

ŽIVOTOPIS

Mgr. Martin Rublík, Ph.D.

E-mail: martin.rublik@bspc.sk
martin.rublik@gmail.com



VZDELANIE

Fakulta hospodárskej informatiky, Ekonomická Univerzita, Bratislava 2005 - 2010
Ph.D. v odbore Hospodárska informatika (študijný odbor 9.2.10)

Fakulta matematiky, fyziky a informatiky, Univerzita Komenského, Bratislava 2000 - 2005
Magister v odbore Informatika (študijný odbor 9.2.1)

CERTIFIKÁTY A ABSOLVOVANÉ ŠKOLENIA

ISC² Certified Information Systems Security Professional (CISSP License ID: 384919)

Microsoft (MCP ID: 7814110)

- **Microsoft Certified IT Professional Enterprise Administrator**
 - 70-680 TS: Configuring Windows 7
 - 70-643 TS: Configuring Windows Server 2008 Applications Infrastructure
 - 70-647 Pro: Windows Server 2008, Enterprise Administrator
 - 70-642 TS: Configuring Windows Server 2008 Network Infrastructure
 - 70-640 TS: Configuring Windows Server 2008 Active Directory
- 70-351 TS: Configuring Microsoft Internet Security and Acceleration Server 2006
- 70-158: Forefront identity Manager 2010, Configuring

Autor kapitoly v knihe:

Názov: „Multidisciplinary Perspectives in Cryptology and Information Security“
Kapitola: Chapter 11 Cryptographic Key Distribution and Management
Autori: Dr. Eng. Sattar B. Sadkhan, Nidaa A. Abbas
Vydavateľstvo: IGI-Global
ISBN: 9781466658080
Rok vydania: 2014

Spoluautor knihy:

Názov: „Počítačové siete v hospodárskej praxi“
Autori: Peter Závodný, Ľubomír Turňa, Martin Rublík
Vydavateľstvo: Ekonóm, Bratislava
ISBN: 978-80-225-2731-6
Rok vydania: 2009

Hakin9

Názov: „SSL/TLS PKI Issues“
Autori: Martin Rublík
Vydavateľstvo: Software Press Sp, Warszawa
ISSN: 1733-7186
Rok vydania: 2012

Hakin9

Názov: „Overview of side-channel and timing attacks“
Autori: Martin Rublík
Vydavateľstvo: Software Press Sp, Warszawa
ISSN: 1733-7186
Rok vydania: 2012

bettercrypto.org

Názov: „Applied Crypto Hardening“
Autori: <https://bettercrypto.org/#acknowledgements>
Autor časti: HTTP Strict Transport Security (HSTS)

ODBORNÁ PRAX

BSP Consulting spol. s r.o., K Železnej studienke 27, 811 04 Bratislava

2005 – súčasnosť

Pozícia: Systémový administrátor a konzultant pre oblasť informačnej bezpečnosti

- Kryptografia a správa identity používateľov

Návrh a implementácia PKI založených na X.509 certifikátoch. Jednotlivé projekty zahŕňali tak technickú podporu (inštalácia a konfigurácia hardvérových a softvérových častí riešenia) ako aj tvorbu certifikačných poriadkov, pravidiel na výkon certifikačných činností a samotnú podporu pri implementácii infraštruktúry verejných kľúčov v rámci podnikového prostredia.

V rámci implementácie PKI som participoval pri inštalácii a konfigurácii viacerých hardvérových šifrovacích modulov (nCipher/Thales a SafeNet). Realizoval som niekoľko typov inštalácií, medzi inými inštalácie HSM pre vysoko-dostupné riešenia.

Návrh a implementácia riešení na ochranu a kontrolu správy prístupu k elektronickým dokumentom (Enterprise rights management). Projekty zahŕňali tak technickú podporu ako aj tvorbu bezpečnostných pravidiel a smerníc a ich začlenenie v rámci podnikového prostredia.

Návrh a implementácia rozličných systémov na riadenie identity používateľov. Medzi inými skúsenosti s autentifikačnými servermi a príbuznými protokolmi. Praktické skúsenosti z oblasti autentifikácie vo webových aj tradičných aplikáciách.

- **Sieťová bezpečnosť**

Inštalácia a konfigurácia rozličných typov sieťových zariadení (firewall, VPN koncentrátory, zariadenia v bezdrôtových sieťach, prepínače, IDS a pod.). Zodpovednosť za návrh LAN a implementácie sieťových služieb ako aj ich administrácia.

- **Správa a riadenie rizika v informačných technológiách**

Vykonávanie auditov IT bezpečnosti s ohľadom na princípy a metódy uvedené v medzinárodných štandardoch ISO/IEC 27005 a ISO/IEC 27002.

- **Bezpečnosť a správa informačných systémov**

Administrácia serverov, ich konfigurácia a hardening operačných systémov.

- **Cloud workplace a kolaborácia**

Migrácia on-premise riešení do Office 365, správa a zabezpečenie/hardening Office 365 / Cloud App Security. Správa identít a viac-faktorová autentifikácia.

Vybrané projekty:

- Implementácia infraštruktúry verejných kľúčov v organizácii Slovak Telekom, a.s.
- Konsolidácia infraštruktúry verejných kľúčov v organizácii Slovak Telekom, a.s.
- Nasadenie systému riadenia čipových kariet v organizácii Slovak Telekom, a.s.
- Implementácia Active Directory Rights Management Services v organizácii Orange
- Implementácia Active Directory Rights Management Services v organizácii Slovak Telekom, a.s.
- Poradenstvo týkajúce sa čipových kariet a kryptografických tokenov v E.ON IS
- Implementácia ADFS a custom attribute store pre komunikáciu s OpenAM pre spoločnosť Posam
- Implementácia systému riadenia životného cyklu identít a ich synchronizácie v rámci informačných systémov pre spoločnosť VW
- Implementácia autentifikačných a autorizačných služieb určených pre nadnárodnú skupinu bánk (Active Directory/Kerberos a Active Directory Federation Services/SAML, OAuth, OpenID Connect) / Erste Group IT International
- Implementácia služby synchronizácie identít v nadnárodnej skupine bánk (Microsoft Identity Manager, Azure AD Connect) / Erste Group International
- Konzultácie v rámci implementácie dátovej klasifikácie v prostredí Office 365 v nadnárodnej skupine bánk (Azure Information Protection) / Erste Group IT International
- Migrácia internej infraštruktúry do Microsoft Office 365 a Azure v prostredí spoločnosti FPT, s.r.o

- Ekonomická univerzita v Bratislave, Dolnozemska cesta 1, 852 35 Bratislava** 2014
Pozícia: Externý spolupracovník
- Diplomové práce:*
- Bc. Peter Melich, Prechod na IPv6 v heterogénnych sieťach, FHI, EUBA, 2014
- Ekonomická univerzita v Bratislave, Dolnozemska cesta 1, 852 35 Bratislava** 2013
Pozícia: Externý spolupracovník
- Učiteľská prax:*
- Vedenie predmetu „Ochrana a bezpečnosť informačných systémov“
- Diplomové práce:*
- Bc. Martin Bešina, Reakcia na narušenie bezpečnosti certifikačnej autority, FHI, EUBA, 2013
 - Bc. Martin Solčanský, Využitie X.509 certifikátov v aplikáciách, FHI, EUBA, 2014
- Účasť vo vedeckom výbore na konferencii:*
- International Conference on Electrical, Communication, Computer, Power, and Control Engineering – 2013 ICECCPCE13 : <http://www.tcmosul.net/conference> (Iraq, Mosul: Dec. 16-17, 2013)
- Ekonomická univerzita v Bratislave, Dolnozemska cesta 1, 852 35 Bratislava** 2009 – 2012
Pozícia: Odborný asistent
- Učiteľská prax:*
- Vedenie predmetu „Ochrana a bezpečnosť informačných systémov“
 - Vedenie cvičení z predmetu „Operačné systémy“
 - Vedenie cvičení z predmetu „Počítačové siete“
- Bakalárske práce:*
- Peter Melich, *Prechod na IPv6 z pohľadu bezpečnosti*, FHI, EUBA, 2012
- Oponentské posudky k dizertačným prácam*
- Ing. Kamil Krauspe, *Riešenie triedy úloh poštára prostredníctvom evolučnej optimalizácie*, FHI, EUBA, 2012
 - Ing. Ján Pittner, *Využitie genetických algoritmov na riešenie úloh geometrickej optimalizácie*, FHI, EUBA, 2012
 - Ing. Marián Šedivý, *Riešenie okružných úloh pomocou Swarm Intelligence*, FHI, EUBA, 2012
- Bakalárske stredisko FHI EU: Bakalár NF, Bystrická 4, Žarnovica** 2007 – 2008
Pozícia: Asistent
- Učiteľská prax:*
- Vedenie predmetu „Počítačové siete“

Sieťová bezpečnosť:

- Konfigurácia firewallov (Microsoft ISA Server, CISCO PIX/ASA),
- Znalosť sieťových a aplikačných protokolov (TCP/IP, DNS, SNMP, SSL/TLS, HTTP, SMTP, LDAP, IPSec, a.i.), Praktické skúsenosti s množstvom nástrojov využívaných pri audite zabezpečenia počítačových sietí. Medzi inými skúsenosti s: Wireshark, Fiddler
- Praktické skúsenosti s budovaním vysoko-dostupných riešení, medzi inými: SQL Server failover clustering, IIS network load balancing, Active Directory Certificate Services failover clustering, Active Directory Rights Management Services load balancing, Forefront Identity Manager Certificate Management load balancing, Hyper-V failover clustering
- SSL/TLS hardening konfigurácia web serverov

Šifrová ochrana informácií a správa identity používateľov:

- Znalosti z oblasti teoretickej informatiky a matematických metód ochrany informácie,
- Špecialista pre autentifikačné protokoly (NTLM/Kerberos/integrovaná autentifikácia, SAML, WS-Security, OpenID Connect, OAuth)
- Praktické skúsenosti s infraštruktúrou verejných kľúčov (Public Key Infrastructure – PKI), skúsenosti so softvérom pre certifikačné autority:
 - Active Directory Certificate Services
 - IDNomic/Opentrust/Keynectis PKI
 - EJBCA
 - Signserver
- Praktické skúsenosti s ochranou a správou prístupu k elektronickým dokumentom (Enterprise Rights Management), skúsenosti so softvérom na ochranu elektronických dokumentov ako napr.:
 - Azure Information Protection
 - Active Directory Rights Management Services
 - Microsoft Cloud App Security
- Praktické skúsenosti so špecializovaným hardvérom určeným na bezpečné vykonávanie šifrových operácií, medzi inými skúsenosti s čipovými kartami (Gemalto ID Prime .NET/MD, Crescendo C700, SafeNet eToken, Oberthur IAS-ECC), kryptografickými tokenmi iKey, a hardvérovými šifrovacími modulmi (HSM) nCipher netHSM / Thales nShield Connect a SafeNet Luna.
- Praktické skúsenosti so systémami riadenia životného cyklu čipových kariet, napr.:
 - IDNomic/Opentrust/Keynectis CMS,
 - Forefront Identity Management 2010 Certificate Management / Microsoft Identity Manager
- Praktické skúsenosti v oblasti správy identity používateľov, znalosť produktov:
 - Active Directory / Azure AD / Azure MFA
 - Active Directory (Lightweight) Directory Services, OpenLDAP
 - Forefront Identity Manager 2010 / Microsoft Identity Manager / DirSync / Azure AD Connect
 - Active Directory Federation Services / MFA on-premise
 - Safenet Authentication Service
- Praktické skúsenosti z oblasti správy cloudových služieb a identít používateľov
 - Azure Active Directory / Office 365
 - Safenet Authentication Services / Cloud
- Praktické skúsenosti z oblasti Cloud Access Security Broker
 - Microsoft Cloud App Security

Správa informačných systémov (oblasť aplikačnej bezpečnosti a správy informačných systémov):

- Správa viacerých druhov operačných systémov (Microsoft Windows Server, Linux)
- Administrácia a konfigurácia aplikačných serverov (Microsoft Internet Information Services, Apache)

- Skúsenosti s nástrojmi business intelligence (Microsoft SQL Server, Microsoft Reporting Services)
- Administrácia, správa a používanie nástrojov na skupinovú spoluprácu (Microsoft Exchange, Microsoft Office, Microsoft Sharepoint Portal Server, Office 365)

Programovacie jazyky:

- Skriptovacie jazyky: powershell, bash, perl,
- Základy T-SQL
- Základy C, C#

ZNALOSŤ JAZYKOV

Angličtina: plynulá konverzácia, písané slovo

Nemčina: pasívne