ZMLUVA
O ADMINISTRÁCII POČÍTAČOVEJ SIETE

Objednávateľ:

IČO:
DIČ:
Zastúpený:

/ďalej ako užívateľ/

a

Zhotoviteľ: Jozef Tóth – T – SOFT
Sídlo: Peder č. 107, 044 05 Peder
IČO: 41 941 161
DIČ: 1073336484
Zapísaný v Živnostenskom registri OÚ Košice-okolie
č. OŽP-C/2006/00280-2/CR1
č. živnostenského registra 830-11720
Bankové spojenie: VÚB, a.s.
Číslo účtu: 2178 3293 55 / 0200
IBAN: SK42 0200 0000 0021 7832 9355
BIC/SWIFT: SUBASKBX

/ďalej ako administrátor/

Základné pojmy

Informačné systémy (IS) – súhrn technických prostriedkov, programové a aplikačné vybavenie, údajová základňa, pamäťové médiá s údajmi, inštalačné médiá, dokumentácia súvisiaca s technickým a programovým vybavením.

Informačné technológie (IT) – hardvérové a softvérové prostriedky, metódy a spôsoby určené na prenos, spracovanie a uchovanie informácií.

Užívateľský účet – (prihlasovacie meno a heslo) slúži na identifikáciu užívateľa v informačných systémoch a počítačovej sieti, umožňuje správne priradenie pridelených užívateľských práv prihlásenému užívateľovi. S každým jednotlivým užívateľským účtom sú spojené prístupové práva, ktoré rozhodujúcim spôsobom definujú oprávnenie užívateľa pristupovať k zdrojom počítačovej siete.

Cudzia osoba – osoba, ktorá nie je zamestnancom firmy resp. organizácie. (napr. syn, dcéra, kamarát, atď. zamestnanca, klient firmy resp. organizácie, atď.)

Oprávnený užívateľ (resp. len užívateľ) – zamestnanec (a cudzia osoba), ktorému bol zriadený užívateľský účet a pridelené príslušné prístupové práva na vykonanie danej činnosti.

Nepovolaná osoba – zamestnanec (a cudzia osoba), ktorý nemá pridelené prístupové práva na vykonanie danej činnosti alebo operácie.

Sieťové prvky – zariadenia napr. osobný počítač, pracovná stanica, server, lokálna sieť (LAN), aktívny rozbočovač (HUB), prepínač (SWITCH), smerovač (ROUTER), FIREWALL, prístupový bod pre bezdrôtové spojenie (ACCESS POINT) a pod., vrátane príslušného programového vybavenia.

Pracovné dokumenty – všetky súbory, ktoré užívatelia informačného systému vytvorili alebo prevzali pre potreby plnenia pracovných povinností.

Správca siete – osoba, ktorá je v zmluvnom vzťahu a ktorého náplň práce je definovaná v Čl. 9 Práva a povinnosti administrátora, ďalej len „administrátor“.

Čl. 1
Predmet zmluvy

Administrátor sa zaväzuje optimalizovať počítačovú sieť, jednotlivé pracovné stanice a bezpečnosť Internetového pripojenia podľa Čl. 7 Pripojenie počítača do siete, Čl. 10 Postupy zabezpečenia počítača.

Čl. 2
Čas plnenia

Administrátor mesačne alebo podľa potreby užívateľa, okolnosti na diaľku prekontroluje určené počítače, pracovné stanice, servera, routra, NAS. Spraví aktualizácie operačných systémov, Internetového prehliadača, antivírusového systému, servera, OpenWRT routra, NAS zariadenia. Prekontroluje správnu funkčnosť antivírového systému, servera, Internetového prehliadača, OpenWRT routra, NAS zariadenia.

Čl. 3
Cena

Dohodnutá paušálna cena za administráciu počítačovej siete je 50,00 EUR/mesiac. Celková fakturovaná suma sa môže zmeniť na základe nad rámec realizovaných prác.

Čl. 4
Práva a povinnosti užívateľov

1. Používanie hesiel

Každý užívateľ IS a počítačovej siete sa musí identifikovať - musí sa prihlásiť príslušným užívateľským menom a heslom. Autorizácia užívateľa v informačnom systéme môže byť viac úrovňová, pri prihlásení sa do IS a počítačovej siete, pred vstupom do určitej aplikácie, prípadne pred vykonaním určitej činnosti v rámci aplikácie. Na každej úrovni je vhodné používať iné heslo (heslá pre prihlásenie do siete a do konkrétnych aplikácií môžu byť rôzne). Meno užívateľa a prvotné heslo je užívateľovi pridelené administrátorom alebo aplikácie. Heslo je možné zmeniť. Správu hesiel vykonáva administrátor. Heslo musí obsahovať minimálne 6 znakov, kombináciu veľkých a malých písmen, číslic a špeciálnych znakov. (napr.: 89JahodaAQ) Kombinácia znakov tvoriacich heslo nesmie byť jednoducho dešifrovateľná. Je nevhodné používať mená a priezviská užívateľov, ich rodinných príslušníkov, dátumy narodení a pod. **Za utajenie hesla zodpovedá užívateľ.** Heslá nesmú byť voľne dostupné, napr. vedľa počítača, pod klávesnicou, na stole a pod. Každý užívateľ je zodpovedný za neoprávnené sprístupnenie svojho hesla inej osobe, následne i za jeho zneužitie. V prípade straty hesla užívateľ je povinný informovať administrátora počítačovej siete a zabezpečiť výmaz hesla, aby nemohlo dôjsť k jeho zneužitiu inou neoprávnenou osobou. V prípadoch keď je žiaduce zabezpečenie zvýšenej ochrany dát alebo prístup do IS prostredníctvom pracovnej stanice je potrebné používať zaheslovaný šetrič obrazovky.

Kľúčové heslá potrebné na zabezpečenie prevádzky IS a počítačovej siete sú uložené na predpísaných formulároch.

2. Používanie prostriedkov IS a počítačovej siete

Základnými prostriedkami IS a počítačovej siete, ktoré je možné používať pri plnení pracovných povinností sú:

a) pracovná stanica, ktorá bola zamestnancovi pridelená, resp. iný počítač, ktorý je zamestnanec oprávnený používať,
b) nainštalované programové vybavenie,
c) sieťové služby dátových serverov,
d) výpočtová kapacita počítačových systémov pri používaní sieťových aplikácií,
e) elektronická pošta E-mail,
f) pripojenie do globálnej siete Internet.

3. Zásady používania prostriedkov IS a počítačovej siete

a) Užívateľ nesmie svojvoľne meniť konfiguráciu pracovných staníc a počítačov.
b) Užívateľ nesmie počítače odpájať prípadne sám zapájať do počítačovej siete.
c) Užívateľ nesmie k počítačom pripájať ďalšie zariadenia, premiestňovať počítače, ani nijakým iným spôsobom zasahovať do ich hardvérového a softvérového vybavenia.
d) Užívateľ nesmie sám inštalovať akékoľvek programy, nesmie používať a šíriť nelegálne programové vybavenie, nesmie kopírovať a distribuovať nainštalované programy a operačné systémy, ich časti, súvisiacu dokumentáciu a manuály.
e) Všetky zmeny v konfigurácii počítača a ostatného technického vybavenia môžu byť vykonávané len spolu s administrátorom.
f) Pracovné dokumenty sa na pridelenom počítači odporúča ukladať do preddefinovaných priečinkov alebo do pracovného priečinka „Moje dokumenty“, resp. „Dokumenty“. **Každý užívateľ je zodpovedný za zálohovanie vytvorených pracovných dokumentov (má povinnosť ukladať ich na pridelené externé pamäťové médium, resp. do prideleného priečinka na sieťovom disku, na lokálnom disku, atď.).**
g) Užívateľ je povinný vo svojom počítači i na sieti udržiavať poriadok v priečinkoch, rušiť nepotrebné súbory a dokumenty, zbytočne nevytvárať prázdne priečinky, ich chaotické kópie a pod.
h) Užívateľ využíva pridelené výpočtové prostriedky, počítačovú sieť, pridelenú elektronickú adresu (E-mail) a pripojenie do Internetu na plnenie úloh súvisiacich s jeho pracovným zaradením.
i) Každý užívateľ je povinný uposlúchnuť výzvu administrátora na ukončenie práce v počítačovej sieti. V prípade opakovanej výzvy administrátora a jej následného neuposlúchnutia, je administrátor oprávnený ukončiť prihlásenie užívateľa na strane servera. *Poznámka: Administrátor má v prípade havarijného stavu právo na odstavenie prevádzky siete na dobu potrebnú k uvedeniu siete do štandardnej prevádzky aj bez predchádzajúceho upozornenia.*
j) Pri opustení pracovnej stanice (PC) pripojenej na počítačovú sieť je užívateľ povinný sa zo siete odhlásiť alebo zabezpečiť, aby nebolo možné pracovať pod jeho identitou (napr. zaheslovaním šetriča obrazovky).
k) Žiaden užívateľ nesmie zneužiť nedbanlivosť iného užívateľa na to, aby používal PC, IS alebo počítačovú sieť pod cudzou identitou.
l) Užívateľ nesmie vedome a zbytočne rušiť prácu ostatných užívateľov počítačovej siete, obmedzovať jej chod a výkonnosť.

m) Každý oprávnený užívateľ je povinný dodržiavať bezpečnostné opatrenia vyplývajúce z bezpečnostnej politiky, definovanej v „Bezpečnostnom projekte“.
n) Počítače musia byť umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia pracovnej stanice, teplom, vodou, priamym slnečným svetlom a pod.
o) Užívateľ môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp dodávateľa zariadenia.
p) Užívateľ nesmie znižovať životnosť pracovných staníc hrubým zaobchádzaním a ich znečisťovaním.
q) V blízkosti počítačov je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie a podobne).
r) Čistenie povrchu počítačov od prachu je v kompetencii používateľa pracovnej stanice.

4. Používanie elektronickej pošty na plnenie pracovných povinností

Pri používaní elektronickej pošty platia rovnaké pravidlá ako pri obyčajnej pošte (rešpektovanie listového tajomstva). Elektronická pošta má charakter lístkov a pohľadníc, ktoré sa zasielajú bez obalu. Zabezpečenie dôvernosti a utajenia sa realizuje nadstavbovými prostriedkami (napr. zakódovaním správy tak, aby ju mohli dekódovať a prečítať len oprávnení príjemcovia).

Je zakázané:

a) používať elektronickú poštu spôsobom, ktorý je v rozpore s pracovným poriadkom a s platnou legislatívou Slovenskej republiky,
b) obťažovať ostatných užívateľov zasielaním nevyžiadaných informácií, šírením počítačových vírusov, šírením tzv. „reťazových listov“ a poplašných správ (hoax) typu „Dieťa s leukémiou“ alebo „vírus, ktorý nedokáže odhaliť žiaden antivírový program“ a pod., na konci so žiadosťou „pošli to všetkým známym“,
c) zasielanie hromadných nevyžiadaných oznamov (okrem organizačných útvarov ktoré na to majú povolenie),
d) používanie vulgárnych a znevažujúcich výrazov v komunikácii,
e) posielanie a otváranie k elektronickej pošte pripojených súborov, ktoré by mohli nejakým spôsobom ohroziť alebo poškodiť prevádzku IS a počítačovej siete, trvale alebo dočasne znížiť ich výkonnosť alebo ohroziť ich bezpečnosť.

Príjemca elektronickej pošty potvrdí odosielateľovi jej prevzatie vtedy, ak o to odosielateľ v texte správy výslovne žiada.
Používanie špeciálnych zariadení akými sú scanner, CD a DVD napaľovačka, prenosné USB pamäte a pod. je možné iba v súlade s bezpečnostnou politikou.
Užívatelia majú z dôvodu plnenia pracovných povinností zabezpečený prístupu na Internet. Pri vyhľadávaní informácií je zakázané navštevovať pornografické a hackerské stránky, ktoré predstavujú pre Internetový prehliadač hrozbu nielen vírusovú. Zasielanie nevyžiadanej elektronickej pošty - SPAM je v SR zakázané, viď §3 ods. 6 zákona č. 147/2001 Z. z. o reklame a o zmenách a doplnení niektorých zákonov. Pretože sa väčšinou jedná o propagáciu rôznych komerčných firiem a pornografických stránok, je zakázané ju po prevzatí otvárať a klikať na linky v nej uvedené. O tejto skutočnosti je potrebné informovať administrátora.
Každý užívateľ absolvuje zaškolenie a písomne potvrdí, že je oboznámený s pravidlami používania IS a počítačovej siete a, že ich bude dodržiavať.

Čl. 5
Ochrana údajov

(1) Užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva, alebo privilegovaný stav, ktorý mu nebol pridelený administrátorom. Pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť administrátorovi. Užívateľ nesmie vykonávať takú činnosť, ktorá by ostatným užívateľom bránila v riadnom používaní siete, napr. šírenie počítačových vírusov, alebo pokusy o neoprávnený prístup k prvkom IS a počítačovej siete.

(2) Užívateľ sa nesmie pokúšať získať prístup k chráneným informáciám a dátam (resp. dátovej komunikácii) iných užívateľov. Všetky dáta obsiahnuté v zariadeniach siete sú považované za dôverné, pokiaľ nie je explicitne uvedené alebo z ich povahy zrejmé (napr. obsah verejnej web stránky), že sú určené pre všeobecné a neobmedzené použitie.

(3) Užívateľ nesmie napomáhať iným osobám pri získavaní prístupových práv alebo privilegovaných stavov, ktoré im neboli pridelené administrátorom, ani pri získavaní prístupu k chráneným informáciám a dátam iných užívateľov.

(4) Užívateľom je zakázané neodôvodnené sťahovanie a prijímanie súborov (hlavne súbory s príponami: **.EXE, .COM, .SCR, .REG, .CPL, .DLL, .SYS, .VBE, .VBS, .VXD, .BAT**) z Internetu, z príloh časopisov CD a DVD a z iných nedôveryhodných zdrojov akými sú napr. nelegálne kópie FD, CD a DVD a rôzne DEMO, TRIAL, BETA, FREEWARE, SHAREWARE, POSTCARDWARE verzie programov a pod. Výnimka je povolená len od administrátora alebo na základe pracovnej náplne užívateľa.

(5) V prípade úniku alebo podozrenia z úniku informácií z IS a počítačovej siete sú všetci zamestnanci povinní oznámiť túto skutočnosť osobe poverenej výkonom dohľadu nad ochranou osobných údajov.

(6) Prostriedky výpočtovej techniky na ktorých sú údaje z informačnej bázy dát, pamäťové médiá s údajmi a programami (napr. CD, DVD) a výstupné tlačové zostavy, musia byť mechanicky zabezpečené pred prístupom nepovolaných a cudzích osôb (napr. umiestnením v uzamykateľných priestoroch).

(7) Inštalačné médiá (napr. MS-WINDOWS®, MS-OFFICE® a pod.) a médiá so zálohami dát z informačných systémov (CD, DVD) musia byť evidované a uložené v priestoroch, v ktorých budú zabezpečené pred znehodnotením a neoprávneným použitím.

(8) Všetci zamestnanci, ktorí pracujú s osobnými a dôvernými údajmi sú povinní riadiť sa ustanoveniami zákonov č. 18/2018 Z.z. a 540/2001 Z.z. Každý zamestnanec má povinnosť zachovávať mlčanlivosť o osobných a dôverných údajoch o ktorých sa dozvedel pri plnení pracovných povinností a o tých, ktoré v záujme zamestnávateľa nie je možné oznamovať iným osobám. Povinnosť zachovávať mlčanlivosť trvá aj po skončení pracovného pomeru, obdobného pracovného alebo zmluvného vzťahu. Spracovanie osobných a dôverných údajov na počítačoch mimo pracovísk je zakázané.

Čl. 6
Ochrana osobných údajov

Administrátor pri spracúvaní osobných údajov postupuje v súlade so zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi prepismi a rešpektuje príslušné povinnosti určené objednávateľom. Administrátor nesmie spracúvané osobné údaje využiť pre osobnú potrebu, či potrebu inej osoby, ani sprístupniť alebo na iné, než služobné/pracovné účely. Administrátor je povinný zachovať mlčanlivosť o osobných údajoch s ktorými príde do styku.

Čl. 7
Pripojenie počítača do siete

(1) Do siete môže byť zapojený počítač, ktorý je vedený v evidencii majetku firmy resp. organizácie a má pridelené inventárne číslo. Počítače, ktoré nie sú evidované v majetku firmy resp. organizácie (napr. PC cudzích osôb), môžu byť pripojené do siete len so súhlasom administrátora.

(2) Do siete môže počítač pripojiť len administrátor.

(3) Počítače v sieti sú určené nasledovnými identifikačnými údajmi:
   a) IP adresa
   b) MAC adresa
   c) Meno a priezvisko zamestnanca, ktorý zodpovedá za daný počítač
   d) Inventárne číslo (u počítača cudzích osôb súhlas administrátora)

(4) Počítač ktorému chýba niektorý z týchto 4 atribútov, nemôže byť zapojený v sieti.

Čl. 8
Súvisiace predpisy

Zákon č. 18/2018 Z.z. o ochrane osobných údajov (GDPR)
platnosť: 30.01.2018, účinnosť: 25.05.2018, zdroj: Zbierky zákonov

Zákon č. 540/2001 Z.z. o štátnej štatistike,
platnosť: 20.12.2001, účinnosť: 01.01.2002, zdroj: Zbierky zákonov.

Zákon č. 185/2015 Z.z. Autorský zákon,
platnosť: 05.08.2015, účinnosť: 01.01.2016, zdroj: Zbierky zákonov.

Zákon č. 300/2005 Z.z. Trestný zákon,
platnosť: 02.07.2005, účinnosť: 01.01.2006, zdroj: Zbierky zákonov

Čl. 9
Práva a povinnosti administrátora

Správa počítačovej siete sa stáva v dobe prudkého rozvoja Internetu zložitejšou a náročnejšou úlohou, než bola kedykoľvek predtým. Administrátor má na základe svojej kvalifikácie predpoklady na výkon tejto funkcie. (príloha č. 5)

(1) Administrátor zodpovedá za prevádzku siete, jej technický rozvoj, dátovú bezpečnosť a dodržiavanie pravidiel pripojenia do siete.
(2) Administrátor je prvým konzultantom pre všetkých zamestnancov v oblasti funkčnosti siete a pri následnom riešení poruchových stavov.
(3) Administrátor je kontaktnou osobou pri riešení problémov komunikácie v sieti.
(4) Administrátor zodpovedá za:
    a) technickú a systémovú správu lokálnej siete na určených počítačoch pripojených do LAN,
    b) správne nastavenie komunikačných parametrov počítačov pripojených na LAN,
    c) dodržiavanie podmienok pripojenia podľa **Čl. 7 Pripojenie počítača do siete**,
    d) okamžité odpojenie od počítačovej siete takého počítača, ktorý porušuje pravidlá pripojenia, alebo správania sa v sieti,
    e) prešetrenie príčin porušovania pravidiel a ich odstránenie.
(5) Administrátor nezodpovedá:
    a) za užívateľov ktorí nerešpektujú, ignorujú **Čl. 4 Práva a povinnosti užívateľov, Čl. 5 Ochrana údajov, Čl. 7 Pripojenie počítača do siete, Čl. 8 Súvisiace predpisy, Čl. 9 Práva a povinnosti administrátora**
    b) za porušenie zákona č. 185/2015 Z.z. Autorský zákon
    c) za pharming a nefunkčnosť vonkajších DNS serverov,
    d) za legálne a nelegálne programy používané vo firme, resp. v organizácie,
    e) za funkčnosť alebo nefunkčnosť softvérov používaných vo firme, resp. v organizácie,
    f) za audit softvérov,
    g) za archiváciu údajov,
    h) za nefunkčnosť Internetu pôsobené poskytovateľom (ISP),
    i) za nefunkčnosť vonkajších elektronických služieb ako napr.: webové stránky, E-mail, Internet banking, atď.
    j) za router, switch, firewall, kábeláž ktorý už bol nainštalovaný pred administráciou siete a administrátor nemá k tomu prístup,
    k) za nesprávnu konfiguráciu routera, firewalla, proxy servera ktorý už bol nainštalovaný pred administráciou siete a administrátor nemá k tomu prístup.
(6) Pri mimoriadne vážnych ohrozeniach siete môže odpojiť z komunikácie celú sieť, resp. jeho časť na nevyhnutne potrebnú dobu.
(7) Správca siete prideľuje IP adresy z rozsahu, ktorý má k dispozícii a vedie evidenciu, vrátane mena zodpovedného zamestnanca, udržuje ich v aktuálnom stave.
(8) Sleduje stav siete a podľa potreby informuje jej užívateľov. Pozná a používa monitorovacie a diagnostické techniky.
(9) Vykonáva analýzu bezpečnostných incidentov zo systému firewallu, antivíru a pod.
(10) Užívateľom siete poskytuje poradenské služby a navrhuje potrebu absolvovania školení na rozvoj zručností, ktoré by zvyšovali kvalifikáciu užívateľov siete, čím napomáha optimalizovať jej prevádzku a správu.
(11) Vedie dokumentáciu o počítačovej sieti a navrhuje potrebu jej inovácie.

Čl. 10
Postupy zabezpečenia počítača

(1) Zaplombovanie krytu počítača resp. pracovnej stanice.

(2) Nastaviť heslo pre prístup do BIOSu.

(3) Nastaviť štartovanie počítača iba z pevného disku. Nastaviť prvotný HDD-0 ako boot. Zrušiť prvotný boot z FD/CD/DVD/LAN/USB.

(4) Zapísať štandardný BOOT LOADER na HDD-0. (mazanie možného BOOT vírusa)

(5) Nastaviť v BIOSe ochranu MBR proti prepísaniu. (ochrana proti BOOT vírusu)

(6) Pri použití operačného systému Windows® NT/2000/XP/Vista/Win7/Win8.x/Win10 použiť súborový systém NTFS. Na pevných diskoch pod kapacitou 2TB používať MBR partíciu namiesto GPT partície.

(7) Vytvorenie administrátorského konta, vytvorenie užívateľských kont.

(8) Zapnúť integrovaný firewall v operačnom systéme, povoliť odpoveď ICMP [0]Echo Reply na žiadosti ICMP [8]Echo Request.

(9) Len na žiadosť užívateľa Internetový prístup riešiť podľa prílohy č. 4. V tomto prípade pre jednotlivé programy ktoré potrebujú Internetové pripojenie nastaviť prístup cez proxy server s overovaním, pre Internetový prístup nepoužívať gateway, nevyplniť predvolenú bránu na jednotlivých pracovných staniciach, iba na centrálnom počítači. (podľa prílohy č. 4).

(10) Vypnúť sieťovú službu počúvajúcu na porte TCP135 – vzdialené volanie procedúr.

(11) Vypnúť sieťovú službu počúvajúcu na porte TCP5000 – Universal Plug and Play.

(12) Vypnúť službu vzdialená pracovná plocha, vzdialená pomoc, vzdialený register.

(13) Vypnúť kuriérsku službu messenger.

(14) Vypnúť službu zdieľanie súborov a tlačiarní, ak nie je využitá. V prípade potreby povoliť iba pre daný počítač s filtrovaním cez integrovaný firewall pre lokálnu sieť.

(15) Vypnúť Full Raw Sockets. Platí pre operačné systémy Windows® NT/2000/XP.

(16) Vypnutie zbytočných procesov pri spustení operačného systému. (napr. extra ovládače grafických a zvukových kariet, monitorovacie softvéry iných aplikácií, atď.)

(17) Inštalovanie antivírového systému schopnosťou HTTP, SMTP, POP3 kontroly.

(18) Nastaviť antivírový systém tak, aby skontroloval BOOT sektory, všetky (*.*) súbory pri otváraní, vytváraní, spúšťaní. Nastaviť heuristickú analýzu. Nastaviť HTTP, SMTP, POP3 kontrolu. Nastaviť automatické aktualizácie antivírového systému.

(19) Z bezpečnostných dôvodov je odporúčané používať nasledovné softvéry: Internetový prehliadač - Mozilla® Firefox®, E-mailový klient - Mozilla® Thunderbird®, Proxy server - FreeProxy®.

Čl. 11
Záverečné ustanovenia

(1) Všetci užívatelia IS a počítačovej siete sú povinní dodržiavať túto zmluvu, ustanovenia súvisiacich právnych noriem a ďalšie pravidlá, pokyny a platné predpisy.

(2) Táto zmluva je záväzná pre všetkých užívateľov IS a počítačovej siete.

(3) Administrátor pri spracúvaní osobných údajov postupuje v súlade so zákonom o ochrane osobných údajov, inými zákonmi, všeobecne záväznými právnymi prepismi a rešpektuje príslušné povinnosti určené objednávateľom. Administrátor nesmie spracúvané osobné údaje využiť pre osobnú potrebu, či potrebu inej osoby, ani sprístupniť alebo na iné, než služobné/pracovné účely. Administrátor je povinný zachovať mlčanlivosť o osobných údajoch s ktorými príde do styku.

(4) Zmluva sa uzatvára na dobu neurčitú. Platnosť a účinnosť nadobúda dňom podpisu obidvoma zmluvnými stranami.

(5) Platnosť a účinnosť tejto zmluvy zaniká dňom ukončenia zmluvy. Povinnosť mlčanlivosti trvá aj po ukončení platnosti a účinnosti tejto zmluvy.

(6) Zmluvné strany sa dohodli, že text tejto zmluvy bude utajené pred tretími stranami a predstavuje dôverné informácie.

(7) Zmeny a dodatky tejto zmluvy vyžadujú písomnú formu.

(8) Neoddeliteľnou súčasťou tejto zmluvy sú:
- príloha č. 1 – Vymedzenie niektorých odborných pojmov (5 strán)
- príloha č. 2 – Ako funguje predvolene nastavený FIREWALL? (1 strana)
- príloha č. 3 – Menej bezpečné riešenie Internetového prístupu (1 strana)
- príloha č. 4 – Bezpečnejšie riešenie Internetového prístupu (1 strana)
- príloha č. 5 – Osvedčenie: Jozef Tóth – správca počítačových systémov – kópia (1 strana, podpisy boli odstránené z osvedčenia)
- príloha č. 6 – Osvedčenie: Jozef Tóth – Zákon o ochrane osobných údajov – kópia (1 strana, podpis lektora bol odstránený z osvedčenia)

(9) Strany prehlasujú, že túto zmluvu prečítali a zhodne porozumeli jej obsahu, ktorý zodpovedá ich skutočnej, vážnej a slobodnej vôli, na dôkaz čoho pripájajú svoje podpisy.

(10) Táto zmluva je vyhotovená v 2 exemplároch, z ktorých každá má platnosť originálu.

(11) Táto zmluva obsahuje 20 strán spolu s prílohami.

V Pederi, dňa:

_____	_____
Objednávateľ	Zhotoviteľ

príloha č. 1

Vymedzenie niektorých odborných pojmov

(podľa logického postupu)

HARDWARE
Hardvér. Technické prostriedky počítača. Napr.: monitor, tlačiareň, zvuková karta, grafická karta, pevný disk – **HDD**, atď.

SOFTWARE
Softvér. Programové vybavenie počítača. Napr.: operačný systém, program pre účtovníctvo, antivírusový program, osobný **firewall**, počítačové hry, atď.

ASCII
American Standard Code for Information Interchange. Americký normalizovaný kód na výmenu informácií. Predpis, podľa ktorého je k znakom abecedy, číslicam a ďalším typografickým znakom priraďovaný určený numerický kód (napr. A=65). ASCII kódovanie nepovažuje sa za kryptovanie.

BOOT
Štart zariadenia. Počiatočné zavedenie programového vybavenia. (napr. z boot sektora FD, CD, DVD, HDD)

MBR
Master Boot Record. Hlavný štartovací záznam. Obsahuje rozmiestnenie partícií a úvodnú časť programu. (**BOOT LOADER**)

BOOT LOADER
Úlohou boot loadera je spustenie operačného systému. Boot vírusy práve ten boot loader zvykli prepísať.

PC
Personal Computer. Osobný počítač, pracovná stanica.

LAN
Local - Area Network. Lokálna počítačová sieť, sieť fyzicky rozložená na pomerne malom území, väčšinou v rámci organizácie (napr. v jednej budove) spájajúca osobné počítače.

IP ADRESA
Fyzická adresa počítača v sieti, pomocou ktorej sa počítače dokážu "nájsť". Jej analógiou z reálneho sveta je poštová adresa. IP adresa je číselný kód, jednoznačne identifikujúci počítač v počítačovej sieti **LAN**. Napr.: 192.168.0.1

MAC ADRESA
Fyzická adresa. Hardwarová adresa, unikátne číslo, ktoré nesie sieťová karta od výrobcu. Býva dvanásť miestna a skladá sa z číslic a písmen. Napr.: 00-10-A7-2A-AF-3D

BROWSER
Prehliadač. Internetový prehliadač. Počítačový program, ktorý zobrazí textovú a grafickú informáciu v jazyku **HTML** na obrazovke počítača v čitateľnej podobe. Najrozšírenejšími prehliadačmi sú Internet Explorer® (súčasť operačného systému Windows®), Netscape Navigator®, Opera®, Mozilla®Firefox®.

KLIENT
Počítač, zariadenie alebo iná entita, ktorá využíva prostriedky siete, servera alebo iných zariadení. Súčasť **klient/server** architektúry.

SERVER
Počítač, zariadenie alebo iná entita, ktorá poskytuje služby ostatným počítačom alebo zariadeniam, ktoré tieto služby (ak sú na to oprávnené) využívajú. Súčasť **klient/server** architektúry. (napr. súborový server, tlačový server, aplikačný server, databázový server, poštový server, **WWW** server, Mail server, **Proxy server**, **DNS** server, atď.)

KLIENT / SERVER
Komunikačná štruktúra prepojená napríklad sieťou, kde počítače alebo iné zariadenia (servery) poskytujú služby iným počítačom alebo zariadeniam (klienti), ktoré tieto služby využívajú.

PROXY SERVER
Zástupca. Niekedy sa objaví požiadavka (z bezpečnostných dôvodov), aby počítače - hlavne programy, celý operačný systém - nemali priamy prístup na Internet. Na tento účel napr. hardwarový **firewall** nestačí. Firewall sa totiž pozerá len na hlavičky a typ **paket**ov a podľa toho ich rozdeľuje. V prípade, že je nutné, aby komunikácia bola filtrovaná na základe **URL**, ktorú používateľ zadal do svojho web prehliadača (**browser**a), je nutné nasadiť **proxy server**. Na proxy serveroch dá sa aj nastaviť overenie užívateľa. (Typicky používaný **TCP** port: 8080)

TCP
Transmission Controll Protocol. Protokol na riadenie prenosu. Spojovo orientovaný protokol. Kvalitný pomalý prenos údajov. (napr. elektronická pošta, Web, atď.)

UDP
User Datagram Protocol. Používateľský datagramový protokol. Nespojovo orientovaný protokol. Nekvalitný rýchly prenos údajov. (napr. DNS preklad, prenos zvuku / videa, atď.)

Port
Port / brána. Prístupový bod pre jednotlivé štandardné/neštandardné elektronické služby. Napr.: nezabezpečená elektronická pošta používa porty: TCP25, TCP110; Web servery: TCP80, TCP443; FTP servery: TCP20, TCP21; DNS servery: UDP53; Proxy servery: TCP8080; ICQ® server (America-Online): TCP5190; Kerio® personal firewall: TCP,UDP44334.
Pre vstup do systému Windows®XP® (najnebezpečnejšie otvorené porty): vzdialené volanie procedúr (**RPC**): TCP135; Universal Plug & Play (**UPnP**): UDP1900, TCP5000; Windows® file sharing - zdieľanie súborov a tlačiarní (**NetBIOS**): UDP137, 138, TCP139, 445; isakmp LSASS: UDP500; network blackjack DCOM: TCP1024–1030. Keď firewall je vypnutý, operačný systém Windows®XP® je oveľa zraniteľnejší. Možnosťou je aj vypnutie nepotrebných nebezpečných služieb.

Universal Plug and Play (UPnP)
Vo Windows®XP® hľadá nové zariadenia pripojené na vzdialený PC v sieti. Môže byť potrebný, ak sa používa Internet Connection Sharing (zdieľanie Internetu). Povoľuje iným modifikovať možnosti pripojenia. (Používané porty: UDP1900; TCP5000)

Remote Procedure Call (RPC)
Vzdialené volanie procedúr. Windows® aplikácie všeobecne bežia ako separátne procesy. Ak napríklad nastane problém s jednou aplikáciou, spravidla to nemá vplyv na iné aplikácie. Komunikáciu medzi službami a procesmi zabezpečuje RPC. Ako sieťová služba je nebezpečná. (Používaný port: TCP135)

DNS

Domain Naming System. Systém doménových mien sa používa na preklad mien počítačov na ich fyzické adresy (tieto sú pre človeka ťažko zapamätateľné). Napríklad www.priklad.sk sa preloží na IP adresu 192.168.1.10. (Používaný UDP port: 53)

FTP

File Transfer Protokol. Protokol transferu súborov. Protokol na prenos súborov sa používa na kopírovanie a na inú manipuláciu so súbormi uloženými na serveri. (TCP/IP, **RFC** 959) (Používané TCP porty: 20, 21)

RFC

Request For Comments. Množina štandardov v sieti Internet.

HTML

HyperText Markup Language. Hypertextový značkovací jazyk. Používaný na vytváranie webových stránok.

HTTP

HyperText Transfer Protocol. Komunikačný protokol zabezpečujúci prístup na web servery a prenos HTML stránok. Nezabezpečený protokol. Používa ASCII kódovanie. (Používaný TCP port: 80)

HTTPS

HTTP Secure. Zabezpečený HTTP protokol. (napr. zabezpečený webový server pre Internet banking) (Používaný TCP port: 443)

IRC

Internet Relay Chat. Konferenčný systém. Protokol Internetových rozhovorov umožňuje vzájomnú komunikáciu medzi viacerými používateľmi.

JAVASCRIPT

Skriptovací jazyk založený na jazyku Java, ktorý je zabudovaný do všetkých moderných webových prehliadačov. Umožňuje tvorcom web stránky pridať jednoduchú logiku (kontrola zadaných údajov, jednoduché výpočty).

LINUX

Opensource (pozri definíciu **OPENSOURCE**) Free (bezplatný, pozri definíciu **FREEWARE**) operačný systém používaný prevažne na serveroch, ktoré vyžadujú vysokú stabilitu, výkon a dostupnosť. Skladá sa z jadra (kernel) a základných utilít. V súčasnosti je rovnako dobre použiteľný pre prácu na bežných počítačoch.

OPENSOURCE

Softvér, ktorý je dodávaný spolu so zdrojovým kódom. Nahliadnutie do zdrojových kódov umožňuje širokej odbornej verejnosti odhaliť chyby alebo priniesť vylepšenia.

ROUTER / GATEWAY

Smerovač. Zariadenie (fyzické alebo počítač), ktoré smeruje sieťovú prevádzku na základe informácií o jej vzniku alebo cieli. Veľké siete (napríklad aj Internet) je prepojený množstvom týchto zariadení.

PACKET

Paket. Komunikačná jednotka v sieti.

SWITCH

Prepínač / ústredňa, viacportový most. Prepínač je zariadenie, ktoré na krátku vzdialenosť prepája skupinu počítačov v rámci jednej podsiete. Môže byť pripojený s ďalšími prepínačmi, rozbočovačmi alebo s routrom (pozri definíciu **ROUTER**).

HUB

Rozbočovač, viacportový opakovač. HUB je zariadenie, ktoré na krátku vzdialenosť prepája skupinu počítačov v rámci jednej podsiete. Môže byť pripojený s ďalšími rozbočovačmi, prepínačmi alebo s routrom.

XHTML

Extended HyperText Markup Language. Rozšírená verzia jazyka HTML (pozri definíciu **HTML**).

XML

Extended Markup Language. Dnes de facto štandardným formátom pre ukladanie a výmenu informácií medzi aplikáciami.

404 (ERROR - RESOURCE NOT FOUND)

Štandardná chybová správa, ktorú odošle webový server užívateľovi, keď tento požiada o stránku alebo iný zdroj, ktorý na serveri neexistuje.

404 (ERROR - RESOURCE NOT FOUND) ERROR PAGE

Štandardná chybová správa, ktorú odošle webový server užívateľovi, keď tento požiada o stránku alebo iný zdroj, ktorý na serveri neexistuje je nahradená špeciálnou stránkou, ktorú vytvorí administrátor.

SSL

Secure Sockets Layer. Protokol zabezpečenej komunikácie. Protokol umožňujúci bezpečnú komunikáciu v prostredí počítačových sietí. Umožňuje taktiež identifikáciu komunikujúcich strán.

SPAM

Nevyžiadaná elektronická pošta. Masové rozosielanie nevyžiadaných E-mailových správ - UCE (pozri definíciu **UCE**).

FLASH

Multimediálny prezentačný systém pridávajúci webovým stránkam interaktivitu a funkcionalitu. Obsahuje programovací jazyk, pomocou ktorého sa dajú vytvárať prezentácie alebo hry.

UCE

Unsolicited Commercial E-mail. Nevyžiadaný obchodný E-mail. E-mail s obchodnou ponukou produktov alebo služieb, na odoslanie ktorého odosielateľ nedostal od príjemcu povolenie. Podľa zákona je takéto šírenie E-mailov protiprávne.

UPS

Uninterruptible Power Supply. Zdroj neprerušiteľného napájania.

Demilitarizovaná zóna (DMZ)

Demilitarizovaná zóna sa realizuje prostredníctvom firewallu, ktorý má tri sieťové karty: jednu pre Internet, druhú pre vnútornú sieť a tretiu pre demilitarizovanú zónu, ktorá obsahuje aplikačné služby prístupné zvnútra aj zvonku siete. V prípade potreby vyššieho stupňa bezpečnosti je nutné fyzicky oddeliť siete na ktorých sa nachádza proxy server a pracovné stanice koncových užívateľov. Spojenie s Internetom je filtrované jedným alebo dvoma firewallmi a aplikačnou bránou (proxy serverom).

FIREWALL
Bezpečnostný sieťový prvok poskytujúci ochranu privátnych sietí. Protipožiarna stena kombinácia bezpečnostného hardvéru a softvéru, vytvárajúceho ochrannú vrstvu (stenu) medzi vnútornou počítačovou sieťou organizácie - intranetom a verejnou sieťou - Internetom. Kontroluje prístup do/z siete a je navrhnutý aj ako ochrana proti vírusom z vonkajších sietí.

HDD
Hard Disk Drive. Pevný disk, počítačové zariadenie na ukladanie dát pracujúce na magnetickom princípe, umožňujúce rýchle zapisovanie a čítanie.

FDD
Floppy Disk Drive. Disketová mechanika, počítačové zariadenie na ukladanie dát pracujúce na magnetickom princípe, umožňujúce zapisovanie a čítanie.

FD
Floppy Disk. Disketa. Kapacita 1,44 MB.

CD
Compact Disk. Kapacita 700 MB.

DVD
Digital Versatile Disk. Veľkokapacitný disk. Kapacita 4.7 GB.

PROTOKOL
Pravidlo určujúce formát a prenos údajov. (Napr. TCP/IP protokol)

Net, Network
Počítačová sieť.

NET
Network Enity Title. Označenie sieťovej entity (CLNS).

CLNS
Connectionless Network Service. Sieťová služba bez spojenia.

BIOS
Basic Input/Output System. Elektrický obvod (integrovaný obvod). V BIOSe sa nachádza základný softvér, ktorý umožňuje najzákladnejšiu komunikáciu s hardvérom. Zároveň uchováva informáciu o konfigurácii systému. Prístup k BIOSu sa dá obmedziť zaheslovaním.

NetBIOS
Network Basic Input/Output System. Sieťový základný vstupný/výstupný systém (IBM). (Používané porty: UDP-137, UDP-138, TCP-139, vo Windows NT/2000/XP/2003 TCP-445)

Internet
Názov globálnej intersiete. Počítačová sieť pozostávajúca z celosvetovej siete počítačových sietí používajúcich sadu TCP/IP sieťových protokolov zabezpečujúcich odosielanie a výmenu dát.

internet
Intersieť. Prepojenie sieťových segmentov.

intranet
Vnútropodniková sieť.

ISP
Internet Service Provider. Poskytovateľ pripojenia do Internetu.

PROVIDER
Poskytovateľ. Pozri definíciu **ISP.**

POP3
Post Office Protocol version 3. Nezabezpečený protokol. Protokol pre prístup užívateľov k E-mail správam uloženým na mail serveri. (Používaný TCP port: 110)

SMTP
Simple Mail Transfer Protocol. Jednoduchý protokol transferu pošty. Nezabezpečený protokol. Je normou pre prenos pošty v Internete. (Používaný TCP port: 25)

TCP/IP
Transmission Control Protocol / Internet protocol. Protokol na riadenie prenosu / medzisieťový protokol. Počítačový komunikačný protokol, základný protokol na komunikáciu v sieti Internet, LAN, WAN, intranet atď.

URL
Uniform Resource Locator. Univerzálny lokátor zdrojov. Adresa určujúca umiestnenie WEB stránky (Internetová adresa) na WWW.

UTP
Unshielded Twisted Pair. Metalické vedenie (netienený skrúcaný pár, krútená dvojlinka) používané na vytváranie počítačových sietí typu Ethernet.

WWW
World Wide Web, alebo len Web. Počítačová sieť pozostávajúca zo súboru Internetových sídiel a ponúkajúca textové, grafické, zvukové a animované informácie prostredníctvom HTTP.

DEMO
Demo je software uvoľnený do užívania zadarmo, niektoré funkcie programu sú obmedzené (umelo znefunkčnené). Väčšinou sa jedná o hry, alebo rôzne aplikácie. V podstate je to druh reklamy, ktorá umožňuje užívateľovi zoznámiť sa so základnou funkciou programu a rozhodnúť sa, či si ostrú verziu programu kúpi. Pozor! Malware (pozri definíciu **MALWARE**) programy môžu sa šíriť ako DEMO!

FREEWARE
Tento software je šírený zadarmo, je možné ho získať napríklad stiahnutím z Internetu, alebo z rôznych CD, predávaných s časopismi. Program je možné používať zadarmo po neobmedzenú dobu, je možné ho šíriť ďalej. Nie je ale dovolené, podobne ako u shareware ho šíriť za úplatu, teda s cieľom zisku. Z definície freeware tiež plynie, že autorské práva prináležia autorovi, nie je dovolené bez

súhlasu autora meniť programový kód produktu, alebo ho upravovať pre komerčné účely. Pozor! Malware programy môžu sa šíriť ako FREEWARE!

POSTCARDWARE

Postcardware je podobný ako freeware, v skutočnosti je to freeware. Za užívanie programu ako poďakovanie, či uznanie je možné zaslať autorovi pohľadnicu. Pečiatka na pohľadnici je spätnou kontrolou (informáciou), kde všade na svete sa používa jeho produkt. Pozor! Malware programy môžu sa šíriť ako POSTCARDWARE!

SHAREWARE

Tento produkt je tiež šírený zadarmo napríklad cestou Internetu, alebo na rôznych CD. Taký program je možné používať po určitú dobu, ktorú stanoví autor. Býva to obvykle 3-4 týždne, alebo presne stanovený počet spustení programu. Po uplynutí stanoveného času (počtu spustení), celý program prestane fungovať, alebo aspoň jeho kľúčové funkcie. Pre ďalšie použitie je potrebné zaplatiť nejakú, väčšinou symbolickú cenu, za ktorú užívateľ obdrží aktivačný kľúč, alebo heslo. Zadaním tohto hesla potom program funguje ďalej bez obmedzenia. Shareware býva podstatne lacnejší, ako podobné, ale komerčné programy. Pozor! Malware programy môžu sa šíriť ako SHAREWARE!

RETAIL

Konečná, ostrá verzia programu. Nemôže obsahovať Malware!

TRIAL / BETA

Skúšobná, testovacia verzia komerčného (RETAIL) programu. Nemal by obsahovať Malware.

SPYWARE

Špeciálny software, ktorý sa do počítača nainštaluje bez vedomia užívateľa. Môže sa šíriť ako SHAREWARE, FREEWARE, POSTCARDWARE, DEMO, TRIAL, BETA. Beží na pozadí a sleduje aktivitu systému, browsera, atď. Na základe tejto aktivity sú potom užívateľovi posielané reklamné E-maily (pozri definíciu **UCE**). Spyware môže tiež odcudziť rôzne heslá alebo čísla kreditných kariet.

ADWARE

Je to druh programu, ktorého získanie nestojí ani korunu, podobne ako freeware. Programátor umiestni svoju, alebo inú reklamu priamo do programu. Táto reklama zaberá určité miesto v okne programu, alebo môže obťažovať užívateľa. Na odstránenie tejto reklamy je potrebné zaplatiť autorovi, potom pomocou obdržaného registračného kľúča, alebo hesla sa reklama odstráni z programu.

MALWARE

Malicious software. Malware je akýkoľvek program alebo súbor, ktorý je škodlivý pre užívateľov počítača. Malware zahŕňa počítačové vírusy, červy, trójske kone a taktiež spyware. Pozor! Malware software môže zbierať informácie o počítači užívateľa bez jeho povolenia.

CAREWARE

Jedná sa o software, ktorý je možné získať zadarmo, napr. stiahnutím z Internetu. Cenou za používanie tohto produktu je niečo, ako ďalšia starostlivosť o program, ďalšie jeho šírenie a podobne. Pozor! Malware programy môžu sa šíriť ako CAREWARE!

TROJAN (HORSES)

Trójske kone. Tieto programy sa nainštalujú do systému, v naprogramovanom termíne sa spustia a prenášajú informácie z vnútra infikovanej internej počítačovej siete prostredníctvom Internetu útočníkovi cez firewall. Takýmto spôsobom, sa môžu dostať mimo spoločnosť aj mimoriadne citlivé informácie. Ide o cielené útoky na konkrétne IS z vonkajšieho prostredia. Trójsky kôň je program, ktorý sa po spustení správa na prvý pohľad ako legálny program. Vykonáva tajné škodlivé operácie. Typickým príkladom trójskeho koňa je falošná verzia antivírového programu. (Bola vzhľadovo podobná tomuto antivíru, v skutočnosti mazala súbory z disku). Dôležitou skutočnosťou je to, že trójsky kôň nie je schopný sa replikovať a nepripája sa k hostiteľskému súboru. Trójsky kôň sa vyskytuje na počítači spravidla iba v jednom exemplári, ktorý neobsahuje nič iné ako telo spomínanej infiltrácie. (súbor = trojan).

WORMS

Červy. Dnes sa týmto názvom označuje infiltrácia, ktorá sa dostane do PC elektronickou poštou (E-mailom). Červ má niekoľko čŕt spoločných s trójskym koňom. V počítači sa opäť vyskytuje najčastejšie iba v jednom exemplári - súbore, ktorý v sebe neobsahuje nič iného, ako menovaného červa (súbor = červ). Ako bolo povedané, červy do systémov prichádzajú v elektronickej pošte. "Postihnutý E-mail" obsahuje prílohu s pripojeným súborom. (Súbory majú názov napr.: citajma.txt.exe, setric.scr, SantaClaus.com, I_Love_You.txt.exe, Foto.jpg.exe, atď.) **Pokiaľ príjemca tento súbor spustí, dôjde k aktivácii červa!** Ten sa najčastejšie nakopíruje na počítač a vo vhodnom okamžiku odošle takto infikované E-maily na všetky adresy, ktoré nájde v užívateľovom adresári. Červy sú dnes mimoriadne rozšírené. Šíria sa aktívne, automaticky. Využívajú nedostatky v operačných systémoch (bezpečnostné diery). Šíria sa bez aktívnej účasti užívateľa. Prejdú cez firewall. Infikujú čo najviac počítačov v sieti a spôsobujú viaceré poškodenia systému. Jeden infikovaný dokument stačí k zamoreniu celej siete. Tieto vírusy predstavujú globálnu hrozbu a šíria sa vysokou rýchlosťou. Vírus Love.Letter za 4 hodiny obehol celý svet. Tieto infiltrácie počítajú s ľudskou zvedavosťou a psychikou, ukrývajú sa za názvy Anna Kurnikova, Pamela Anderson, Fotografie z môjho večierka a podobne. Toto je v texte podporené správou, že sa v pripojenom súbore nachádza atraktívny obrázok uvedenej dámy, alebo fotografie zo skvelej akcie, ktorej sa zúčastnil aj prijímateľ správy. Vzhľadom k tomu, že sa červy šíria prostredníctvom elektronickej pošty, rýchlosť a nebezpečenstvo šírenia sú obrovské. Dokazuje to aj prípad červa I_Love_You (VBS/Loveletter.A), ktorý sa dokázal po celom svete rozšíriť doslova za pár hodín. Červov je možné pokladať za podskupinu vírusov.

VÍRUS

Programy vytvorené za účelom infikovania jednotlivých súborov v počítači. Nie sú zamerané na vlastné aktívne šírenie. Šíria sa výhradne ľudskou komunikáciou, výmenou súborov. Tieto vírusy predstavujú lokálne nebezpečenstvo a šíria sa relatívne pomaly. Názov je odvedený z podobnosti správania sa týchto programátorských produktov s biologickými originálmi. Počítačový vírus je taká forma infiltrácie, ktorá má schopnosť vlastného množenia a infikovania ďalších systémov bez vedomia užívateľa.

MAKROVÍRUS

Vírus zapísaný do dokumentu vo formáte MS-Office®. Programy z MS-Office® neukladajú makrá spojené s dokumentom so zvláštneho súboru, ale tieto sa stávajú integrálnou súčasťou vytvoreného dokumentu. (Príkladom týchto súborov sú šablóny) V tomto prípade nejde o jednoduché súbory, ale o svojim spôsobom o programy.

VoIP (Voice over IP - Prenos hlasu cez IP)

Schopnosť prenášať štandardnú telefonickú/faxovú komunikáciu cez dátovú sieť. V technológii VoIP je hlas pretransformovaný digitálnymi signálovými procesormi do dátových segmentov, ktoré sú ukladané po dvoch do hlasových paketov. Tieto sú potom prenášané cez IP v súlade so štandardom H.323 ITU-T.

VÍRUS V POČÍTAČI

Vírus v počítači je program, alebo programujúci kód, ktorý sa aktivuje kopírovaním alebo spúšťaním jeho kopírovania do ďalších programov, počítačových zavádzacích sektorov alebo dokumentov.
Vírusy môžu byť prenášané ako prílohy k E-mailom alebo sťahovaním (download) súborom alebo sú prítomne na diskete alebo CD, DVD, USB kľúč, atď. Priamym zdrojom môže byť E-mail, download súboru alebo diskety, ktoré ste prijali. Väčšinou si nie ste vedomý toho, že obsahuje vírus. Niektoré vírusy sa prejavia hneď ako je spustený, iné vírusy ležia, čakajú až kým okolnosti nezapríčinia, že ich kód bude rozlúštený počítačom. Niektoré vírusy sú mierne alebo žartovné v úmysle a dojme (“Happy Birthday, Ludwig!").

COOKIES, ČO JE TO A AKO TO FUNGUJE

Cookies je informácia, ktorú web stránka uloží na hard disk (pozri definíciu **HDD**), tak si môže neskôr spomenúť na informáciu o vás. Je to informácia pre budúce využitie, ktorá je uložená serverom na klientovej strane klient/serverovej komunikácie. Cookie zapisuje vaše preferencie, keď používa určitú stránku. Každá žiadosť pre webovú stránku je nezávislá od ďalších požiadaviek.
Cookies je mechanizmus, ktorý umožňuje serveru uskladniť jeho vlastné informácie o užívateľovi na užívateľovom vlastnom počítači. Môžete si zobraziť cookies, ktoré boli na vašom hard disku, (hoci obsah uložený v každej cookies vám nemusí dávať zmysel).
Umiestnenie cookies záleží na prehliadači. Internet Explorer ukladá každú cookies v samostatnom súbore v podadresári Windows. Netscape ukladá všetky cookies v jednotnom cookies.txt súbore. Opera ich ukladá v jednotnom cookies.dat súbore.
Cookies sú zvyčajné používane na rotáciu reklám, ktoré posiela stránka, takže vám neposiela stále tie iste reklamy. Taktiež môžu byť použité na prispôsobenie stránok pre vás, založené na type prehliadača alebo iných informácií, ktoré ste poskytli web stránkam. Web užívatelia musia súhlasiť s ich uložením, ale vo všeobecnosti to pomáha web stránkam lepšie slúžiť užívateľom.
Existencia cookies a ich použitia je užívateľovi známa. Užívateľ môže zabrániť prístup informácií ku cookies. Napriek tomu, web stránka uskladní informácie o Vás v cookies, o ktorých neviete, takže cookies môžu byť považované za jednou z foriem spyware.

KEYSTROKE LOGGER (KEYLOGGER)

Niekedy nazývaný aj systémový monitor, je hardwarové zariadenie alebo malý program, ktorý monitoruje každý úder do klávesnice. Ako hardwarové zariadenie sa keystroke logger podobá zástrčke batériovej veľkosti, ktorá slúži ako konektor medzi užívateľovou klávesnicou a počítačom. Pretože sa zariadenie podobá na obyčajnú klávesnicovú zástrčku, je relatívne ľahko sledovať užívateľovo správanie tomu, kto chce skryť také zariadenie "z dohľadu".
Keystroke logger taktiež pomáha klávesniciam pracovných staníc zapojiť sa do zadnej časti počítača. Ako užívateľ píše, zariadenie zozbiera každý úder na klávesnici a uloží to ako text v jeho vlastnom miniatúrnom pevnom disku.
Keystroke logger program nepožaduje fyzicky prístup na užívateľov počítač. Môže to byť zámerné načítané niekým, kto chce monitorovať aktivitu na určitom počítači.
Keystroke logger zvyčajne pozostáva z dvoch súborov, ktoré sa inštalujú v rovnakom zozname. "DLL" knižnica (A dynamic link library), ktorý vykonáva všetku evidenciu a spustiteľný program EXE, ktorý inštaluje a zároveň spúšťa DLL knižnicu.
Keystroke logger zaznamenáva každý úder do klávesnice, ktorý užívateľ urobil a posúva informácie po Internete pravidelne tomu, kto program inštaloval.

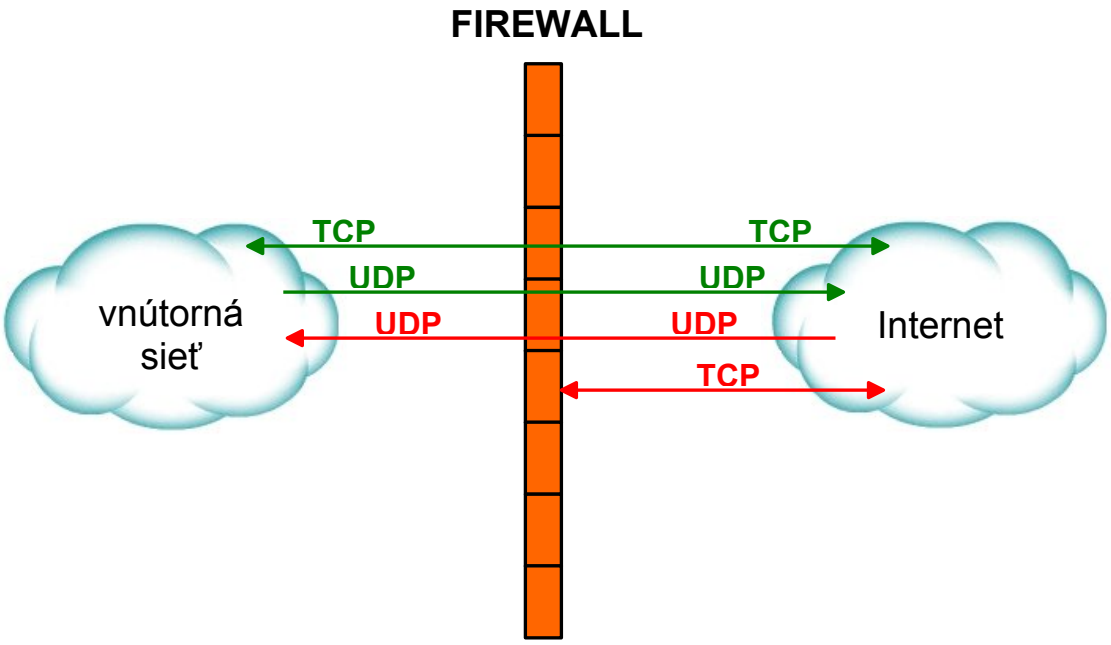
Pharming – nový druh finančných podvodov prostredníctvom Internetu

Pharming je formou Internetového podvodu, ktorý je oveľa nebezpečnejší ako **phishing**, pretože nevyžaduje využitie techník sociálneho inžinierstva.
Podľa údajov zozbieraných sieťou medzinárodnej technickej podpory antivírusovej spoločnosti dochádza k nárastu výskytu Internetových podvodov. Na celom svete sú každý deň detekované nové hrozby typu **phishing**. Táto nebezpečná technika sa používa za účelom zhromažďovania dôverných informácií. Dochádza pri nej k ukradnutiu totožnosti skutočnej osoby alebo organizácie, zvyčajne prostredníctvom podvodných E-mailov, ktoré používateľov nasmerujú na falošné web stránky.
Antivírusové spoločnosti však varujú pred novou podvodnou technikou, ktorou je **pharming**. Je oveľa nebezpečnejší.
Pharming je založený na zmene DNS (pozri definíciu **DNS**) položiek. To znamená, že web stránky, ktoré používateľ navštívi, nie sú web stránky pôvodné, ale falošné, vytvorené cyber-podvodníkmi, ktorí chcú získať dôverné údaje. Cieľom sú predovšetkým informácie spojené s on-line bankingom (Internet Banking).
Aké je pozadie pharming postupov? Keď používateľ napíše Internetovú adresu a chce vstúpiť na stránku, adresa sa musí zmeniť na skutočnú IP adresu, napr. 192.168.1.2. Prehliadač túto konverziu mena na IP adresu uskutočňuje prostredníctvom súboru **Hosts** na danom počítači a prostredníctvom nakonfigurovaných DNS serverov. DNS servery zabezpečujú konverziu mena servera na jeho IP adresu. Ak server nepridelí správnu IP adresu zadanému menu domény, používateľ sa na zvolenú stránku nedostane.
Pharming **útočí priamo na (vonkajšie) DNS servery,** a to takým spôsobom, že zmena adresy **postihne všetkých používateľov**, ktorý sa chcú dostať na daný server. Dá sa vykonať aj lokálne, napr. v prostredníctvom jednotlivých PC. Tento druhý scenár je ľahší pre útočníkov. Stačí urobiť dve veci: modifikovať malý súbor, nazývaný Hosts, ktorý je v každom počítači bežiacom pod systémom Windows a vytvoriť falošnú web stránku. Hosts súbor obsahuje mená serverov a IP adresy, ktoré sa použijú prednostne pri konverzii mena na adresu, takže na zmenu Internetovej adresy (URL) na IP adresy nie je potrebný. Napríklad, ak sa tento súbor prepíše falošnou adresou on-line bankingovej stránky, vždy, keď používateľ napíše meno tejto banky v prehliadači, dostane sa na stránku vytvorenú hackerom, ktorá vyzerá úplne rovnako ako stránka pôvodná. Nič netušiaca obeť na nej môže uviesť dôverné údaje a bez toho, aby si uvedomila, že ich práve dáva cyber-podvodníkovi.
Hacker môže editovať Hosts súbor (do systému sa dostane na diaľku) alebo použiť škodlivý kód, zvyčajne nejaký variant trójskych koňov z rodiny **Bancos, Banker a Banbra**. Pharmingové útoky sa dajú realizovať aj tak, že sa zneužije zraniteľnosť, ktorou sa dá dostať do systémových súborov.
Pharming indikátor všeobecnej veľkej zmeny vo vzťahu k Internetovým hrozbám. Narastá počet útokov, ktoré nie sú namierené výlučne na zasiahnutie čo najväčšieho počtu používateľov, ale na finančné obohatenie sa. Je preto nutné riešiť tento stav a prijať primerané preventívne opatrenia pred týmito útokmi.
Ak sa používatelia nechcú stať obeťami pharmingu, odporúča sa:
Používať software chrániaci pred škodlivými kódmi, ktorý kombinuje proaktívne a reaktívne detekčné systémy: počítač sa najľahšie stáva obeťou pharming útoku prostredníctvom škodlivých kódov, najmä trojanov. Majte na pamäti, že veľký počet trojanov sa do systémov dostáva tak, že používateľ si to ani nevšimne. Môžu byť v obehu aj dlhšie obdobie, kým ich antivírusové spoločnosti vôbec detekujú a prídu s vhodnou vakcínou. Preto veľmi odporúčame používať systémy proaktívnej ochrany, ktoré dokážu na báze analýzy správania predísť útokom a škodlivé kódy zablokovať.
Nepoužívať priamo URL pre Internet Banking. Napr. namiesto **https://www.otpdirekt.sk** používať IP adresu servera **https://212.5.211.52**.
Nainštalovať personálny firewall: toto predbežné opatrenie zabráni prístupu hackerov do počítača cez nechránený komunikačný port. Zabráni aj modifikácii systému.
Pravidelne aktualizovať software, ktorý máte nainštalovaný alebo používať systémy automatickej aktualizácie, čím sa vyhnete tomu, aby niekto využil zraniteľnosti vášho systému na podobné útoky.

príloha č. 2

Ako funguje predvolene nastavený FIREWALL?

(integrovaný Windows® firewall, hardwarový firewall)



odchádzajúce pripojenia (outgoing connections)
odchádzajúce žiadosti o pripojenie na vzdialený počítač – obojsmerný prenos

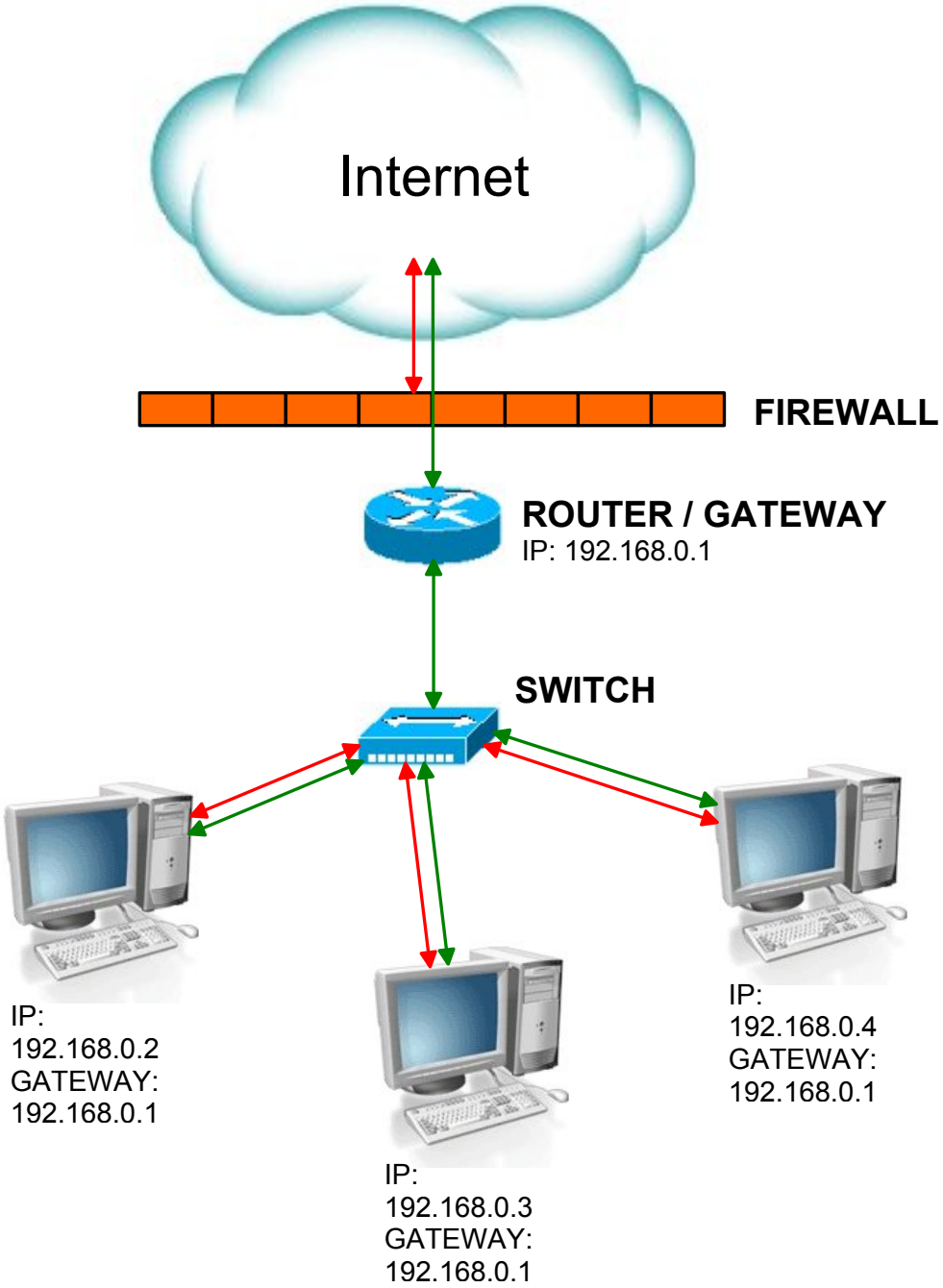
prichádzajúce pripojenia (incoming connections)
prichádzajúce žiadosti o pripojenie na lokálny počítač – obojsmerný prenos

Predvolene je povolené TCP a UDP pripojenie z vnútornej siete smerom von. Cez odchádzajúce TCP pripojenie môžu prúdiť údaje obojsmerne! Toto pripojenie sa používa na prístup pre vonkajšie servery, napr. Web server – TCP80,443; E-mail server – TCP25,110; ICQ® server – TCP5190, resp. TCP servery ktoré poskytujú elektronické služby. Túto skutočnosť môžu využívať hlavne SPYWARE programy, ktoré rovno idú na daný vonkajší cieľový server pre ktorý pošlú získané osobné údaje, a to všetko cez FIREWALL. Jediná možnosť ochrany v tomto prípade používať osobný (softvérový) firewall, ktorý môže jednotlivým aplikáciám individuálne blokovať komunikáciu. (Veľmi špeciálne SPYWARE programy nepoužívajú služby operačného systému a bez problémov vedia obísť softvérovú ochranu s tým, že buď vypínajú softvérový firewall alebo priamo používajú sieťovú kartu cez vlastné I/O porty. Tu je dôvod, prečo je veľmi riskantné sťahovať a spúšťať spustiteľné programy z Internetu a z príloh E-mailových správ. SPYWARE môže obsahovať akýkoľvek softvér.)

Predvolene je zakázané TCP a povolené UDP pripojenie z vonkajšej siete smerom do vnútra. V tomto prípade nemôžeme vo vnútri za firewallom umiestniť Web server, E-mail server, resp. TCP servery ktoré poskytujú elektronické služby. Z vonka nemajú prístup kvôli firewallu, lebo TCP komunikácia je filtrovaná. UDP pripojenie je povolené a to kvôli funkčnosti DNS prekladu – UDP53, hlasovej komunikácie (napr. ICQ® – UDP5190, Skype®), Windows® synchronizácia času (time synchronization - ntp) – UDP123.

príloha č. 3

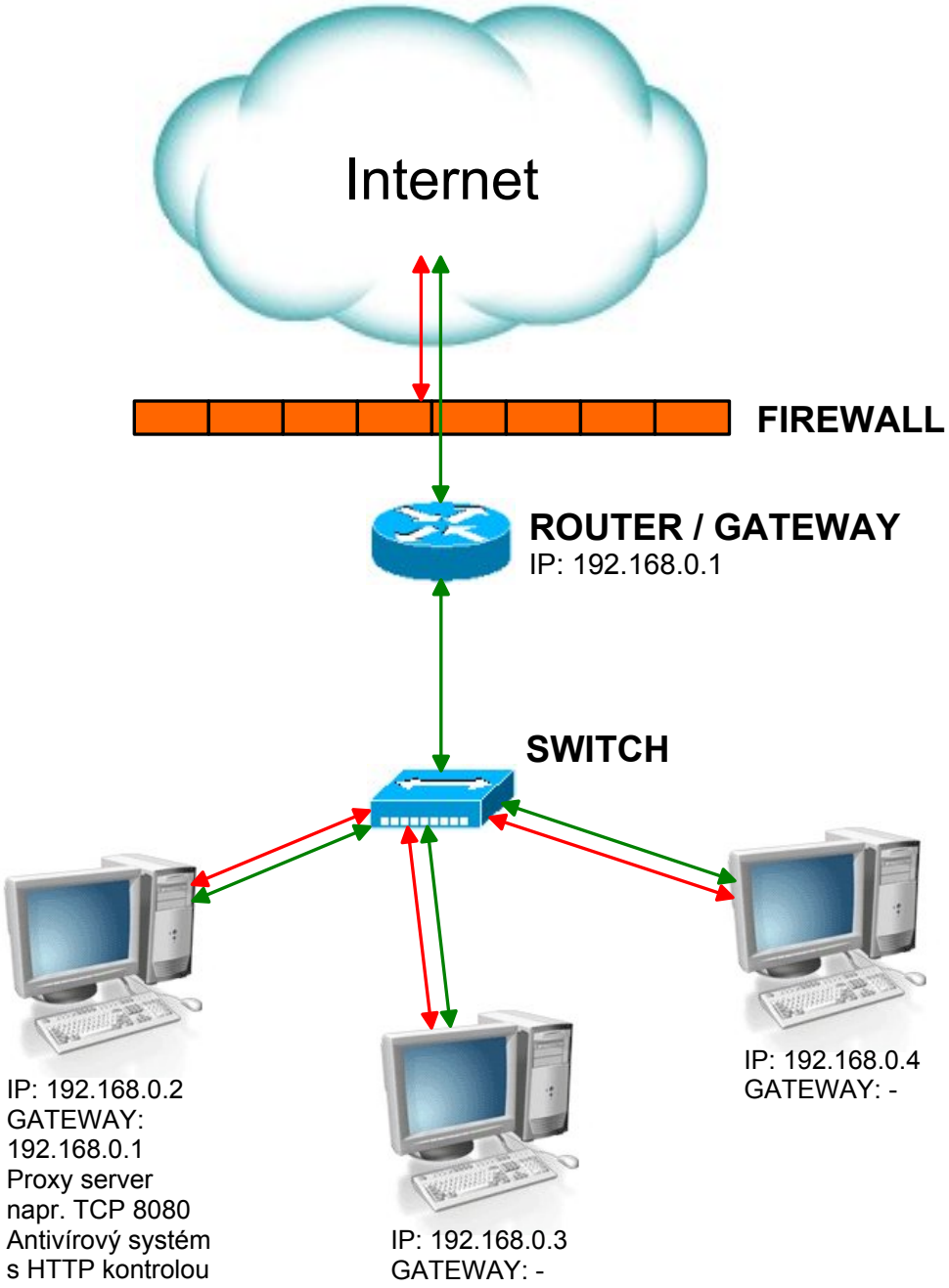
Menej bezpečné riešenie Internetového prístupu



V tomto prípade všetky pracovné stanice majú priamy prístup na Internet. Všetky stanice "vedia" kam posielať balíky (ďalej len packety), ktoré nepatria do lokálnej siete. Pre Internetový prístup ohľadom funkčnosti to je najfunkčnejšie riešenie, ale zároveň aj najnebezpečnejšie. Každý počítač musí byť dostatočne zabezpečený. Musí mať nainštalovaný antivírový systém, osobný firewall, operačný systém musí mať zapnuté automatické aktualizácie. Pre SPYWARE programy je to najideálnejšia konfigurácia prístupu na Internet. SPYWARE nemusí hľadať cestu kam má smerovať získané osobné údaje. Operačný systém mu zabezpečí prístup rovno cez ROUTER a FIREWALL.

príloha č. 4

Bezpečnejšie riešenie Internetového prístupu



V tomto prípade na jedenom - centrálnom - počítači beží služba Proxy (Proxy server – aplikačný Proxy server). Ten má priamy prístup na Internet. Ostatné pracovné stanice nemajú priamy prístup. Tie stanice “nevedia“ kam posielať packety, ktoré nepatria do lokálnej siete. Toto riešenie je oveľa bezpečnejšie pre Internetový prístup. Zabezpečiť treba len ten centrálny počítač. Ostatné počítače sa dostanú na Internet cez Proxy server. Na ostatných počítačoch stačí zapnúť integrovaný firewall. Počítače nemusia mať nainštalovaný osobný firewall, nainštalovaný antivírový systém pokiaľ na centrálnom počítači beží rezidentný antivírový systém schopnosťou HTTP kontroly. Pre SPYWARE programy je to najťažšia konfigurácia ohľadom prístupu na Internet. SPYWARE musí hľadať cestu (počítač, zariadenie) cez ktorú má smerovať packety a musí ešte nájsť aj správny port. V prípade keď nájde, Proxy server ešte žiada o overenie.

príloha č. 5

VZDELÁVACÍ INŠTITÚT

elfa
nové myšlienky nové možnosti

Číslo potvrdenia o akreditácii: 0726/4676/2005/172/1

OSVEDČENIE

o získanom vzdelaní s celoštátnou platnosťou

Jozef Tóth

meno a priezvisko

Úspešne absolvoval(a) kurz:

SPRÁVCA POČÍTAČOVÝCH SYSTÉMOV

v čase od 15.11.2004 do 31.12.2004

s odborným obsahom v predmetovej skladbe:

Technické prostriedky
Programové vybavenie
Počítačové siete a sieťové komunikácie
Bezpečnosť a legálne aspekty využívania počítačov

Osvedčenie o získanom vzdelaní s celoštátnou platnosťou vydané podľa §8 odst. 1 zákona č. 386/1997 Z. z. o ďalšom vzdelávaní a o zmene zákona Národnej rady Slovenskej republiky č. 387/1996 Z. z. o zamestnanosti v znení zákona č. 70/1997 Z. z. v znení zákona č. 567/2001 Z. z.

Číslo osvedčenia: 0088/05/2005

V Košiciach dňa 18. mája 2005

ELFA spol. s r.o. KOŠICE 0726 ČÍSLO KREDITU MŠV SR

Ing. Marián Bučko, CSc.
predseda skúšobnej komisie

Ing. Igor Sivý, CSc.
riaditeľ vzdelávacieho inštitútu

TÜV MANAGEMENT SERVICE ISO 9001

príloha č. 6

ECON CONSULTING obchodno-vzdelávacia agentúra, s.r.o.
P.O. Hviezdoslava č. 396/36, 922 42 Madunice, IČO: 44978961 , DIČ: 2022953042

OSVEDČENIE

o absolvovaní školenia

Zákon o ochrane osobných údajov

Meno účastníka:

Jozef Tóth

Účastník sa zúčastnil školenia, ktoré svojim obsahom zodpovedá **Zákonu č. 18/2018 o ochrane osobných údajov** účinnému od 25.5.2018 a získal vedomosti potrebné pre osobu, ktorá spracováva osobné údaje.

Osvedčenie vydáva **ECON CONSULTING obchodno-vzdelávacia agentúra, s.r.o.**

V **Košiciach** dňa **17.4.2018**

.....
Ing. Edita Svoreňová
lektor