PKI** (Public Key Infrastructure) - pokročilá možnost přihlašování se pomocí digitálních certifikátů. Jde o infrastrukturu správy a distribuce veřejných klíčů u asymetrické kryptografie.
- **P2P** (Peer-to-Peer) – jednoduchá architektura sítě klient-klient, kdy si uživatelé mohou přímo vyměňovat data mezi sebou.
- **REK** – Rektorát JU.
- **SQL** (Structured Query Language) – standardizovaný dotazovací jazyk používaný pro práci s daty v relačních databázích.
- **SW** (SoftWare) - programové vybavení počítače.
- **VPN** (Virtual Private Network) – virtuální privátní síť.

ODPOVĚDNOSTI A PRAVOMOCI

- **Hlavní správce AVO JU** (**HS AVO**)

a) definuje a aktualizuje obecně závaznou metodiku antivirové ochrany na JU
b) metodicky řídí činnost lokálních správců AVO na jednotlivých součástech – vydává metodické pokyny pro LS AVO
c) kontroluje dodržování antivirových předpisů na JU
d) odpovídá za aktuálnost prostředků AVO a jejich distribuci správcům AVO na součástech JU
e) udržuje přehled o nových typech parazitních kódů a v případě potřeby o nich informuje LS AVO
f) vybírá antivirové prostředky pro potřeby JU s předchozím ověřením jejich vlastností a účinnosti
g) řídí řešení výjimečných situací AVO
h) vyhodnocuje hlášení o nalezených parazitních kódech

i) komunikuje s dodavatelem AV SW za JU
j) upozorňuje ředitele CIT na potřebu obnovy smlouvy s dodavatelskou firmou AV SW.

- **Lokální správce AVO** - správce IT součásti JU (ITM, BS či jiný zaměstnanec) pověřený zabezpečením AVO počítačů své součásti - vykonává tyto činnosti:

a) kontroluje dodržování předpisů AVO na své součásti
b) řídí se pokyny hlavního správce AVO JU či jeho zástupce
c) odpovídá za distribuci aktuálního antivirového SW uživatelům své součásti
d) instaluje a konfiguruje prostředky AVO podle pokynů HS AVO a podle této směrnice, případně v souladu s platnou metodikou vydanou v rámci své součásti
e) řeší případy výskytu parazitních kódů na svěřených počítačích
f) má povinnost po nápravě infikovaných PC ve své působnosti zkontrolovat správnost jejich nastavení AVO a dle závažnosti parazitního kódu informovat HS AVO
g) archivuje formuláře potvrzující předání licenčního klíče zaměstnancům, studentům či účastníkům CŽV JU pro domácí použití
h) informuje uživatele své součásti o důležitých změnách v antivirové problematice.

- **Uživatel** - zaměstnanec, student nebo účastník CŽV JU, který využívá počítač v majetku JU a jeho programové vybavení nebo se připojuje z domova do sítě JU. Při činnostech na počítači musí dodržovat následující pokyny:

a) dodržuje pravidla vyplývající z této směrnice
b) řídí se pokyny svého lokálního správce AVO nebo HS AVO
c) plně zodpovídá za následky způsobené zavirováním jemu svěřeného PC, pokud bylo prokázáno nedodržení této směrnice nebo jiných zásad AVO na JU
d) nesmí rozesílat či dále šířit žádné zprávy typu hoax
e) v případě podezření na přítomnost parazitního kódu na svém PC bezodkladně kontaktuje LS nebo jeho zástupce, popřípadě HS AVO
f) je-li uživatelem fyzická nebo právnická osoba, která není zaměstnancem, studentem či účastníkem CŽV JU, je povinností zaměstnance JU, který s touto osobou uzavírá smlouvu, zakotvit do této smlouvy smluvní pokutu či jinou obdobnou sankci pro případ porušení povinností uživatele vyplývající z této směrnice.

Další odpovědnosti jsou součástí textu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Toto je třetí verze 3.0 dokumentu.

Ve verzi 2.0 oproti původní verzi 1.0 došlo ke změně kapitoly 1. Antivirový SW na JU.
Důvodem je diverzifikace používaného antivirového SW na jednotlivých univerzitních součástech,
dále plánovaná výměna SW Avast! za SW jiný a další změny, v současné době (únor 2017) ještě ne přesně definovány.

Oproti verzi 2.0 došlo ke změně popisu antivirového SW (nyní SW Bitdefender GravityZone)

B. POPIS

Se zabezpečením PC provozovaných na JU souvisí řada kroků a aktivit, jejichž realizací chceme zabránit nežádoucím změnám, infiltraci PC či dalšímu šíření parazitních kódů v síti JU či mimo ni. Proto je nutné nepodceňovat tuto problematiku, dodržovat dále stanovená pravidla a apelovat na uživatele a jejich rozumné chování při práci s PC. Ti pak v případě potřeby naleznou podporu u správců antivirové ochrany (AVO) na jednotlivých součástech JU, kteří zajistí profesionální instalaci předepsaného AV SW a nastavení jeho automatické aktualizace, které nesmí být změněno.

1. ANTIVIROVÝ SW NA JU

Na základě výběrového řízení na JU byl vybrán (2019) antivirového systém Bitdefender GravityZopne včetně pravidelných upgradů a updatů celého systému a virových databází, dostupných pomocí WWW služby. Kompletní řešení antivirové ochrany podporuje AVO pracovních stanic (OS Windows, Linux), serverů (OS Windows, Linux), virtuálních strojů a mobilních zařízení. Zajišťuje automatické aktualizace virové databáze a poskytuje technickou podporu.

Licence JU na AV SW Bitdefender GravityZone je platná 3 roky, tj. do konce roku 2022. Dojde-li k zásadním změnám u nových aktualizovaných AV produktů, a to i včetně uvažované změně používaného AV software, budou LS AVO informováni od HS AVO formou metodických pokynů, případně dojde k aktualizaci této směrnice, tj. bude vydána její nová verze.

Licence SW Bitdefender GravityZone je určena pro všechny počítače, které jsou ve vlastnictví JU, tedy nikoli pro soukromé domácí PC, NB, mobilní zaměstnanců, studentů a účastníků CŽV JU.

Pokud je používán na některých součástech JU AV SW jiný, např. Microsoft **System Center Endpoint Protection**, je zapotřebí dodržet ekvivalentní zásady. personální zajištění AVO.

2. PERSONÁLNÍ ZAJIŠTĚNÍ AVO

2.1. HLAVNÍ SPRÁVCE AVO (HS AVO)

HS AVO je zaměstnanec JU určený ředitelem CIT, který má pravomoci řídit lokální správce AVO jednotlivých součástí a vydává dle potřeby doplňující metodické pokyny. Jeho odpovědnosti a další pravomoci jsou popsány v oddíle A. Nejedná se o samostatnou pracovní pozici, ale funkci spojenou obvykle se správou počítačů na CIT. Má svého zástupce.

2.2. LOKÁLNÍ SPRÁVCE AVO (LS AVO)

LS AVO je určen IT manažerem nebo vedoucím dané součásti JU pro činnosti spojené s AVO v rozsahu své působnosti. Nejde o samostatnou katalogovou funkci, ale bývá obvykle kumulovaná s dalšími činnostmi v oblasti ICT. Může se jednat o BS, správce PC či sítě nebo samotného ITM. Jeho odpovědnosti a pravomoci jsou popsány v oddíle A. Měl by mít svého zástupce.

Seznam správců AVO na JU je uveden v příloze této směrnice – viz "*ISMS-006-P1_AVO-Správci JU*" a bude dle potřeby aktualizován. Je také interně dostupný všem uživatelům JU po přihlášení na portál ISMS ve složce "*Kontakty*".

3. ŘÍZENÍ ANTIVIROVÉ OCHRANY

Instalaci AV SW "Bitdefender GravityZone" popřípadě "*System Center Endpoint Protection*“ na PC uživatele JU zajišťuje LS AVO dané součásti.

3.1. DOPORUČENÉ NASTAVENÍ KOMPONENT ANTIVIROVÉ OCHRANY NA PC JU

Po instalaci AV SW BitDefender GravityZone jsou nastaveny standardní hodnoty, které zajišťují automatickou aktualizaci virové DB (mění se dle potřeby), rovněž i vlastního AV SW Bitdefender GravityZone a je důležité toto nastavení zachovat, aby nedošlo k infiltraci PC a dalších zařízení. Je-li používán i jiný prověřený AV SW, je nezbytné, aby byla databáze virů rovněž automaticky aktualizována.

Rovněž je doporučeno spustit alespoň jednou týdně kompletní sken test pevných disků počítače.

3.2. OCHRANA E-MAILOVÝCH SLUŽEB

Vzhledem k tomu, že je elektronická pošta potenciálním zdrojem přenosu parazitních kódů a spamů, jež mohou mít za následek zpomalení či dokonce zahlcování univerzitní sítě (nehledě na ztrátu času uživatelů s tím spojenou), přijala JU určitá opatření, která mají tomuto negativnímu fenoménu zabránit a platí pro všechny její součásti.

3.2.1. Princip provozování elektronické pošty na JU

Jednotlivé součásti JU mají vlastní doménová jména třetí úrovně pod doménou jcu.cz. Součásti provozují vlastní e-mailové servery, které zpracovávají elektronickou poštu pro danou součást a danou subdoménu. Zpracování, archivace a přístup uživatelů k elektronické poště je v kompetenci správců e-pošty jednotlivých součástí.

3.2.2. Antispamová služba

JU využívá pro filtrování příchozí elektronické pošty služby externího dodavatele – firmy Excello. Tyto služby zahrnují několikanásobnou filtraci příchozí pošty proti virům a spamům. Záznamy DNS určující cílový server elektronické pošty, ukazují na servery dodavatele, kde dojde k odfiltrování spamu a virů. Následně je pošta doručena na příslušnou součást dle cílové subdomény a seznamu cílových emailových serverů, který znají servery dodavatele. Zprávy, jež nejsou jednoznačně považovány za spam, ale ani za legální e-mail, jsou přesměrovány na příslušnou součást na adresu "karantena@doména_součásti", pro rektorát na karantena@jcu.cz. Ukládání těchto zpráv, archivace a další zpracování je v kompetenci správců ICT jednotlivých součástí. Odchozí pošta vychází z předpokladu existence antivirového SW na PC uživatelů a dodržování předepsaných pravidel a chování uvedených v této směrnici.

3.3. OCHRANA SÍŤOVÉHO PROVOZU

AV SW Bitdefender GravityZone obsahuje řadu modulů s konkrétními funkcemi. Nejdůležitější z nich jsou:

- **Pokročilá ochrana před hrozbami**
- **Kontrola obsahu** .
- **Kontrola zařízení**.
- **Pokročilý uživatel**

4. POSTUP UŽIVATELE PŘI ZAVIROVÁNÍ POČÍTAČE

Máte-li podezření, že se na vašem PC vyskytuje spyware, viry, či jiný nechtěný SW - počítač se "divně chová" a sami si netroufáte závadu detekovat či odstranit, postupujte následovně:

1. Ukončete veškeré programy a počítač ponechte v nečinnosti do doby reakce lokálního správce AVO.
2. Odpojte PC od počítačové sítě vytažením síťového kabelu (ze zásuvky pro počítačovou síť JU).
3. Neprodleně informujte LS AVO Vaší součásti, případně HS AVO a popište mu chování PC. Seznam těchto správců a kontakty na ně naleznete na portále https://isms.jcu.cz/ po přihlášení ve složce „ISMS dokumenty“, a to v příloze této směrnice pod názvem "*ISMS-006-P1_AVO-Správci JU".*
4. Jde-li o PC v univerzitní učebně, ihned informujte lokálního správce AVO součásti JU, jíž učebna patří a nebo správce PC této učebny.

Správce AVO nebo jeho zástupce provede odvirování, zprovozní PC, zkontroluje nastavení AV SW a provede případné preventivní opatření. Jedná-li se o zvláště nebezpečný typ infiltrace, informuje hlavního správce AVO JU.

Nejčastěji se vyskytující typy malware jsou popsány v kapitole 8 této směrnice.

5. PREVENCE UŽIVATELE PROTI PARAZITNÍM KÓDŮM

Aby uživatel PC udržel počítač provozuschopný bez nežádoucího škodlivého či nechtěného SW, který by mohl jakýmkoli způsobem narušit jeho chod či se dokonce šířit dál, musí dodržovat stanovená pravidla bezpečnosti práce na PC JU, jež jsou základní prevencí proti infiltraci počítače či jeho zneužití. Bezpečnostní požadavky na provoz PC, které musí uživatel počítače na JU dodržovat, jsou tyto:

- Na PC s OS Windows mít **nainstalovaný licenční antivirový program pro JU - "Bitdefender GravityZone"** popřípadě **"System Center Endpoint Protection"** a ty nastaveny tak, aby docházelo k **automatické aktualizaci** jak programu, tak databáze – instaluje a konfiguruje lokální správce AVO součásti a uživatel sám toto nastavení nemění.
- Zajistit trvalé **zapnutí brány firewall na PC**, která chrání PC před hackery, a zkontrolovat nastavení automatické aktualizace.
- Neměnit předepsané nastavení **automatické aktualizace OS a jiného základního SW**, případně není-li toto zajištěno, pak tuto aktualizaci nastavit.
- **Používat pouze legální SW** s přidělenou licencí od správce IT dané součásti nebo z webu JU určeného pro uložení legálního SW (viz https://itportal.jcu.cz/login_form, nabídka Licence – nutné přihlášení), případně prověřený freeware potřebný pouze pro pracovní nebo studijní účely.
- Uživatel **nesmí bez souhlasu správce PC instalovat jakýkoliv SW, a to ani freeware**, nepotřebuje-li jej pro výukové, vzdělávací či pracovní účely a nebo pokud mu správce PC neudělil prokazatelně výjimku.
- **Nespouštět na PC bez rozmyslu vše**, co je nabízeno či doporučováno a v případě pochybností se poradit s lokálním správcem AVO.
- Pečlivě **kontrolovat a zvažovat od koho jsou data přijímána** a používat pouze dokumenty z důvěryhodných zdrojů.
- **Neotvírat žádné soubory v příloze e-mailů**, které jsou **neočekávané** nebo s neznámým obsahem.
- **Kontrolovat** AV programem **obsah každého externího média** (CD, DVD, FD, flash disk), které je vloženo do PC uživatele.
- **Při prvním přihlášení na PC či do IS JU**, kde je vyžadována autentizace a není vynucena změna hesla, si **heslo změnit** na své vlastní a nikomu jej nesdělovat. Volit dostatečně silné heslo - na JU je to řetězec min. 8 znaků, který obsahuje kombinaci znaků alfabetických, a to velkých i malých písmen, numerických a speciálních (od každého typu aspoň jeden znak – např. 3Pj5:kup)
- U spouštěných IS či aplikací JU **nepotvrzovat zapamatování hesel** (např. IDM, ODYSEA, STAG, atd**.)**, pokud tuto možnost systém nabízí a **nesdělovat svá hesla nikomu jinému**. Je striktně zakázáno ponechávat u PC heslo někde napsané.
- Nikdy **nerozesílat žádný HOAX**, i když bude uživatel k tomu vyzýván. V případě pochyb si to nejdříve ověřit na http://www.hoax.cz, pokud nejistota trvá, obrátit se na lokálního správce AVO.
- **Nemazat žádné soubory na základě různých varování** obdržených e-mailem, neboť varování před viry je na JU záležitostí správců AVO a pouze ti mohou rozesílat uživatelům pokyny a informace související s AVO. Jejich instrukce je nutno akceptovat a dodržovat!
- **Při restartu neponechávat datové médium v zaváděcí mechanice** (DVD, CD, FD, ZIP, atd.), případně nastavit v PC zavádění operačního systému pouze z pevného disku.
- Je-li na některém PC lokálnímu správci AVO **znemožněn administrátorský přístup**, **odpovídá za stav antivirového programu uživatel tohoto PC**. Změnu tohoto přístupového oprávnění musí prokazatelně povolit HS nebo LS AVO, případně správce PC dané součásti JU.
- **Nenavštěvovat webové stránky s podezřelým obsahem.**
- Nevyžaduje-li to charakter práce, **nesdílet počítač s jinými uživateli.** V opačném případě se **každý uživatel musí přihlásit a pracovat pod vlastním uživatelským účtem** a po skončení relace ukončit všechny aplikace a odhlásit se.
- **Zapojit vlastní rozum a zkušenost** a chovat se obezřetně zvláště při e-mailové komunikaci.
- **Zálohovat vlastní data** na externí médium (CD, flash disk, externí disk či server pro tyto účely vyhrazený) pro případ infiltrace nebo SW či HW havárie PC a možnosti jeho obnovení.
- Bude-li na počítači v síti JU používána **komunikace přes ICQ**, je **zakázáno** touto formou **přijímat soubory**, zvláště jsou-li od neznámých subjektů. Výjimku může schválit pouze HS AVO.
- Vlastník **certifikátu** jej musí mít **umístěn na bezpečném úložišti** (USB token, ID karta) a zodpovídá za jeho utajení.

- Běžně **nepovolovat sdílení** obsahu médií, adresářů či souborů v síti P2P, v případě nutnosti povolit sdílení **jen důvěryhodné osobě**.

Pokud dojde ke ztrátě dat nebo jiným škodám, způsobeným nedodržováním těchto pravidel nebo nerespektováním předepsané konfigurace antivirového programu, bude to posuzováno jako porušení pracovní kázně zaměstnancem, studentem či účastníkem CŽV JU, který je odpovědný za stav antivirového programu na jemu svěřeném počítači JU nebo na vlastním PC či NB, jímž je připojen do sítě JU.

6. AVO SOUKROMÝCH POČÍTAČŮ STUDENTŮ, ZAMĚSTNANCŮ A ÚČASTNÍKŮ CŽV JU

Studenti, zaměstnanci a účastníci CŽV připojující se do počítačové sítě JU ze soukromých počítačů musí mít svůj počítač rovněž chráněn spolehlivým a prověřeným antivirovým softwarem (AV SW), a to buď volně dostupným či placeným. AV SW Bitdefender GravityZone lze použít pouze na počítačích ve vlastnictví JU. Pro soukromé PC mohou uživatelé využít některou z dále uvedených variant.

6.1. AV SW ZDARMA - FREEWARE

- **Platforma Windows - avast! 4 Home Edition / avast! 5 Free Antivirus**
  Tento AV SW je dostupný uživatelům OS Windows na http://www.alwil.com/avast-5-free-antivirus.html nebo www.avast.com. Podmínkou jeho delšího užívání (>30 dní) je bezplatná registrace a použití pro nekomerční účely na dobu jednoho roku. Pak lze legální využití opět prodloužit.
  Program avast! (Home Edition nebo Free Antivirus) je určený pro jednotlivé uživatele a představuje kompletní ochranu proti virům, červům a trojským koním, je spolehlivý a prověřený. Je navržen tak, aby ochránil vlastní data a programy a přitom si zachoval jednoduchost používání. Jeho charakteristickým rysem je jeho snadné ovládání a automatické aktualizace, o kterých je uživatel informován pomocí vyskakovacího okna na základní liště. Ovládání programu zvládne i úplný začátečník.

- **OS Linux**
  Pro PC s operačním systémem **Linux** je nezbytné tento OS pravidelně denně (minimálně však týdně) aktualizovat. Jinak je pro tuto platformu možno použít freeware **avast! 4 Linux Edition** - zdroj na adrese http://www.avast.com/cze/download-avast-for-linux-edition.html nebo **Aegis Virus Scanner** či jiný. Je-li na PC s OS Linux současně nainstalován OS Windows, pod nímž běží AV SW, lze prověřovat data na diskách tímto AV SW.

- **Mac OS X**
  PC s Mac OS X je údajně více odolný proti infiltraci, přesto výrobce doporučuje instalaci AV SW – např. VirusBarrier X5, McAfee VirusScan. Uživatel má též k dispozici AV freeware - např**. PC Tools iAntiVirus,** volně dostupný na http://www.iantivirus.com/, který poskytuje ochranu proti různým druhům infekce a spyware.

6.2. BEZPLATNÁ INTERNETOVÁ SLUŽBA

ESET Online Scanner je bezplatná internetová služba, která dokáže účinně nalézt a odstranit viry, trojské koně a další druhy infiltrací bez potřeby mít nainstalovaný antivirový program. Tato služba ale vyžaduje administrátorská práva uživatele. Více na http://www.eset.cz/cz v záložce „**ESET Online Scanner**“. Služba využívá technologii ThreatSense® a pracuje s nejnovějšími virovými databázemi. Plnohodnotně ovšem nenahrazuje rezidentní AV SW a lze ji využít spíše nárazově.

7. TYPY MALWARE

Uživatel počítače se může setkat s řadou různých typů parazitních kódů a nežádoucího SW. S vývojem IT se způsoby infiltrace zdokonalují a mění. Tato kapitola je určena pro ty, kteří chtějí získat přehled o nejběžnějších typech malware a zjistit, v čem spočívá jejich negativní funkce či jak se projevují. Jsou seřazeny podle abecedy.

7.1. ADWARE

Produkt obvykle šířený pomocí SW, který se tváří jako freeware a přitom má za úkol posílat uživateli na PC cílenou reklamu. Způsobuje automatické stahování, zobrazování nebo přehrávání reklamních a propagačních materiálů v počítači uživatele bez jeho vědomí nebo i za částečné asistence. Příznaky jsou například vyskakující okna, vnucování stránek (nastavení jiné domovské stránky bez vědomí uživatele) apod. Existují i programy, které vstupují do počítače se souhlasem uživatele, protože podmínkou jejich bezplatného používání je právě přítomnost reklamních materiálů.

7.2. BACKDOOR

Jde o aplikace typu klient - server, která umožní autorovi vzdálený přístup na počítač, aniž by proběhla legální autentizace. Na rozdíl od běžných legálních aplikací s podobnou funkcí probíhá její instalace bez vědomí klienta. Na PC se může dostat pomocí Trojského koně nebo jiného SW šířeného viry.

7.3. ČERV (WORM)

Je podtřída počítačového viru, který se obvykle šíří automaticky bez účasti uživatele, přičemž distribuuje své úplné nebo pozměněné kopie v rámci sítí (Internet či LAN) a tím je zahlcuje. Přebírá kontrolu nad funkcemi v počítači, které mohou přenášet soubory nebo informace, zatěžuje paměť PC, a to může vést ke zhroucení počítače. Vysokým nebezpečím červů je jejich schopnost replikace ve velkých objemech. Červ může například rozesílat kopie sebe sama všem členům vašeho e-mailového adresáře, jejichž počítače poté provedou to samé, což způsobí domino efekt nebo rozsáhlý síťový přenos, který může zpomalit pracovní sítě i Internet jako celek. Může s sebou nést i další škodlivý program, který může vykonat rozličné činnosti jako např. instalovat tzv. backdoor. Klasický virus je pasivní a na rozšíření potřebuje kopírování nakaženého souboru. Červ se rozšiřuje aktivně rozesíláním kopií po síti a využívá e-mailovou komunikaci, případně bezpečnostní díry OS. I bez tohoto "nákladu" může červ způsobit velké škody vlivem zahlcení komunikačních kanálů. Díky Internetu je červ schopný se rozšířit po celém světě v průběhu několika hodin.

7.4. HOAX

Falešné varování před neexistujícím virem, mystifikace, podvod, poplašná zpráva, výmysl či žert, které šíří neinformovaní a důvěřiví uživatelé prostřednictvím e-mailů. Hoax přímo neškodí, ale zbytečně zahlcuje síť a připravuje nás o čas. Nepoučený uživatel může na základě jeho doporučení například smazat část operačního systému a tím způsobit jeho nefunkčnost nebo v dobré víře rozeslat své e-mail kontakty apod.

Společným jmenovatelem těchto zpráv je výzva na okamžité postoupení dalšímu uživateli. Tímto způsobem se fáma šíří k dalším uživatelům Internetu. Bližší informace jsou na http://www.hoax.cz.

Není-li si příjemce e-mailu s výše popsaným obsahem jist, zda jde o hoax, měl by se před případným odesláním takové zprávy přesvědčit na zde uvedené adrese, zda nejde skutečně o hoax. Jejich seznam je stále aktualizován. Rozesílání těchto zpráv je na JU zakázáno – viz kapitola 6 této směrnice.

7.5. PHISHING

Druh internetového podvodu zaměřený na získání přístupových údajů uživatelů k účtům elektronického bankovnictví, nebo jiným službám, a jejich zneužití pro obohacení podvodníků.

Obvykle je nic netušícímu uživateli odeslán email s URL adresou a výzvou k aktualizaci potřebných údajů. Na cílové adrese je falešná stránka nějaké webové služby či bankovního ústavu, která vybízí k zadání přihlašovacích údajů, čísla platební karty, apod. V těchto případech je nutné zkontrolovat adresní řádek prohlížeče a URL adresu v něm uvedenou, zda není podezřelá svým obsahem, nebo stránka neobsahuje nějaké nesmyslné informace. Většina provozovatelů internetových služeb a bankovních ústavů tímto způsobem nepostupuje.

7.6. ROOTKIT

Speciální typ infiltrace, která má schopnost skrýt svoji přítomnost v napadnutém systému a tak uniknout detekci. Obvykle jde o balík škodlivého kódu, který umožňuje útočníkovi zneužít zranitelné místa v systému a získat tak plnou kontrolu nad napadeným počítačem. U rootkitu je nejdůležitější prevence, tedy schopnost proaktivně zastavit infiltraci už při pokusu proniknout do systému a dříve, než se stihne aktivovat. Rootkit se dokáže v systému po svojí aktivaci „zneviditelnit“ a napadnutý uživatel tak může získat falešný pocit bezpečí.

7.7. SPAM

Nevyžádané sdělení obvykle masově šířené Internetem, nejvíce využívané k rozesílání nežádoucí reklamy. Nejčastěji se vyskytuje v e-mailové komunikaci, ale můžeme se s ním setkat také ve formě nevyžádaných příspěvků u diskusního fóra nebo při komunikaci s přáteli přes Internet (Instant Messaging).

7.8. SPYWARE

Je souhrnný název pro škodlivé kódy nejrůznějšího účelu, napadající počítače při návštěvě webových stránek nebo při instalaci software pochybného původu. Slouží ke špehování uživatele a jeho činností na počítači. Většinou si uživatel ani neuvědomí, že si program na počítač nainstaluje sám, když dá svolení k doporučené instalaci nějakého SW doplňku, např. přehrávače hudby či videa a tím se spyware dostane na jeho PC, kde může shromažďovat data a později je zaslat autorovi tohoto spyware. Ten pak může získat údaje o zvycích uživatele na internetu, např. jaké stránky často navštěvujete nebo jaký využíváte software, nebo odposlechnout citlivé osobní údaje při přihlašování do webových služeb. Někdy spyware provede též změny v nastavení počítače, způsobuje přesměrování prohlížeče a problémy s internetovým připojením nebo může instalovat a spouštět různé další programy.

7.9. TROJSKÝ KŮŇ

Maskovaná část programu nebo aplikace, která předstírá nějakou užitečnou činnost (např. hra, spořič obrazovky či jiný na první pohled užitečný program) s funkcí, která je ve skutečnosti škodlivá. Obvykle provádí bez vědomí uživatele nějakou destruktivní činnost. Na rozdíl od viru nedokáže sám infikovat další počítače, tj. samovolně se šířit.

7.10. VIRUS

Je počítačový kód, který připojí sám sebe k programu nebo souboru a může se šířit mezi počítači. Při tomto šíření napadá počítače a může poškodit software, hardware i soubory uživatele. Je vyvinut za účelem nějaké destrukční akce na PC. Virus se do PC může dostat především z Internetu. Další možnosti jeho šíření jsou například přenos v rámci lokální sítě nebo kopírování z datového média jako je disketa, CD, DVD apod. Existují *souborové viry*, tedy samostatné škodlivé programy, *boot viry*, které napadají zaváděcí sektor disku a zabezpečí tak svůj start už při spuštění počítače a *makroviry*, které jsou nejčastější součástí dokumentů sady Microsoft Office s příponou .doc (.docx) a .xls (.xlsx). Další dělení závisí na způsobu vykonávání škodlivé činnosti. Zatímco *přímé viry* jsou aktivní v okamžiku spuštění infikovaného objektu, *rezidentní viry* zůstanou v paměti počítače a vykonávají škodlivou činnost.

Další zdroje, které poskytují detailní popis různých parazitních kódů a nežádoucího SW lze nalézt na Internetu. Patří mezi ně např. http://www.viry.cz/, http://www.hoax.cz, http://www.eset.cz/.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice jsou pověřeni lokální správci AVO, hlavní správce AVO a ředitel ISMS. Úmyslné porušení či nedodržení zde uvedených pravidel zaměstnancem, studentem či účastníkem CŽV JU poškozuje dobré jméno a zájmy JU a je považováno za porušení pracovních povinností.

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-006-P1	AVO-Správci JU
ISMS-006-P3	AVO-Metodický pokyn HS-zdroj.

SOUVISEJÍCÍ DOKUMENTY

Označení dokumentu	Název dokumentu
ČSN EN ISO 9001	Systémy managementu jakosti
ČSN ISO/IEC 27001	Systém řízení bezpečnosti informací - ISMS
ČSN ISO/IEC 17799	Soubor postupů pro řízení bezpečnosti informací
ISMS-001	Politika ISMS JU
ISMS-002	Celková bezpečnostní politika JU