Směrnice MU č. 6/2011

Správa a užívání počítačové sítě Masarykovy univerzity

(ve znění účinném od 24. 5. 2010)

Podle § 10 odst. 1 zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), dále jen „zákon", vydávám tuto směrnici:

Článek 1
Předmět úpravy, definice základních pojmů

(1) Tato směrnice upravuje správu a užívání počítačové sítě Masarykovy univerzity (dále jen „MU") a počítačů, které jsou do ní libovolnými prostředky funkčně připojeny. Vztahuje se na všechny osoby spravující či užívající tuto síť a tyto počítače.

(2) Pro účely této směrnice se následující termíny definují takto:

a) Počítač – jakékoliv technické zařízení disponující výpočetním výkonem připojitelné do počítačové sítě.

b) Počítačová síť – technické a programové prostředky používané k propojení počítačů.

c) Síť MU – počítačová síť ve vlastnictví či správě MU.

d) Počítačové prostředky – počítačová síť a počítače k ní přímo či nepřímo připojené.

e) Uživatel – každý, kdo přímo užívá počítačové prostředky.

f) Správce počítače – v případě počítačů ve vlastnictví či správě MU osoba, která je v rámci své činnosti pro MU pověřena údržbou počítače, včetně oprávnění na něm provádět systémové změny. U ostatních počítačů připojených do sítě MU ten, kdo daný počítač do sítě MU připojuje.

g) Doména – část počítačových prostředků užívaných a spravovaných některou součástí MU.

h) Administrátor domény – subjekt, který je pověřen k výkonu činností souvisejících se systémovou správou a údržbou počítačových prostředků svěřené domény.

i) Bezpečnostní politika – soubor opatření a pravidel k zajištění bezpečnosti sítě.

j) Bezpečnostní incident – jednotlivé narušení či ohrožení síťové bezpečnosti či bezpečnostní politiky.

Článek 2
Hierarchie sítě

(1) Síť MU je distribuovaná síť s určitým stupněm hierarchie. Skládá se z jednotlivých podsítí (domén), které jsou vytvářeny podle jednotlivých součástí MU a jejich lokalit. Univerzitní síť je zapojena do větších celků - české akademické sítě CESNET a globální sítě Internet - a je budována v souladu se zásadami budování těchto sítí.

(2) Globálním správcem sítě MU je Ústav výpočetní techniky MU (dále jen „ÚVT"). Jako takový je administrátorem celouniverzitní (nejvyšší) domény MU a odpovídá za provoz celouniverzitní páteře a za připojení jednotlivých fakult, vysokoškolských

ústavů a ostatních součástí univerzity. ÚVT přiděluje internetové adresy jednotlivým doménám.

(3) Koordinaci a řešení bezpečnostních incidentů v síti MU zajišťuje ÚVT prostřednictvím svého týmu CSIRT-MU (Computer Security Incident Response Team at Masaryk University). V oblasti bezpečnostních incidentů komunikuje s nadřazeným týmem akademické sítě CESNET a s podřízenými doménami sítě MU primárně tento tým.

(4) Jednotlivé domény v síti MU jsou spravovány těmi fakultami, vysokoškolskými ústavy, případně jinými součástmi univerzity, respektive jednotlivými pracovišti součástí univerzity, které je vytvořily, a to v úzké spolupráci s ÚVT. V rámci této správy rozhodují o tom, které pracoviště (zpravidla své Centrum informačních a komunikačních technologií, Laboratoř výpočetní techniky nebo Centrum výpočetní techniky, případně jiné oficiálně určené pracovníky) pověří být administrátorem dané domény. Pracovníci pověřeného pracoviště jsou zároveň styčnými osobami pro komunikaci se správcem nadřazené domény.

Článek 3
Základní úkoly a oprávnění administrátorů domén

(1) Administrátor domény dbá o to, aby provozem počítačových prostředků v jemu svěřené doméně nebyl omezován nebo dokonce poškozován provoz jiných částí sítě MU. Po odborné stránce je podřízen správci nadřazené domény; změny konfigurace sítě v rámci jeho domény jsou v jeho kompetenci, avšak je povinen uposlechnout pokyny správce nadřazené domény k nápravě případných technických nedostatků.

(2) Administrátoři jednotlivých domén musejí být pro případ nutnosti řešení bezpečnostních incidentů a jiných problémů dosažitelní globálním správcem sítě MU. Za tímto účelem administrátor domény poskytuje globálnímu správci sítě MU na sebe e-mailový kontakt, okamžitě mu hlásí jeho případné změny a bezodkladně reaguje na pokyny globálního správce sítě MU na něj zaslané. Administrátor domény přímo podřízené globálnímu správci sítě MU je povinen poskytnout rovněž i kontakt na mobilní telefon.

(3) Administrátor domény je povinen po dobu nejméně 1 měsíce uchovávat provozní záznamy (logy). V případě šetření bezpečnostního incidentu je administrátor příslušné domény povinen zajistit, pokud je toho s vynaložením nejvyššího možného úsilí schopen, identifikaci přihlášeného uživatele napadeného systému.

(4) Administrátor domény je oprávněn monitorovat provoz počítačových prostředků v ní v mezích daných právními předpisy týkajícími se ochrany soukromí, ochrany komunikace a zpracování osobních údajů. O informacích, se kterými v rámci této činnosti přijde do styku, je povinen zachovávat mlčenlivost. V případě zjištěného porušení pravidel provozu sítě MU je povinen s touto skutečností seznámit odpovědného akademického funkcionáře (rektora, děkana příslušné fakulty, ředitele vysokoškolského ústavu nebo univerzitního zařízení MU). V rámci monitorování může administrátor monitorovat i provoz v subdoménách, které spadají pod jeho doménu. Používání bezpečnostních aplikací pracovníky ÚVT na síti MU upravuje opatření ředitele ÚVT.

(5) Administrátor domény může odpojit subdoménu, ke které byly připojeny s ním nekonzultované technické prostředky nebo na níž byla provedena s ním nekonzultovaná změna konfigurace síťového programového vybavení a tyto prostředky či tato změna vedly k závažným poruchám, které ohrožují provoz sítě MU. Administrátor domény může také odpojit konkrétní stroj subdomény nebo subdoménu, pokud má důvodné podezření z jejich zneužití neoprávněnou osobou (útočníkem) a také stroj subdomény nebo subdoménu, jejíž administrátor

adekvátně nereaguje na hlášení bezpečnostního incidentu, který se dotýká tohoto stroje či subdomény.

(6) Administrátor domény je oprávněn stanovit další závazná pravidla, upravující specifické činnosti v připojených subdoménách (specifikace serverů služby DNS, komunikační protokoly, míra otevřenosti některých síťových služeb, pravidla pro hlášení bezpečnostních incidentů a reakci na ně, apod.).

Článek 4
Zabezpečení sítě a připojovaných počítačů

(1) Metodické řízení antivirové ochrany a dalších prvků zabezpečení sítě MU vykonává a jejich realizaci koordinuje globální správce sítě MU. Na centrální úrovni antivirovou ochranu rovněž přímo zajišťuje. Pokud ve výjimečných případech pošta neprochází přes centrální univerzitní poštovní server, tuto ochranu jsou povinni zajistit administrátoři jednotlivých poštovních serverů.

(2) Elektronická pošta obsahující v přílohách virus, který byl rozpoznán antivirovými nástroji na hlavních poštovních serverech MU, a elektronická pošta obsahující přílohy s typem souboru, který je potenciálně spustitelný a představuje riziko počítačového viru šířeného na běžně používaných platformách, nebude doručována adresátům, ale bude neprodleně odstraněna. Povinnost odstraňovat kontaminovanou nebo podezřelou poštu se vztahuje na poštovní servery všech součástí MU. Výjimky ze stanoveného postupu pro konkrétní doručovací adresy povoluje ředitel ÚVT.

(3) Provozovatelé univerzitních informačních systémů jsou povinni kontrolovat všechny datové soubory vkládané uživateli na výskyt virů. Všechny kontaminované či podezřelé soubory musejí být neprodleně odstraněny.

(4) Správce počítače, který připojuje svůj stroj prostřednictvím univerzitních přístupových bodů (např. sítě eduroam či VPN), je povinen dbát na odpovídající zabezpečení takového počítače (např. používat firewall, pravidelně aktualizovanou antivirovou ochranu, aplikovat záplaty používaného programového vybavení) a předcházet tak šíření škodlivých programů a útokům, které by mohly být prováděny prostřednictvím takto připojovaného počítače.

Článek 5
Přístupová práva

(1) Přístup k síti MU předpokládá jednoznačnou identifikaci každého uživatele. Přístup uživatele k síti MU (zpravidla prostřednictvím osobního počítače připojeného k této síti) je možný pouze autentizovaně (typicky pomocí uživatelského jména a hesla).

(2) Každý zaměstnanec MU a každý její student má právo na zřízení uživatelského účtu (dále jen „účet"). S každým jednotlivým účtem jsou spojena určitá přístupová práva, která určují oprávnění uživatele ve vztahu ke zdrojům a službám sítě MU.

(3) Uživatel, kterému je účet zřízen, je povinen jej chránit netriviálním heslem a toto heslo udržovat v tajnosti. Heslo k vlastnímu (individuálnímu) účtu nesmí sdělit druhé osobě a to ani správci počítače, na němž je účet zřízen. Heslo nesmí být zasíláno nezabezpečenou elektronickou poštou.

(4) Uživatel smí používat pouze ta přístupová práva, která mu řádným způsobem náleží, a nesmí vyvíjet žádnou činnost směřující k obejití tohoto ustanovení. Pokud uživatel počítače ve vlastnictví či správě MU jakýmkoliv způsobem získá přístupová práva,

která mu nebyla přidělena (např. chybou programů nebo technického vybavení), je povinen tuto skutečnost neprodleně oznámit správci počítače. Takto získaná práva nesmí použít. Uživatel nesmí zneužít nedbalosti jiného uživatele (např. opomenuté odhlášení) k tomu, aby v síti pracoval pod cizí identitou.

Článek 6
Obecná pravidla užívání

(1) Uživatelé využívají počítačové prostředky MU ve shodě se svými pracovními a studijními úkoly.

(2) Je zakázáno využívat počítačových prostředků MU k:

a) páchání přestupků, trestných činů či jakékoliv jiné činnosti, která je v rozporu s českým právním řádem,

b) politické a náboženské agitaci, rasové a národnostní diskriminaci,

c) výdělečné činnosti, šíření obchodních sdělení či jiným aktivitám komerčního charakteru mimo rámec pracovního či studijního vztahu s MU,

d) obtěžování, klamání nebo zastrašování jiných uživatelů. Za takovou činnost se považuje i rozesílání řetězových e-mailů či e-mailů na náhodně vybrané adresy v síti.

(3) Je zakázáno používat vulgárních a silně emotivních výrazů při komunikaci otevřené dalším účastníkům (elektronické diskusní skupiny, fóra apod.).

(4) Uživatelé musejí postupovat tak, aby jejich činnost negativně ovlivňovala možnosti využití počítačových prostředků dalšími uživateli v co nejmenším rozsahu. To platí jak pro neúměrné zatěžování linek v době jejich maximálního využití, tak i pro neúměrné zatěžování jednotlivých počítačů. V případě, že uživatel potřebuje užít počítačové prostředky nad tento rámec, věc konzultuje s administrátorem domény a řídí se dále jeho rozhodnutím a pokyny.

(5) Využívání sítě MU v rámci vědecké a pedagogické spolupráce se studenty a zaměstnanci jiných organizací je možné pouze na základě písemného svolení, vydaného děkanem příslušné fakulty, ředitelem vysokoškolského ústavu nebo univerzitního zařízení nebo rektorem. V případě, že se jedná o dlouhodobější vztah, je nezbytné konkrétní podmínky využívání počítačové sítě MU, včetně případných sankčních opatření, specifikovat ve smlouvě mezi MU a organizací, jejíž pracovníci síť MU využívají. Tato smlouva nemusí být uzavřena v případě, že se jedná o spolupráci se zaměstnanci či studenty jiných veřejných vysokých škol v České republice či pracovišť Akademie věd České republiky.

Článek 7
Vlastnická a autorská práva

(1) Uživatelé jsou povinni respektovat vlastnická a autorská práva MU, ostatních uživatelů i jiných subjektů.

(2) Především je zakázáno, a to ať již by měla být ohrožena či narušena vlastnická či autorská práva kohokoliv:

a) poškozování, zcizování nebo ničení počítačů, programového vybavení, komunikačních linek, či jiných počítačových prostředků,

b) neautorizovaná modifikace programů, dat nebo technického vybavení. Obzvláště nesmějí být prováděny neautorizované změny konfigurace počítačových prostředků, které by mohly mít vliv na provoz celé sítě,

c) neoprávněná instalace, sdělování veřejnosti nebo rozmnožování uměleckých děl, počítačových programů, databází a dalších výsledků tvůrčí duševní činnosti, které jsou chráněny autorským zákonem, neautorizované kopírování (byť i částí) dat,

d) užívání počítačové sítě k získání neautorizovaného přístupu k neveřejným informačním zdrojům.

Článek 8
Soukromí dat uživatelů

(1) MU se snaží chránit práva a oprávněné zájmy všech uživatelů své sítě a v této souvislosti i chránit data a informace uložené na počítačích MU nebo přenášených sítí MU. MU však nemůže technicky zabezpečit úplné soukromí a bezpečnost dat uložených na počítačích nebo přenášených sítí. Vysoce citlivá data proto nemohou být na počítačích sítě uložena či sítí přenášena bez použití dodatečných prostředků jejich zabezpečení (minimálně na úrovni šifrování).

(2) Pro zajištění maximální možné míry soukromí a bezpečnosti dat je uživatelům zakázáno:

a) provádění jakýchkoliv akcí vedoucích k neoprávněnému narušení soukromí jiného uživatele, a to i v těch případech, kdy uživatel svá vlastní data explicitně nechrání,

b) prohlížení obsahu uživatelských adresářů, jakož i kopírování jakýchkoliv dat nebo programů z nich bez výslovného svolení uživatele. Toto omezení platí i v případě, že uživatelské adresáře jsou svými oprávněnými uživateli ponechány volně přístupné elektronickými prostředky,

c) odposlouchávání provozu a vytváření kopií zpráv procházejících jednotlivými uzly sítě,

d) vědomé využívání neoprávněně získaných dat, případně jejich nabízení jiným subjektům.

Článek 9
Sankce

(1) Administrátor domény má právo zrušit přístup k počítačové síti uživateli, který porušil ustanovení této směrnice, a to na dobu nejvýše jednoho měsíce. Uživatel má právo odvolat se proti tomuto rozhodnutí k děkanovi příslušné fakulty, respektive řediteli vysokoškolského ústavu, nebo v případě jiných součástí univerzity k rektorovi. Odvolání nemá odkladný účinek.

(2) Porušení ustanovení této směrnice studentem bude považováno za disciplinární přestupek.

(3) Porušení ustanovení této směrnice bude u zaměstnanců považováno za porušení základních povinností zaměstnance (§ 301 odst. 1 písm. c) a d) zákoníku práce) a lze z něj vyvodit příslušné pracovněprávní důsledky včetně rozvázání pracovního poměru.

Článek 10

Závěrečná ustanovení

(1) Tato směrnice nabývá účinnosti dnem zveřejnění, s výjimkou uvedenou v odst. 2.

(2) Pro Správu kolejí a menz MU se účinnost ustanovení této směrnice, týkajících se povinnosti zabezpečit přístup k síti MU pouze za podmínky jednoznačné identifikace každého uživatele, stanoví ve vztahu k Unihotelu Žerotínovo náměstí, Unihotelu Čejkova, Unihotelu Grohova a Univerzitnímu centru Šlapanice od 1. srpna 2011, ve vztahu ke kolejím od 1. září 2011.

(3) Kontrolou dodržování pravidel touto směrnicí předepsaných a jejich bližším výkladem se pověřuje ředitel ÚVT.

(4) Směrnice č. 2/2003 Užívání počítačové sítě Masarykovy univerzity a směrnice č. 3/2004 Antivirová ochrana počítačové sítě Masarykovy univerzity se zrušují.

V Brně 24. května 2011

Petr Fiala
rektor