S T U

Smernica rektora
Číslo: 3/2016 – SR

Zvýšenie bezpečnosti AIS Slovenskej technickej univerzity v Bratislave

Dátum: 22. 02. 2016

Slovenská technická univerzita v Bratislave, Vazovova 5, Bratislava

V Bratislave 22. 02. 2016
Číslo: 3/2016–SR

Rektor Slovenskej technickej univerzity v Bratislave (ďalej len „rektor“) v súlade s článkom 3 smernice rektora číslo 4/2013-SR Pravidlá vydávania interných predpisov Slovenskej technickej univerzity v Bratislave vydáva nasledovnú smernicu rektora

Zvýšenie bezpečnosti AIS
Slovenskej technickej univerzity v Bratislave:

Článok 1
Úvodné ustanovenia

1. Smernica rektora „Zvýšenie bezpečnosti AIS Slovenskej technickej univerzity v Bratislave“ (ďalej len „smernica“) je vnútorná organizačná a riadiaca norma Slovenskej technickej univerzity v Bratislave (ďalej tiež ako „STU“), ktorá určuje opatrenia na zvýšenie úrovne bezpečnosti prístupu k Akademickému informačnému systému STU (ďalej len „AIS“) dvojfaktorovou autentifikáciou pomocou verejných kľúčov a preukazov s kontaktným čipom (ďalej tiež ako systém na zvýšenie bezpečnosti AIS“).
2. Smernica umožňuje implementovať a prevádzkovať uzavretú infraštruktúru verejných kľúčov (ďalej len „PKI“), v rámci ktorej bude zriadená certifikačná autorita „IS STU Bratislava CA“ (ďalej len „certifikačná autorita“ alebo „CA“).
3. Smernica je záväzná pre všetkých zamestnancov STU a študentov doktorandského štúdia na STU, ktorí sú povinní oboznámiť sa s jej obsahom a dodržiavať jej ustanovenia; študenti doktorandského štúdia na STU sa oboznámia s touto smernicou prostredníctvom vedúceho školiaceho pracoviska, zamestnancov STU oboznámia s touto smernicou ich nadriadení vedúci.
4. Rektor poveruje riaditeľa Centra výpočtovej techniky STU vydaním Certifikačného poriadku certifikačnej autority, ktorým sa spresnia a doplnia organizačné postupy a práva a povinnosti v zmysle tejto smernice.

Článok 2
Definície pojmov

Na účely tejto smernice:

1. **Dvojfaktorovou autentifikáciou** sa rozumie identifikácia a overenie identity používateľa informačného systému pomocou súboru dvoch bezpečnostných

prvkov: PIN kódu, ktorý pozná len používateľ, a čipovej karty s certifikátom, ktorú vlastní rovnako len používateľ.

2. **Infraštruktúra verejných kľúčov (PKI)** je technické, programové a organizačné vybavenie prevádzkované na Centre výpočtovej techniky STU (ďalej len „CVT“) zaisťujúce služby pre vydávanie a správu certifikátov.
3. **Certifikát** je súbor dát podľa štandardu X.509, ktorý preukazuje spojitosť medzi verejným kľúčom a identitou jeho držiteľa.
4. **Certifikačná autorita (CA)** je dôveryhodná autorita, ktorá zabezpečuje vydávanie certifikátov, ich spravovanie, uloženie do bezpečného úložiska, zrušenie a správu zoznamu zneplatnených certifikátov.
5. **Registračné autority (RA)** sú zaškolení zamestnanci personálnych útvarov súčastí STU, ktorí zabezpečujú objednávanie, výrobu a odovzdávanie preukazov vydávaných na STU ich držiteľom a ďalší rektorom alebo riaditeľom Centra výpočtovej techniky STU poverení zamestnanci.
6. **Certifikačný poriadok** je dokument, ktorý obsahuje informácie o podmienkach poskytovania certifikačných služieb, práva a povinnosti účastníkov PKI, spôsob overovania identity žiadateľov a pravidlá vydávania, používania a zneplatňovania certifikátov.
7. **Čipová karta** je karta s kontaktným čipom Gemalto IDCore 40 (80 KB), ktorý slúži na bezpečné uloženie certifikátu. Čipová karta vydaná študentovi STU alebo zamestnancovi STU musí okrem kontaktného čipu obsahovať aj bezkontaktný čip Mifare Desfire EV1 (8 KB) (zjednodušene označovaná aj ako „hybridná karta“), a zaručovať kompatibilitu so systémami STU využívajúcimi bezkontaktné študentské a zamestnanecké preukazy typu Mifare Desfire EV1.

Článok 3
Chránené aplikácie AIS

1. V podmienkach STU si vyžadujú dvojfaktorovú autentifikáciu používateľov, a to najneskôr po skončení implementačnej fázy, nasledovné aplikácie:
   a) Záznamník učiteľa – všetky aplikácie v ňom.
   b) Správa kariet – všetky aplikácie v nej, okrem aplikácie „Overenie platnosti identifikačných kariet“.
   c) Študijná evidencia – všetky aplikácie v nej.
   d) Prijímacie konanie – všetky aplikácie v ňom.
2. Po zneplatnení certifikátu môže byť do chránených aplikácii AIS dočasne, najviac na dobu 30 dní, povolený prístup v štandardnom režime bez použitia dvojfaktorovej autentifikácie. Podmienkou je osobná návšteva držiteľa zneplatneného certifikátu na pracovisku RA, overenie jeho identity podľa certifikačného poriadku a podanie žiadosti o vydanie následného certifikátu. Po vydaní následného certifikátu alebo po vypršaní doby štandardného režimu, bude používateľovi automaticky nastavený režim dvojfaktorovej autentifikácie bez možnosti predĺženia doby štandardného režimu.

Článok 4
Okruh používateľov
s povinnosťou vlastniť certifikát vydaný CA

Používatelia, ktorí v rámci plnenia svojich pracovných povinností alebo na základe interného predpisu STU pristupujú do chránených aplikácii AIS definovaných v článku 3 bod 1 tejto smernice (ďalej len „oprávnení používatelia PKI“) sú povinní stať sa držiteľmi certifikátu a čipovej karty.

Článok 5
Implementácia PKI

1. Implementačná fáza PKI začína dňom účinnosti tejto smernice a končí uplynutím 12 mesiacov.
2. Počas implementačnej fázy musia byť všetky existujúce preukazy oprávnených používateľov PKI, ktoré nemajú kontaktný čip, vymenené za čipové alebo hybridné karty.
3. Po skončení implementácie PKI nesmú byť oprávneným používateľom PKI vydávané iné preukazy, než čipové alebo hybridné.
4. Organizáciou a riadením implementácie PKI je poverený riaditeľ CVT.
5. CVT stanoví harmonogram a postupy implementačných prác, v rámci ktorých poverí svojich zamestnancov na vykonávanie úloh certifikačnej a registračnej autority.
6. Na každej fakulte STU[1] rektor poveruje úlohami registračnej autority v zmysle certifikačného poriadku CA príslušného systémového integrátora AIS[2] a príslušné pracovníčky pre personálne činnosti. Ďalších zamestnancov RA vyberie a písomne poverí riaditeľ CVT z ním riadených organizačných zložiek.
7. Zamestnanci RA vytvárajú žiadosti o vydanie certifikátu za oprávnených používateľov PKI podľa harmonogramu implementácie PKI.

Článok 6
Povinnosti účastníkov PKI a priamo nezúčastnených strán

1. Všetci zamestnanci STU a študenti doktorandského štúdia na STU:
   a) nesmú za žiadnych okolností použiť čipovú kartu iného držiteľa alebo poznať kód PIN alebo PUK iného používateľa. Porušenie tohto ustanovenia je hrubým porušením smernice,
   b) v prípade nálezu akéhokoľvek preukazu s logom STU sú povinní odovzdať ho na ľubovoľnom študijnom alebo personálnom oddelení STU, alebo na pracovisku CA,

[1] Článok 2 bod 2 platného Organizačného poriadku STU.
[2] Podľa aktuálneho zoznamu integrátorov zverejneného na http://is.stuba.sk/dok/integratori.pl

c) v prípade podozrenia zo zneužitia akejkoľvek súčasti PKI alebo pri podozrení z kompromitácie pripojených systémov, čipových kariet alebo certifikátov sú povinní bezodkladne ohlásiť túto skutočnosť pracovisku CA na CVT.

2. Všetci držitelia certifikátu CA:
   a) nesmú za žiadnych okolností poskytnúť svoju čipovú kartu alebo kód PIN alebo PUK na použitie inej osobe, ani nesmú vedome dopustiť, aby ich čipovú kartu použila iná osoba. Porušenie tohto ustanovenia je hrubým porušením smernice,
   b) nesmú uchovávať kódy PIN a PUK v dosahu inej osoby, ani spolu s čipovou kartou, čítačkou alebo s počítačom,
   c) sú povinní oboznámiť sa a riadiť sa ustanoveniami certifikačného poriadku CA.
3. Delegovanie práv a superpráva v AIS:
   Pre použitie inštitútu delegovania práv a superpráva sú používatelia, na ktorých boli práva delegované a používatelia, ktorí využijú superprávo povinní použiť svoju vlastnú čipovú kartu pre prístup do chránených aplikácii AIS.

Článok 7
Disciplinárny postih študentov za porušenie smernice a certifikačného poriadku

Porušenie pravidiel stanovených v certifikačnom poriadku a v článku 6 tejto smernice je považované za porušenie interných predpisov STU a rieši sa disciplinárnym konaním v zmysle platného Disciplinárneho poriadku pre študentov STU.

Článok 8
Disciplinárny postih zamestnancov za porušenie smernice a certifikačného poriadku

Porušenie pravidiel stanovených v certifikačnom poriadku a v článku 6 tejto smernice je považované za porušenie základných povinností zamestnanca v zmysle platného Pracovného poriadku pre zamestnancov STU.

Článok 9
Záverečné a prechodné ustanovenia

1. Riaditeľ Centra výpočtovej techniky STU je oprávnený ku dňu účinnosti tejto smernice spustiť do skúšobnej prevádzky systém na zvýšenie bezpečnosti AIS; pritom je oprávnený určiť okruh osôb a rozsah aplikácií v jednotlivých

chránených aplikáciách AIS podľa článku 3 tejto smernice, na ktorých bude overovaná správnosť a funkcionalita jednotlivých opatrení v rámci systému na zvýšenie bezpečnosti AIS.

2. Skúšobná prevádzka systému na zvýšenie bezpečnosti AIS musí trvať najmenej šesť mesiacov (ďalej len „skúšobná prevádzka“).
3. Po vyhodnotení skúšobnej prevádzky riaditeľ Centra výpočtovej techniky STU:
   a) oboznámi rektora s výsledkami skúšobnej prevádzky systému na zvýšenie bezpečnosti AIS,
   b) určí upravené, doplnené alebo zmenené podmienky, za ktorých sa bude systém na zvýšenie bezpečnosti AIS na základe výsledkov jeho skúšobnej prevádzky trvale prevádzkovať (ďalej len „úprava podmienok trvalej prevádzky systému na zvýšenie bezpečnosti AIS“),
   c) v nadväznosti na kvantitu a charakter úpravy podmienok trvalej prevádzky systému na zvýšenie bezpečnosti AIS posúdi nevyhnutnosť zmeny alebo doplnenia tejto smernice postupom podľa bodu 4 tohto článku,
   d) určí deň začatia riadnej prevádzky systému na zvýšenie bezpečnosti AIS a uvedenú skutočnosť vhodným spôsobom oznámi zamestnancom STU a študentov STU, ktorých sa uvedená skutočnosť týka; od uvedeného dňa platia ustanovenia tejto smernice v plnom rozsahu.
4. Akékoľvek zmeny a doplnenia tejto smernice je možné vykonať len číslovanými dodatkami vydanými a podpísanými rektorom.
5. Táto smernica nadobúda platnosť dňom jej podpisu a účinnosť 1. marca 2016.

prof. Ing. Robert Redhammer, PhD.,[3]
rektor

[3] Originál podpísanej smernice rektora číslo 3/2016-SR Zvýšenie bezpečnosti AIS Slovenskej technickej univerzity v Bratislave je uložený a k nahliadnutiu prístupný na právnom a organizačnom útvare Rektorátu STU.