INFORMATION SECURITY SUMMIT

2011 PRAGUE

May 25th – 26th 2011 | 25. – 26. května 2011

The Minorite Monastery of St. James | Klášter minoritů sv. Jakuba

Prague, The Czech Republic | Praha, Česká republika

INFORMATION SECURITY SUMMIT

12th International Conference / 12. ročník mezinárodní konference

CRISIS PLANS AND SECURITY / KRIZOVÉ PLÁNY A BEZPEČNOST

Under the Auspices of / Pod záštitou

- A Deputy Minister of the Ministry of Industry and Trade, Ing. Jiří Jirka
  náměstka ministra Ministerstva průmyslu a obchodu ČR Ing. Jiřího Jirky
- A Deputy Minister of the Ministry of Interior, Mgr. Michal Moroz
  náměstka ministra Ministerstva vnitra ČR Mgr. Michala Moroze
- A Deputy Minister of the Ministry of Labour and Social Affairs, Bc. Vladimír Šiška, MBA
  1. náměstka ministra Ministerstva práce a sociálních věcí ČR Bc. Vladimíra Šišky, MBA
- A Deputy Director of the National Security Authority, Ing. Jaroslav Šmíd
  náměstka ředitele Národního bezpečnostního úřadu Ing. Jaroslava Šmída
- A Deputy Minister of the Ministry of Finance, Mgr. Zdeněk Zajíček
  náměstka ministra Ministerstva financí ČR Mgr. Zdeňka Zajíčka

Platinum Partners / Platinoví partneři

IBM

ICZ

Dear Madam, Dear Sir,

We would like to offer you an opportunity to meet top experts in information security and information systems risk management from both the Czech Republic and abroad at the Information Security Summit (IS2) Conference. This twelfth annual conference, with its theme "Crisis Plans and Security", will be held at the Minorite Monastery of St. James in the centre of Prague on the 25th – 26th May, 2011.

The conference is one of the top events of the year for information security and information systems risk management in the Czech Republic. The organisers' aim is to try to give information security professionals the opportunity to meet top experts from all over the world and thus facilitate an exchange of information at a top international level. The compositions of both the programme committee and the list of speakers reflect this aim.

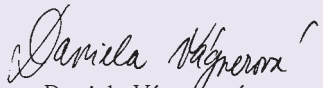
Renowned experts in various areas of crisis management, information security and information systems risk management have accepted our invitation and will be attending this conference. Eugene Schultz and Matthew Pemble will be discussing various aspects of incident management, Danilo Gligoroski, a leading cryptologist, will discuss bottlenecks in digital signatures, Martin Kašša from Slovalco, Ondřej Bos from the Ministry of the Interior, and Jozef Opálený from Mondi Štětí will discuss their experiences of crisis management. Dennis Kügler will share his experiences of introducing new electronic IDs in Germany. During the panel discussion you will be able to discuss issues concerning data leak prevention.

As in previous years, there will not only be a rich professional programme, but also a pleasant environment for informal discussions with the speakers and the other participants. We will certainly not be leaving out the traditional evening party and, by moving to a new venue, the event will also give you the opportunity to see another jewel of Prague's architectural heritage.

We are looking forward to seeing you at the conference, an event you will not want to miss.

Yours

Eva Racková
On behalf of the IS2 Programme Committee



Daniela Vágnerová
On behalf of the IS2 Organizing Committee

Vážená paní, Vážený pane,

jak se již stalo tradicí i letos si dovolujeme Vám nabídnout příležitost k setkání se špičkovými odborníky na informační bezpečnost a řízení rizik informačních systémů z domova i ze zahraničí na konferenci Information Security Summit (IS2). Dvanáctý ročník konference nese podtitul „Krizové plány a bezpečnost". Konat se bude v Kláštěře minoritů sv. Jakuba v centru Prahy ve dnech 25. – 26. května 2011.

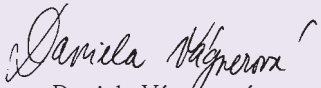
Pro časopis DSM i odbornou obec jeho předplatitelů a čtenářů je tato pravidelná květnová konference jedním z vrcholů celoroční práce v oblasti informační bezpečnosti a řízení rizik informačních systémů. Snahou organizátorů je umožnit odborné veřejnosti mezinárodní výměnu zkušeností v těchto oblastech. Tomu odpovídá složení programového výboru i přednášejících.

I letos přijali naše pozvání světoví odborníci v různých oblastech informační bezpečnosti a řízení rizik informačních systémů. Eugene Schultz a Matthew Pemble budou hovořit o různých aspektech reakce na incidenty. Danilo Gligoroski, uznávaný kryptolog, ukáže na nedostatky digitálních podpisů. Martin Kašša ze společnosti Slovalco, Ondřej Bos z Ministerstva vnitra ČR a Jozef Opálený ze společnosti Mondi Štětí budou prezentovat své zkušenosti s krizovým řízením. Dennis Kügler se podělí o zkušenosti ze zavádění nových elektronických občanských průkazů v Německu. V rámci panelové diskuse pak budete mít možnost diskutovat o problémech prevence úniku dat.

Stejně jako v minulých letech se i letos pro Vás budeme snažit vytvořit nejen bohatý odborný program, ale také příjemné prostředí k neformálním diskusím s přednášejícími nebo dalšími účastníky konference. Chybět nebude ani tradiční večerní setkání. I letos bychom Vám rádi ukázali zajímavý pražský architektonický objekt.

Na setkání s Vámi se těší

Eva Racková
za programový výbor IS2



Daniela Vágnerová
za organizační výbor IS2

Programme Committee

Eva Racková, KPMG CR & DSM (Chairman)
Rudolf Haňka, University of Cambridge
Zdeněk Kaplan, Česká pojišťovna & DSM
Vashek Matyáš, MU Brno & DSM
Jan Mikulecký, RAC & DSM
Zdeněk Říha, MU Brno
Eugene Schultz, Emagined Security

Programový výbor

Eva Racková, KPMG CR a DSM (předsedkyně)
Rudolf Haňka, University of Cambridge
Zdeněk Kaplan, Česká pojišťovna a DSM
Vašek Matyáš, MU Brno a DSM
Jan Mikulecký, RAC a DSM
Zdeněk Říha, MU Brno
Eugene Schultz, Emagined Security

PROGRAMME

Wednesday, May 25th 2011

8:00 – 9:00 Registration, coffee

9:00 – 9:30 Opening Ceremony

9:30 – 10:15 **Enterprise Amnesia and Data Overload**
Jeff Jonas

10:15 – 11:00 **Log Management & Intelligence: Taking Care of What's Important**
Ramses Gallego

11:00 – 11:30 Coffee break and exhibition visits

11:30 – 12:15 **Crisis Plans where Minutes are Essential**
Martin Kašša, Libor Široký

12:15 – 13:00 **The New German Identity Cards**
Dennis Kügler

13:00 – 14:15 Lunch

14:15 – 15:00 **Problems of ISO 27001 Matrix Certification**
Martin Dvořák, Zora Říhová

15:00 – 15:45 **A Recovery Disaster Plan for Primary IT Infrastructure as a Tool for Shareholder Peace of Mind**
Jozef Opálený

15:45 – 16:15 Coffee break and exhibition visits

16:15 – 16:45 **Certain Fundamentals in the Drafting of Crisis Documentation and the Influence of Crisis Planning on the Operations of an Organization**
Ondřej Bos

16:45 – 18:00 **Panel Discussion – Data Leakage Prevention in Practice**
Tomáš Filip, Jiří Maňas, Tomáš Matoušek
Chaired by: **Zdeněk Kaplan**

19:00 – 22:00 Reception Buffet

PROGRAM

Středa 25. května 2011

8:00 – 9:00 Registrace, káva

9:00 – 9:30 Slavnostní zahájení

9:30 – 10:15 **Podniková amnézie a záplava dat**
Jeff Jonas

10:15 – 11:00 **Řízení a analýza logů: řešení toho, co je podstatné**
Ramses Gallego

11:00 – 11:30 Káva a výstavka

11:30 – 12:15 **Krizové plány když jde o minuty**
Martin Kašša, Libor Široký

12:15 – 13:00 **Německé občanské průkazy**
Dennis Kügler

13:00 – 14:15 Oběd

14:15 – 15:00 **Problematika maticové certifikace na ISO 27001**
Martin Dvořák, Zora Říhová

15:00 – 15:45 **Havarijní plán základní IT infrastruktury jako nástroj pro klidný spánek akcionářů**
Jozef Opálený

15:45 – 16:15 Káva a výstavka

16:15 – 16:45 **Některé zásady zpracování krizové dokumentace a vliv krizového plánování na zajištění chodu organizace**
Ondřej Bos

16:45 – 18:00 **Panelová diskuse – Prevence úniku dat v praxi**
Tomáš Filip, Jiří Maňas, Tomáš Matoušek
moderátor: **Zdeněk Kaplan**

19:00 – 22:00 Recepce

PROGRAMME

Thursday, May 26th 2011

8:00 – 9:00 Registration, coffee T-Systems

9:00 – 9:15 Opening Address

9:15 – 9:30 Keynote

9:30 – 10:15 **The Most Common Mistakes in Incident Response**
Eugene Schultz

10:15 – 11:00 **Cryptography for (partially) Compromised Sensor Networks**
Petr Hanáček, Petr Švenda

11:00 – 11:30 Coffee break and exhibition visits

11:30 – 12:15 **Bottlenecks in Applied Digital Signatures Schemes**
Danilo Gligoroski

12:15 – 12:40 **Wiggum in Cyberspace: Legal Issues in Czech and EU Cybersecurity**
Radim Polčák

12:40 – 14:15 Lunch nextiraOne The Communications Experts

14:15 – 15:00 **Network Monitoring – Tool for Detecting and Avoiding Incident**
Pavel Minařík

15:00 – 15:45 **Practical Models for Incident Management**
Matthew Pemble

15:45 – 16:00 Lottery Draw, Closing Ceremony

PROGRAM

Čtvrtek 26. května 2011

8:00 – 9:00 Registrace, káva T-Systems

9:00 – 9:15 Zahájení druhého dne

9:15 – 9:30 Keynote

9:30 – 10:15 **Nejčastější chyby při reakcích na incidenty**
Eugene Schultz

10:15 – 11:00 **Kryptografie pro (částečně) kompromitované sensorové sítě**
Petr Hanáček, Petr Švenda

11:00 – 11:30 Káva a výstavka

11:30 – 12:15 **Omezení v aplikovaných schématech digitálních podpisů**
Danilo Gligoroski

12:15 – 12:40 **Vygum v kyberprostoru: Právní otázky české a evropské kybernetické bezpečnosti**
Radim Polčák

12:40 – 14:15 Oběd nextiraOne The Communications Experts

14:15 – 15:00 **Monitoring sítě – prostředek odhalování a prevence incidentů**
Pavel Minařík

15:00 – 15:45 **Praktické ukázky řízení incidentů**
Matthew Pemble

15:45 – 16:00 Vylosování soutěže – tombola, slavnostní zakončení

JEFF JONAS

Jeff Jonas is the chief scientist at the IBM Entity Analytics group. The IBM Entity Analytics group was formed based on technologies developed by Systems Research & Development (SRD), which was founded by Jonas in 1984 and acquired by IBM in January 2005. Prior to IBM's acquisition of SRD, Jonas lead the company through the design and development of a number of extraordinary systems, including technology used by the surveillance intelligence arm of the gaming industry. Jonas is a senior associate at the Center for Strategic and International Studies. He periodically testifies on privacy and counterterrorism in such venues as the White House before the President's Privacy and Civil Liberties Oversight Board, the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, and other federally convened commissions.

ENTERPRISE AMNESIA AND DATA OVERLOAD

Today, as computing power grows, we are experiencing an unprecedented rise in the amount of data. This unstructured data is generated by social networks, blogs, emails and others. As Eric Schmidt noted, "Every two days now we create as much information as we did from the dawn of civilization up until 2003." This rapid growth of data and the impossibility of keeping up with it presents a challenge for governments, organizations, businesses and individuals and significantly affects fields such as national security, corporate data security or privacy. In order to make better and smarter decisions we need to make sense of what's happening faster.

RAMSES GALLEGO

With a background in Business Administration and Law, Ramses is a +15 years security professional with deep expertise in the Risk Management and Governance areas. After being at CA Technologies (formerly known as Computer Associates) for 8 years and also being Regional Manager for SurfControl in Spain and Portugal, he is now General Manager of Security and Risk Management practice at Entel IT Consulting where he strategizes the vision of the area and oversees the deployment of services. He has been serving in ISACA's CISM Certification Committee for three years and is now a member of the CGEIT Certification Committee. Ramses is also the Chair for ISACA's ISRM Conference, CISM Director at the Barcelona Chapter and part of the Programme Committee for the SecureCloud 2010 event that took place in Barcelona. He is also part of the ISACA's CISM Practice Analysis Task Force as well as serving in the Guidance & Practices Committee. Ramses is one of the first CCSK (Certification of Cloud Security Knowledge) holders from the Cloud Security Alliance and also holds the following certifications: CISM, CGEIT, CISSP, SCPM (Stanford Certified Project Manager), ITIL, COBIT Foundation and Six Sigma Black Belt. He lives in Barcelona.

LOG MANAGEMENT & INTELLIGENCE: TAKING CARE OF WHAT'S IMPORTANT

JEFF JONAS

Jeff Jonas je vedoucím analytické skupiny IBM, která se zabývá ochranou dat. IBM Entity Analytics group staví na technologiích vyvinutých společností Systems Research & Development (SRD), kterou Jonas založil v roce 1984. IBM firmu získala v lednu 2005. Před akvizicí IBM společnost Jeffa Jonase navrhla a vyvinula celou řadu pozoruhodných systémů včetně bezpečnostních technologií, které využívá herní průmysl. Jeff Jonas je spolupracovníkem Centra pro strategická a mezinárodní studia. V otázkách ochrany soukromí a boje s terorismem pravidelně spolupracuje s Bílým domem, Ministerstvem vnitřní bezpečnosti Spojených států a dalšími federálními institucemi.

PODNIKOVÁ AMNÉZIE A ZÁPLAVA DAT

S tím, jak neustále narůstá počítačový výkon, zažíváme v historii nebývalý nárůst množství dat. Tato nestrukturovaná data generují mimo jiné sociální sítě, blogy a emaily. Jak podotkl Eric Schmidt, „Každé dva dny dnes vytvoříme takové množství informací, jako celé lidstvo vytvořilo od počátku civilizace do roku 2003." Tento razantní růst a nemožnost držet s ním krok představují velkou výzvu pro vlády, organizace i běžné uživatele a výrazně ovlivňuje oblasti jako je národní bezpečnost, korporátní ochrana dat nebo ochrana osobních údajů. Abychom mohli docházet k lepším a „chytřejším" rozhodnutím, potřebujeme rychleji analyzovat dění kolem nás.

RAMSES GALLEGO

Ramses Gallego má více než 15 let zkušeností jako bezpečnostní specialista se zaměřením na řízení rizik a otázky celkového řízení bezpečnosti. Jeho zkušenosti podtrhuje praxe ve vedení a v právní oblasti. Po osmi letech v CA Technologies (dříve Computer Associates) a pozici regionálního manažera pro SurfControl ve Španělsku a Portugalsku je nyní generálním ředitelem divize Security and Risk Management v Entel IT Consulting. Zaměřuje se na vize v této oblasti a vývoj služeb. Tři roky byl členem ISACA CISM Certification Committee a nyní je členem CGEIT Certification Committee. Je také předsedou konferencí ISRM pořádaných organizací ISACA, CISM Director pro ISACA v Barceloně a člen programového výboru konference SecureCloud 2010, která se konala v Barceloně. Kromě toho je členem CISM Practice Analysis Task Force organizace ISACA a členem Guidance & Practices Committee. Ramses byl jedním z prvních CCSK (Certification of Cloud Security Knowledge) od Cloud Security Alliance a je držitelem následujících certifikací: CISM, CGEIT, CISSP, SCPM (Stanford Certified Project Manager), ITIL, COBIT Foundation a Six Sigma Black Belt. Žije v Barceloně.

ŘÍZENÍ A ANALÝZA LOGU: ŘEŠENÍ TOHO, CO JE PODSTATNÉ

Martin Kašša

Martin Kašša studied at the Faculty of Economic Informatics of the University of Economics in Bratislava. As a student he started working at Slovalco, moving gradually through various positions; he has been the Continuous Improvement Manager, responsible also for project management, since 2007. In 2010, he headed the BCMS Implementation project, with the business continuity management system being certified in February 2011 by Det Norske Veritas (according to BS 25999:2). This is the first BCMS certification in both Slovakia and the Czech Republic.

Libor Široký

Libor Široký graduated from the Faculty of Nuclear Science and Physical Engineering at the Czech Technical University in 2000. Since then, he has been working at Risk Analysis Consultants as a consultant and senior consultant specializing in risk analysis and business continuity management. He is currently leading two projects in BCMS implementation based on BS 25999-2:2007. This is the first Czech and first Slovak BCMS certification ever completed.

CRISIS PLANS WHERE MINUTES ARE ESSENTIAL

The intention of this paper is to share practical experience with BCMS (Business Continuity Management System) implementation within Slovalco, the largest aluminium manufacturer in Central Europe. The decision to pursue a BCMS implementation according to BS 25999-2:2007 was made at the beginning of 2010. The project itself lasted a full year, with the certification audit taking place in February 2011. Slovalco is the first Slovak company to receive the BCMS certification. An integral part of the BCMS implementation was its incorporation into the existing integrated management system structure (consisting of QMS, EMS, OHSAS, ISMS). The objective of the BCMS implementation was to identify the requirements and needs of continuity and recovery regarding Slovalco's main production processes in the event of their disruption or interruption. Taking into account the specific type of production and other company specifics, it was particularly necessary to focus on incident management procedures following a process interruption after a sustained incident. It was necessary to adjust the existing incident management structure, set up crisis management processes and approve new communication strategies. A newly developed incident management concept was prepared in compliance with the requirements of BS 25999-2 and the existing disaster recovery procedures were verified, updated and added to the final BCMS concept. To enable a quick and effective response and recovery from disruptions, a gold – silver – bronze command structure was defined. The development of business continuity and recovery plans were designed from the beginning with the knowledge that even a brief interruption (as little as a few minutes) of the main production processes could be absolutely fatal. In the cases of more serious incidents, where more than one of the main production processes is interrupted, it was necessary to identify the priorities related to process recovery, as well as the priorities with respect to resource allocation. The starting point in identifying recovery priorities was the business impact analysis and the assessment of risks that could be the potential cause of process interruptions.

Dennis Kügler

Dennis Kügler is the head of the working group responsible for developing security specifications and designing public key infrastructures related to electronic identity documents at the Federal Office for Information Security. Since 2003 he has been participating as a government representative in the New Technologies Working Group of the International Civil Aviation Organization and actively contributing to international standardization at ISO.

THE NEW GERMAN IDENTITY CARDS

After many years of development, the New German Identity Card was introduced on the 1st of November 2010. Besides being just an ordinary identification token for government use, this identity card also provides privacy-protecting authentication on the Internet. Unique features, such as anonymous age verification, the selective disclosure of personal attributes and the automatic creation of unlinkable, service provider dependent, pseudonyms serve the needs of both citizens and Internet service providers. This presentation will give an overview on the features of the card and the infrastructure required. Furthermore, some real world use cases will be described.

Martin Kašša

Ing. Martin Kašša vytudoval Fakultu hospodářské informatiky na Ekonomické univerzitě v Bratislavě. Už v době studií pracoval ve společnosti Slovalco a.s., kde postupně prošel několika pracovními pozicemi, od roku 2007 pracuje na pozici manažer pro trvalé zlepšování a zastřešuje i oblast projektového řízení. V roce 2010 vedl projekt Implementace BCMS. Vybudovaný manažerský systém řízení kontinuity činností byl certifikovaný společností Det Norske Veritas v únoru 2011 podle BS 25999:2. Jedná se o první certifikaci BCMS na Slovensku a v České republice.

Libor Široký

Ing. Libor Široký, CISM, CRISC od ukončení vysokoškolského studia na Fakultě jaderné a fyzikálně inženýrské v roce 2000, pracuje jako samostatný konzultant ve společnosti Risk Analysis Consultants, spol. s r. o., kde se zabývá především oblastí business continuity managementu. V současnosti řídí projekty přípravy dvou společností na získání certifikace podle BS 25999-2:2007.

KRIZOVÉ PLÁNY KDYŽ JDE O MINUTY

Záměrem příspěvku je přiblížit postup implementace systému řízení kontinuity činností (BCMS – Business Continuity Management System) v největší hliníkárně ve střední Evropě. Slovenský hliníkárenský kolos Slovalco se rozhodl přistoupit k zavedení BCMS podle BS 25999-2:2007 počátkem roku 2010. Projekt přípravy probíhal po celý zbytek roku 2010, certifikační audit proběhl v lednu 2011 a jedná se o první Slovenskou certifikaci BCMS. Nedílnou součástí implementace byla integrace nového systému řízení BCMS do stávající struktury IMS (QMS, EMS, OHSAS, ISMS). Cílem implementace BCMS bylo identifikovat požadavky a potřeby pro zajištění kontinuity a obnovy hlavních výrobních procesů společnosti Slovalco v případě jejich narušení nebo přerušení. S ohledem na typ podniku a specifický charakter výroby bylo zejména nutné se detailně věnovat postupům zvládání mimořádných událostí. Bylo nezbytné upravit stávající strukturu reakcí na incidenty, nastavit postupy krizového řízení a schválit komunikační strategie. Nová koncepce zvládání incidentů byla sladěna s požadavky BS 25999-2, existující havarijní postupy byly verifikovány a zahrnuty do cílového konceptu BCMS. Byla vytvořena třiúrovňová struktura řízení incidentů; operativní, taktická a strategická. Příprava plánů kontinuity a obnovy výrobních procesů byla od počátku koncipována se znalostí toho, že i krátkodobé přerušení (v řádu desítek minut) hlavních výrobních procesů může být pro společnost doslova fatální. Pro případ rozsáhlejších incidentů, kdy může dojít k přerušení více procesů současně, bylo nutné stanovit priority obnovy procesů a souvisejících zdrojů již ve fázi plánování. Východiskem pro určování priorit obnovy byla provedená analýza dopadů spolu s hodnocením rizik, která mohou být příčinou narušení hlavních výrobních a podpůrných procesů.

Dennis Kügler

Dr. Dennis Kügler je vedoucí pracovní skupiny zodpovědné za navržení bezpečnostních specifikací a infrastruktury PKI pro elektronické identifikační průkazy ve Spolkovém úřadu pro informační bezpečnost. Od roku 2003 se jako vládní zástupce účastní skupiny NTWG (pracovní skupina pro nové technologie) organizace ICAO (Mezinárodní organizace pro civilní letectví) a aktivně přispívá do mezinárodních standardů v organizaci ISO.

NĚMECKÉ OBČANSKÉ PRŮKAZY

1. listopadu 2010 byl po řadě let vývoje zaveden nový typ německého občanského průkazu. Kromě toho, že se jedná o běžný identifikační průkaz pro úřední účely, umožňuje tato karta internetovou autentizaci způsobem chránícím soukromí držitele. Jedinečné vlastnosti jako anonymní ověření věku, detailní možnost výběru osobních atributů (pro sdělení protistraně) a automatické vytváření nespojitelných pseudonymů pro poskytovatele služeb pokrývají potřeby občanů i poskytovatelů internetových služeb. Prezentace poskytne přehled vlastností občanského průkazu a potřebné infrastruktury. Popsány budou i příklady z praxe.

Martin Dvořák

Martin Dvořák has been the service delivery manager at Siemens IT Solutions and Services since 2010. In addition, he is also responsible for the preparation and organisation of audits according to ISO 27001 and ISO 20000 standards. From 2008 to 2010 he worked as a software architect, focusing on the security of developed solutions. He graduated from the Faculty of Informatics and Statistics at the University of Economics, Prague.

Zora Říhová

Zora Říhová graduated from the University of Economics, Prague, and has practical experience gained from both sides – as a customer of IT services (Head of Informatics and Organizations at Unipetrol; Information Manager at ZSE) and also the supplier of IT Services (Head of SAP Product at PVT). At Siemens IT Solutions and Services, Ltd. she worked as a Senior Project Manager to lead projects to implement large-scale information systems and is now dedicated to quality management. She is also an associate professor at the University of Economics, Prague (the Department of Systems Analysis at the Faculty of Informatics and Statistics), which deals with the system aspects of organization, process and project management issues.

PROBLEMS OF ISO 27001 MATRIX CERTIFICATION

Contribution is focused on problems of matrix certification of organization on conformity with ISO/IEC 27001 standard and definition of advantages and difficulties of this approach toward certification. The goal of this contribution is to discuss essence of matrix certification, its rationale, process and impacts on organization of audit including time and organisational demand. There are also analysed questions on process design; possibilities of alignment between selected regions and are analysed approaches of auditors and points of interest.

Jozef Opálený

Jozef Opálený is the Finance and IT Director at Mondi Štětí. He joined the company in 2008. Over the last 7 years he has worked as a finance director at various companies and industry sectors, such as Danzer Bohemia-Dýhárna (veneers), Mubea (automotive) and Mondi (paper maker). Taking responsibility for the IT department at a well-known Czech TOP100 company is a new challenge for him. Jozef has a Masters Degree from the Faculty of Economy and Management of the Slovak University of Agriculture. He has been living in Czech Republic since 2000.

A RECOVERY DISASTER PLAN FOR PRIMARY IT INFRASTRUCTURE AS A TOOL FOR SHAREHOLDER PEACE OF MIND

Data security is a priority responsibility of the management of every company. A large amount of the Czech Republic's manufacturing capacity is located in the flood zones. Unfortunately, Mondi Štětí has experience of the 2002 floods. Štětí is situated just a few kilometres from the confluence of the Vltava and Elbe rivers. A risk assessment performed some time before the flood gave us a clear message to take care of the security of our data centre and its data, which is indispensable for running the company. There are further security developments currently underway at the company, not only against flooding, but against other risks as well.

Martin Dvořák

Ing. Martin Dvořák je od roku 2010 Service delivery managerem ve společnosti Siemens IT Solutions and Services, spol. s r.o. Dále je ve společnosti zodpovědný za přípravu a organizaci auditů na ISO 27001 a ISO 20000. V letech 2008-2010 pracoval jako softwarový architekt ve společnosti Siemens IT Solutions and Services se zaměřením na bezpečnost vyvíjených řešení. Je absolventem fakulty Informatiky a statistiky na Vysoké škole ekonomické v Praze.

Zora Říhová

Doc. Ing. Zora Říhová, CSc. vystudovala VŠE Praha, praktické zkušenosti získala jak na straně zákazníka služeb IT (např. vedoucí informatiky a organizace v Unipetrol, a.s., informační manažer ZSE a.s.), tak na straně dodavatele služeb IT (např. ředitel produktu SAP v PVT a.s.). V Siemens IT Solutions and Services, spol. s r.o. pracovala jako Senior Project Manager, kde vedla projekty implementace rozsáhlých informačních systémů a nyní se věnuje managementu kvality. Působí jako docent na VŠE Praha (fakulta informatiky a statistiky, katedra systémové analýzy), kde se věnuje systémovým aspektům hospodářské organizace, procesní problematice a projektovému řízení.

PROBLEMATIKA MATICOVÉ CERTIFIKACE NA ISO 27001

Příspěvek se zabývá problematikou maticové certifikace organizace na soulad s normou ISO/IEC 27001 a definicí výhod a úskalí tohoto přístupu k certifikaci. Cílem příspěvku je diskutovat podstatu maticové certifikace, její odůvodnění, průběh a dopady na organizaci auditu včetně časové a organizační náročnosti. Jsou analyzovány otázky průběhu procesů, možnosti věcného sladění mezi vybranými státy, analyzovány přístupy auditorů a oblasti zájmu auditorů.

Jozef Opálený

Ing. Jozef Opálený zastává pozici Finančního a IT ředitele v Mondi Štětí. Ve společnosti působí od roku 2008. Posledních 7 let pracoval jako Finanční ředitel v několika společnostech a odvětvích jako Danzer Bohemia-Dýhárna (výroba dýhy), Mubea (dodavatel komponentů pro automobilový průmysl) a Mondi (výroba papíru). Převzetí zodpovědnosti za IT oddělení ve významné společnosti patřící k Czech TOP100 je novou výzvou v jeho kariéře. Jozef získal vysokoškolské vzdělání na Fakultě ekonomiky a managementu Slovenské zemědělské univerzity. V České republice žije od roku 2000.

HAVARIJNÍ PLÁN ZÁKLADNÍ IT INFRASTRUKTURY JAKO NÁSTROJ PRO KLIDNÝ SPÁNEK AKCIONÁŘŮ

Zabezpečení dat je prioritní zodpovědnost managementu každé společnosti. Velká část výrobních kapacit v České republice se nachází v záplavové zóně. Zkušenost z povodní z roku 2002 má i společnost Mondi Štětí. Její sídlo se nachází jen několik málo kilometrů od soutoku Vltavy a Labe. I toto riziko stálo za rozhodnutím o investici do zabezpečení datového centra a dat, které jsou nepostradatelné pro chod celé společnosti. V současnosti probíhá další posun v oblasti zabezpečení a to nejen proti povodním, ale i jiným rizikům.

Ondřej Bos

Ondrej Bos graduated from the Faculty of Economics of the Technical University of Ostrava. He has worked at the department for security policy of the Ministry of the Interior of the Czech Republic since 2003. He focuses on crisis management, the economic aspects of crisis situations and security threats to the internal security of the state.

CERTAIN FUNDAMENTALS IN THE DRAFTING OF CRISIS DOCUMENTATION AND THE INFLUENCE OF CRISIS PLANNING ON THE OPERATIONS OF AN ORGANIZATION

There are a number of different definitions of a crisis plan. Act No. 240/200 Coll. on crisis management, for example, defines it as a "plan that contains a summary of crisis measures and processes for solving the crisis situation". Another definition describes a crisis plan as being a collection of documents containing descriptions and analyses of threats and a summary of steps to be taken, which has been drafted to ascertain an organisations preparedness to deal with crisis situations. But, how should these documents look in real life? What should they contain? And who should draft the plan and for what purpose? He will try to open these questions in this paper using his experience of being a crisis manager at a central body of the state administration. He believes that the recommendations given in the paper will be useful irrespective of the sector or industry in which a given organization operates.

Ondřej Bos

Ing. Ondřej Bos absolvoval Ekonomickou fakultu Vysoké školy báňské – Technické univerzity v Ostravě. Od roku 2003 pracuje na odboru bezpečnostní politiky Ministerstva vnitra ČR. Jeho profesní zaměření je zejména krizové řízení, ekonomické aspekty řešení krizových situací a bezpečnostní hrozby pro vnitřní bezpečnost státu.

NĚKTERÉ ZÁSADY ZPRACOVÁNÍ KRIZOVÉ DOKUMENTACE A VLIV KRIZOVÉHO PLÁNOVÁNÍ NA ZAJIŠTĚNÍ CHODU ORGANIZACE

Existuje řada definicí krizového plánu. Například zákon č. 240/2000 Sb., o krizovém řízení říká, že je to „plán, který obsahuje souhrn krizových opatření a postupů k řešení krizových situací". Další z obecných definicí popisuje krizový plán, mimo výše uvedené, také jako soubor dokumentů obsahující popis a analýzu hrozeb a souhrn postupů, které se zpracovávají k zajištění připravenosti na řešení krizových situací. Jak však má v praxi takový dokument vypadat, jaké jsou jeho náležitosti, kdo by jej měl zpracovávat a k jakému účelu? Tyto otázky se pokusí v příspěvku otevřít a využít při tom zkušenosti z pozice krizového manažera ústředního orgánu státní správy. Domnívá se, že doporučení, která budou dále zmíněna, jsou užitečná a přínosná bez ohledu na to, v jakém sektoru či odvětví organizace působí a čím se zabývá.

PANEL DISCUSSION – DATA LEAKAGE PREVENTION IN PRACTICE

Data leakage protection in technical terms is frequently focused on network prevention, perimeter and end-user devices. In reality the problem is much broader. A critical part of the project is understanding the business processes as well as typical end-user behavioral patterns. This means that the problem considerably exceeds the scope of IT and requires close cooperation from other business units. The involvement of "business" units is crucial to the success of the venture, because IT delivers technology and supports the process but does not furnish business logic. Moreover, in the IT area actual deployment of technology is only one of the pillars of effective data protection. The panel will concentrate on practical experience from Czech projects.

TOMÁŠ FILIP

Tomáš Filip has focused on IT Security for the past 12 years: first at the Czech National Bank, then at Plzeňský Prazdroj and SABMiller, and for the last three years at Česká pojišťovna as Manager of IT Security and concurrently as Global Security Team Leader at Generali Group – Europe. In the last few years he has led several projects focused on IT Security, for example local compliance with regulatory requirements (SOX), security monitoring, ensuring data integrity, user lifecycle management, segregation of duties at SAP, fraud prevention etc.

TOMÁŠ MATOUŠEK

Tomáš Matoušek studied at the University of Economics in Prague. He is also a graduate of the University of Pittsburgh in the USA. He was appointed CEO and Chairman of the Board at Penzijní fond České pojišťovny in 2008. Previously he worked at Komerční banka and GE Money Bank. He is married and has a four year old son. His hobbies include golf, music, literature and travel.

ZDENĚK KAPLAN

Zdeněk Kaplan graduated from the Faculty of Mathematics and Physics at Charles University, in Prague and the University of Economics, Prague. He then worked for state security agencies, particularly in information security. He was later the Director for Security at APP. In 1997 Zdeněk jointly set up Data Security Management magazine, where he remains a member of the management committee. Between 1998 and 2003 he held various positions at ČSOB, and was then Executive Director for Company Services and Solutions Development at Telefónica O2. He is currently employed at Česká pojišťovna.

PANELOVÁ DISKUSE – PREVENCE ÚNIKU DAT V PRAXI

Prevence úniku dat se v technickém slova smyslu často soustřeďuje na prevenci na síťové vrstvě, perimetru a koncových zařízeních. Ve skutečnosti je problém mnohem širší. Kritickou části prevence je pochopení obchodních procesů a typických vzorců chování uživatelů. To znamená, že řešení této úlohy významně přesahuje rámec IT a vyžaduje úzké zapojení ostatních útvarů společnosti. Zejména zapojení „business" útvarů je alfou a omegou úspěšné implementace, neboť IT primárně dodává technologii/nástroj, podporu procesů, nikoliv business logiku. Také v IT oblasti je faktické nasazení technologie na vybrané prvky infrastruktury pouze jedním z pilířů efektivní ochrany dat. Panelová diskuse se bude soustředit na praktické zkušenosti z projektů v českém prostředí.

TOMÁŠ FILIP

Ing. Tomáš Filip se zabývá problematikou IT bezpečnosti již 12 let, nejprve v České národní bance, následně Plzeňském Prazdroji a SABMiller a nyní již 3 roky v České pojišťovně na pozici ředitel odboru bezpečnosti IT a zároveň jako Global Security Team Leader v evropské Generali Group. V posledních letech vedl mnoho projektů souvisejících s IT bezpečností např. zajištění lokálního soulad s legislativou (SOX), bezpečnostní monitoring, zabezpečení integrity dat, řízení životního cyklu uživatelů, oddělení neslučitelných funkcí (SOD) v SAP, prevence fradu atd.

TOMÁŠ MATOUŠEK

Ing. Tomáš Matoušek, MBA vystudoval VŠE v Praze. Je také absolventem University of Pittsburgh v USA. Od roku 2008 zastává pozici generálního ředitele a předsedy představenstva Penzijního fondu České pojišťovny a.s. V minulosti působil v Komerční bance a GE Money Bank. Je ženatý a má čtyřletého syna. Mezi jeho záliby patří především golf, hudba, literatura a cestování.

ZDENĚK KAPLAN

RNDr. Ing. Zdeněk Kaplan absolvoval MFF UK a VŠE v Praze. Působil v bezpečnostních složkách státu, zejména v oblasti informační bezpečnosti. Později také jako ředitel pro bezpečnost ve společnosti APP. V roce 1997 spoluzaložil časopis Data Security Management, jehož je dodnes členem řídícího výboru. V letech 1998 až 2003 působil v různých pozicích v ČSOB; do roku 2008 na pozici výkonný ředitel pro rozvoj firemních služeb a řešení v Telefónica O2. Aktuálně je zaměstnán v České pojišťovně.

EUGENE SCHULTZ

Eugene Schultz, CISM, CISSP, is the Chief Technology Officer at Emagined Security, an information security consultancy based in San Carlos, California. He is the author/co-author of five books and over 120 published papers. Gene was the Editor-in-Chief of "Computers and Security" from 2002-2007, is currently on the editorial board for this journal, and is an associate editor of "Network Security". He is also a SANS instructor, member of the SANS NewsBites editorial board, co-author of the 2005 and 2006 Certified Information Security Manager preparation materials, and is on the technical advisory board of three companies. Gene has previously managed an information security practice as well as a national incident response team. He has also been professor of computer science at several universities and is retired from the University of California at Berkeley. A Distinguished Fellow of the Information Systems Security Association (ISSA), Gene has also been named to the ISSA Hall of Fame and has received ISSA's Professional Achievement and Honor Roll Awards. While at Lawrence Livermore National Laboratory he founded and managed the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC). He is also a co-founder of FIRST, the Forum of Incident Response and Security Teams. He is currently a member of the accreditation board of the Institute of Information Security Professionals (IISP). Dr. Schultz has provided expert testimony before committees within the U.S. Senate and House of Representatives on various security-related issues, and has served as an expert witness in legal cases.

THE MOST COMMON MISTAKES IN INCIDENT RESPONSE

Security-related incidents have become much more complex, costly and resource-demanding over time, as shown by the Titan Rain, Aurora, Night Dragon and other highly successful and prolonged attacks in which attackers gained control of a myriad of computing systems and stole a huge amount of personal and proprietary information. Responding optimally to incidents, especially incidents that have the most potential impact upon an organization, has thus become a necessity. Yet many organizations continue to repeatedly make the same mistakes in the incident handling process. Mistakes can easily lead to response efforts being inefficient and ineffective, resulting in all kinds of negative consequences, including (but by no means limited to) longer incident durations and costly legal problems. This presentation focuses upon the most common mistakes made in handling incidents, the possible consequences, and the potential solutions.

PETR HANÁČEK

Petr Hanáček is an Associate Professor at the Faculty of Information Technology, at the Brno University of Technology. He has been working in the fields of information system security, risk analysis, applied cryptography, and electronic payment systems for more than ten years. He is an independent consultant in this area.

PETR ŠVENDA

Petr Švenda works as an Assistant Professor at Masaryk University, Brno, focusing on the design of cryptographic protocols for wireless sensor networks, cryptographic smart card security, and privacy protection in information technology. He is the author or co-author of more than 15 peer-reviewed publications and participated consultation and development work for academic, governmental and industrial organizations in both the Czech Republic and abroad.

CRYPTOGRAPHY FOR (PARTIALLY) COMPROMISED SENSOR NETWORKS

Wireless sensor networks are not just another technology, but also exhibit new and complex problems from the security perspective. The majority of the existing security approaches are unsuitable or even impossible to deploy due to the combination of decentralized tasks with high numbers of energy and computational-limited nodes positioned, typically, out of our permanent physical control. Non-conventional and/or novel security techniques are to be considered for situations where a partial network compromise is to be expected.

EUGENE SCHULTZ

Dr. Eugene Schultz, CISM, CISSP, je CTO (Chief Technology Officer) u Emagined Security – konzultační společnosti z kalifornského města San Carlos působící v oblasti informační bezpečnosti. Je autorem či spoluautorem pěti knih a více než 120 odborných článků. V letech 2002 až 2007 byl šéfredaktorem časopisu „Computers and Security", v současnosti je členem redakční rady tohoto časopisu a zástupcem šéfredaktora dalšího časopisu „Network Security". Je rovněž instruktorem výcvikového a školícího institutu SANS (SysAdmin, Audit, Networking and Security), člen redakční rady jeho zpravodaje SANS NewsBites, spoluautor materiálů z let 2005 a 2006 pro přípravu na titul Certified Information Security Manager a člen technických poradních orgánů tří společností. V minulosti se zabýval poskytováním konzultačních služeb v oblasti bezpečnosti IT, a to i v rámci národního CERTu. Působí jako profesor počítačové vědy na několika univerzitách; jeho mateřskou univerzitou byla University of California, Berkeley. Jako čestný člen ISSA (Information Systems Security Association) byl uveden do síně slávy této asociace a získal ISSA's Professional Achievement and Honor Roll Awards. V Lawrence Livermore National Laboratory založil a vedl oddělení U.S. Department of Energy's Computer Incident Advisory Capability (CIAC). Je rovněž spoluzakladatel fóra FIRST (Forum of Incident Response and Security Teams). V současnosti je členem akreditačního výboru IISP (Institute of Information Security Professionals). Dr. Schultz je v USA využíván senátními i parlamentními výbory jako bezpečnostní expert, kde poskytuje odborné posudky v různých právních kauzách.

NEJČASTĚJŠÍ CHYBY PŘI REAKCÍCH NA INCIDENTY

Incidenty vztahující se k bezpečnosti jsou stále komplexnější, nákladnější a vyžadují stále více zdrojů. To ukázaly mimo jiné i úspěšné a déledobější útoky, např. Titan Rain, Aurora, Night Dragon, ve kterých útočníci získaly kontrolu nad velkým počtem informačních systémů a odcizili velké množství osobních údajů a důvěrných informací. Optimální reakce na incidenty, obzvláště na incidenty, které mají zásadní dopad na organizaci, se tak stává nezbytností. Mnoho organizací však při řešení incidentů opakuje stále stejné chyby. Tyto chyby mohou vést k tomu, že reakce na incident je neúčinná a neefektivní, což má celou řadu negativních dopadů, včetně, mimo jiné, delšího trvání incidentu a nákladných právních problémů. Prezentace se soustředí na nejběžnější chyby v reakcích na incidenty, dopady a potenciální řešení.

PETR HANÁČEK

Doc. Dr. Ing. Petr Hanáček je docentem na Fakultě informačních technologií VUT v Brně. Zabývá se více než deset let bezpečností informačních systémů, analýzou rizik, aplikovanou kryptografií, elektronickými platebními systémy, bezdrátovými sítěmi. Je nezávislý konzultant v této oblasti.

PETR ŠVENDA

RNDr. Petr Švenda, Ph.D. působí jako odborný asistent na Masarykově univerzitě, věnuje se výzkumu v oblasti návrhu protokolů pro bezdrátové senzorové sítě, bezpečnosti kryptografických čipových karet a ochraně informačního soukromí. Je autorem a spoluatorem více než 15 recenzovaných publikací. Podílel se na konzultacích a vývoji pro akademické, státní i průmyslové organizace v ČR i zahraničí.

KRYPTOGRAFIE PRO (ČÁSTEČNĚ) KOMPROMITOVANÉ SENSOROVÉ SÍTĚ

Bezdrátové senzorové sítě nejsou jen relativně čerstvou technologií, ale přinášejí zároveň i nové a komplexní problémy z bezpečnostního hlediska. Možnost použití běžných bezpečnostních postupů je výrazně snížena díky kombinaci decentralizovaných úloh s vysokým počtem energeticky a výpočetně omezených uzlů, navíc umístěných typicky v prostředí mimo fyzickou kontrolu vlastníka. Budou předvedeny vybrané nové nebo nekonvenčně použité bezpečnostní přístupy pro prostředí, ve kterém je nutné předpokládat trvalou kompromitaci části uzlů v síti.

DANILO GLIGOROSKI

Danilo Gligoroski is a professor of Information Security and Cryptography at the Department of Telematics, at the Norwegian University of Science and Technology – Trondheim, Norway. He received his Ph.D. at the Cyril and Methodius' University of Skopje in 1997 in the field of Computer Science. His research interests are Cryptography, Computer Security, Discrete algorithms, Information Theory and Coding.

BOTTLENECKS IN APPLIED DIGITAL SIGNATURES SCHEMES

A classical way for allocating bottlenecks in digital signature schemes is to measure the efficiency of the signing and the verification parts. For example, if the process is such that the company server receives a lot of signed transactions from individual clients and have to verify every signature, then an obvious choice would be to use a signature schneme that can do faster verification, while the individual signatures can be produced in a somewhat slower manner (RSA signatures with small public exponents have that property). On the other hand, if a company needs to send a bulk of signed invoices to hundreds of thousands (or millions) of users, then the signing speed is important (elliptical curve signature schemes are usually faster in signing than RSA or DSA signature schemes). However, with the advent of new standards and new technological advancements in medical equipment, especially in real-time teleradiology and mammography, the issue of whether the signing or verification is fast or slow does not at all influence the efficiency of the overall signature scheme. There, the speed of the used hash function is the real bottleneck, taking even up to 99.7% of the time spent on signing or verification. In his talk he will demonstrate several use case scenarios with several typical average sizes, starting from 16 KB (typical PDF files in financial transactions) up to files with a size of 160 MB – images obtained by mammographic scanners. Additionally, from the same perspective He will gives a what-if analysis that includes several new cryptographic hash functions from the ongoing SHA-3 competition.

RADIM POLČÁK

Radim Polčák is the head of the Institute of Law and Technology at the Law Faculty at Masaryk University. He teaches and publishes in ICT law and legal theory at Masaryk University and regularly lectures at law schools in the Czech Republic, Austria, Germany, UK, Netherlands and Hungary. In addition, Dr. Polčak is the general chair of the Cyberspace annual international symposium; editor-in-chief of the Masaryk University Journal of Law and Technology; editor-in-chief of the Review of Law and Technology (Revue pro právo a technologie) and a member of the editorial boards and governing bodies of ICT-law focused scientific journals and international conferences in the Czech Republic, UK, Germany and Hungary. He is a panellist at the .eu ADR arbitration court, a member of the Appellate Tribunal of the Czech Ministry of Transport and a member of various governmental and scientific expert and advisory bodies. He also acts as an ad-hoc expert advisor to Czech, Slovak, Austrian and UK law firms, public bodies and businesses in the field of ICT law, IP law and energy law.

WIGGUM IN CYBERSPACE: LEGAL ISSUES IN CZECH AND EU CYBERSECURITY

Public protection against cyber attacks represents a relatively new set of challenges for the legal system. It combines issues directly arising from the fundamentals of constitutional law with highly specific technical problems. The paper discusses general issues of the legitimacy of state interventions in securing cyberspace and outlines the basic legal problems that have to be dealt with by EU and Czech lawmakers. In particular, the paper focuses on information duties, on the competences of state authorities and on the sensitive issue of blocking, as well as on recent developments in data retention duties.

DANILO GLIGOROSKI

Danilo Gligoroski, Ph.D. je profesorem informační bezpečnosti a kryptografie na Katedře telematiky Norské univerzity věd a technologií v Trondheimu. Získal Ph.D. v informatice na Univerzitě sv. Cyrila a Metoděje ve Skopje v roce 1997. Jeho oblastmi výzkumu jsou kryptografie, počítačová bezpečnost, diskrétní algoritmy, teorie informace a kódování.

OMEZENÍ V APLIKOVANÝCH SCHÉMATECH DIGITÁLNÍCH PODPISŮ

Klasickou cestou pro zjišťování omezení schémat digitálního podpisu je měření efektivity podpisových a verifikačních částí. Např. pokud je proces takový, že firemní server přijímá spoustu podepsaných transakcí od jednotlivých klientů a musí ověřit každý podpis, tak je jednoznačnou volbou schéma, které dělá ověření rychleji než podpis, zatímco jednotlivé podpisy jsou vytvářeny o něco pomaleji (podpisy RSA s malým veřejným exponentem jsou vhodnou ilustrací). Naopak pokud firma potřebuje poslat statisíce či milióny podepsaných faktur zákazníkům, pak je důležitá rychlost podpisu (zde schémata pro eliptické křivky jsou výhodným řešením). Ale s příchodem nových standardů a technologických změn v oblasti zdravotnických zařízení, zejména v teleradiologii a mamografii v reálném čase, ovlivní rychlost či pomalost podpisu nebo verifikace celkovou efektivitu podpisového schématu jen minimálně. Zde je ve skutečnosti hlavním omezením práce hašovací funkce, která může zabrat až 99,7 % času potřebného pro podpis nebo jeho ověření. Ve svém příspěvku poukáže na několik ukázkových situací s několika typickými velikostmi zpracovávaných dat, počínaje 16 KB (obvyklá velikost PDF pro finanční transakce) až po soubory o velikosti 160 MB (obrázky získané mamografem). Dále ze stejné Perspektivy proberu „co když" možnosti zapojení několika nových hašovacích funkcí z probíhajícího výběru SHA-3.

RADIM POLČÁK

JUDr. Radim Polčák, Ph.D. je vedoucím Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Vyučuje a publikuje v oboru práva ICT a právní teorie na Právnické fakultě Masarykovy univerzity a jako host působí na právnických vysokých školách v České republice, Rakousku, Německu, Spojeném království, Nizozemsku a Maďarsku. Dr. Polčák je předsedou organizačního výboru mezinárodního sympozia Cyberspace, šéfredaktorem časopisu Masaryk University Journal of Law and Technology, šéfredaktorem časopisu Revue pro právo a technologie a členem redakčních a řídících orgánů odborných časopisů a konferencí v České republice, Spojeném království, Německu a Maďarsku. Je rovněž rozhodcem rozhodčího soudu .eu ADR, členem rozkladové komise Ministra dopravy ČR a členem vládních a vědeckých odborných a poradních sborů. Jako ad-hoc expert v oboru práva ICT a energetického práva spolupracuje s právními kancelářemi, vládními a soukromými institucemi z ČR, Slovenska, Rakouska a Spojeného království.

VYGUM V KYBERPROSTORU: PRÁVNÍ OTÁZKY ČESKÉ A EVROPSKÉ KYBERNETICKÉ BEZPEČNOSTI

Veřejná ochrana před kybernetickými útoky představuje pro právo doposud neznámou výzvu. Spojuje v sobě totiž faktory dotýkající se samotných základů ústavního systému se specifickými technickými problémy. Příspěvek se zaměří na diskusi obecné otázky legitimity státu při zajišťování bezpečnosti kyberprostoru a nastíní základní právní problémy, s nimiž se musí potýkat evropský a český právotvůrce. Vedle informačních povinností, kompetencí správních orgánů a citlivé problematiky nuceného odpojování, bude zvláštní pozornost věnována též aktuálnímu právnímu vývoji problematiky povinného uchovávání provozních údajů.

Pavel Minařík

Pavel Minařík received his masters' degree in computer science in 2005 from the Faculty of Informatics of Masaryk University in Brno. He currently works as the Chief Technology Officer at AdvaICT. He is the main architect of AdvaICT's ADS (Anomaly Detection System) and outgoing products. Pavel's main focus is network traffic analysis and anomaly detection. He has participated in several research projects (mainly for the U.S. and Czech Armies) as a senior researcher of the Institute of Computer Science of Masaryk University. He is a co-author of two technology transfers (2010) from the University and co-author of 7 published research papers in the field of network behavior analysis (2007-2009).

NETWORK MONITORING – TOOL FOR DETECTING AND AVOIDING INCIDENT

The complexity of IT infrastructure is growing continuously. More products are being incorporated and more services are being used. Enterprises rely on computer network and information technology since their primary processes completely depend on the IT department or it's outsourcing partners. Malware infection or data loss a single computer might be troublesome. A successful attack on the core infrastructure, or client data loss, or malware infection of the whole network is a disaster. There are widely used methods to stop network attacks and malware from spreading based on signatures (intrusion detection system) in combination with host protection (antivirus, anti spyware). However, the latest results show that these methods are not bulletproof and that we need to focus on network traffic and its monitoring and analysis. We present a network-centric approach to the detection and prevention of incidents on computer networks with a focus on security. This approach is based on the detailed measuring and monitoring of computer networks using flow data. Methods based on flow data processing are unique in their usability, scalability and performance while there is no need for a deep understanding of the topology of target networks and no need for software installation or configuration changes. The proposed approach is called Network Behavior Analysis (NBA) and will be illustrated on a series of case studies from network traffic audits and analyses performed by AdvaICT during the last year.

Matthew Pemble

Matthew Pemble is a strategic and operations manager, with specialities in information security architecture, compliance and incident response. Experienced within numerous government, business and infrastructure sectors, he is currently working at a small specialist consultancy, Idrach Ltd. Mathew previously worked as a security strategist at the Royal Bank of Scotland. He holds various security and other certifications (e.g., CISSP or CFE).

PRACTICAL MODELS FOR INCIDENT MANAGEMENT

Information Security Incident Management is a complex process that is greatly assisted by having a structured framework to guide managers and technicians. This paper presents both a functional framework, suitable as a base for the development of local ISO 27001/PCI-DSS 2.0 compliant processes, and a timeline model, suitable for business analyses and loss/cost modelling.

Pavel Minařík

RNDr. Pavel Minařík absolvoval v roce 2005 Fakultu informatiky Masarykovy univerzity v Brně. V současné době pracuje jako technologický ředitel ve společnosti AdvaICT. Je hlavním architektem platformy ADS (Anomaly Detection System) a odvozených produktů společnosti AdvaICT. Mezi jeho hlavní oblasti zájmu patří analýza provozu na síti a detekce anomálií. Účastnil se řady výzkumných projektů (převážně pro americkou a českou armádu) jako výzkumný pracovník Ústavu výpočetní techniky Masarykovy univerzity. Je spoluautorem dvou transferů výsledků výzkumu a vývoje do praxe a spoluautorem sedmi výzkumných článků v oblasti behaviorální analýzy chování na síti (v letech 2007-2009).

MONITORING SÍTĚ – PROSTŘEDEK ODHALOVÁNÍ A PREVENCE INCIDENTŮ

Složitost IT infrastruktury stále vzrůstá. Jsou nasazovány nové produkty a využívány nové služby. Organizace spoléhají na počítačové sítě a informační technologie, neboť jejich primární procesy zcela závisí na IT oddělení nebo outsourcingových partnerech. Virus nebo ztráta dat na jedné stanici je nepříjemná. Úspěšný útok na IT infrastrukturu, ztráta dat klientů nebo virová epidemie celé sítě je katastrofa. Metody založené na signaturách sloužící k zastavení útoků na síti nebo šíření virů jsou v kombinaci s ochranou klientských stanic antiviry nebo antispyware obecně rozšířené a používané. V několika posledních letech se však ukazuje, že ochrana založený na tomto přístupu není dostatečná a že je nutné se soustředit na provoz datové sítě, jeho monitoring a analýzu. Metody pro odhalování a prevenci incidentů se zaměřením na bezpečnost založené na monitorování datové sítě jsou tématem této přednášky. Přístup je založený na detailním měření a monitorování datových toků v síti vykazuje rychlou použitelnost, vysokou škálovatelnost a výkon bez nutnosti znalosti topologie monitorované sítě, instalace software na jednotlivé stanice nebo změn konfigurace. Prezentované metody jsou souhrnně označovány jako Network Behavior Analysis (NBA) a budou ilustrovány na řadě případových studií z auditů a analýz provozu datové sítě provedených společností AdvaICT v průběhu minulého roku.

Matthew Pemble

Matthew Pemble je manager pro strategii a provoz, specializuje se na architekturu informační bezpečnosti, soulad a na procesy řízení incidentů. Má zkušenosti z mnoha vládních, privátních i infrastrukturních organizací. V současné době pracuje pro malou specializovanou konzultační společnost Idrach Ltd. Dříve pracoval jako bezpečnostní stratég pro Royal Bank of Scotland. Je držitelem řady certifikací (např. CISSP nebo CFE).

PRAKTICKÉ UKÁZKY ŘÍZENÍ INCIDENTŮ

Řízení incident týkajících se informační bezpečnosti je složitý proces, který významně zefektivní vytvoření strukturovaného rámce, který manažery a techniky celým procesem provádí. Tento příspěvek prezentuje funkční rámec, který je vhodný jako základ pro vytvoření vlastního procesu, který bude v souladu s procesy ISO 27000/PCI-DSS 2.0. Zároveň poskytuje časový model vhodný pro analýzu a modelování ztrát a nákladů.

Registration Fee / Konferenční Poplatek

The registration fee includes the two-day conference ticket, conference materials, DVD, coffee breaks, lunches and an evening party.

Poplatek zahrnuje kompletní účastnické materiály, vstup na oba dny konference, DVD, občerstvení, obědy a večerní raut.

For DSM Subscribers / Pro předplatitele DSM		including VAT	bez DPH	včetně DPH
Early bird up to / do	**31. 3. 2011**	**EUR 654**	**11 990,- Kč**	**14 388,- Kč**
Registration up to / do	**30. 4. 2011**	**EUR 763**	**13 990,- Kč**	**16 788,- Kč**
Registration after / po	**1. 5. 2011**	**EUR 872**	**15 990,- Kč**	**19 188,- Kč**

Other Participants / Ostatní účastníci		including VAT	bez DPH	včetně DPH
Early bird up to / do	**31. 3. 2011**	**EUR 981**	**17 990,- Kč**	**21 588,- Kč**
Registration up to / do	**30. 4. 2011**	**EUR 1 308**	**23 990,- Kč**	**28 788,- Kč**
Registration after / po	**1. 5. 2011**	**EUR 1 636**	**29 990,- Kč**	**35 988,- Kč**

Special Offer / Speciální Nabídka

An annual subscription of DSM magazine as a bonus added to the registration fee
Roční předplatné časopisu DSM jako bonus ke konferenčnímu poplatku

	EUR 927	**16 990,- Kč**	**20 388,- Kč**

Documentation / Dokumentace
In the event that you cannot attend the conference but would like to receive the related materials, you can purchase a complete set of all the presentations.

Pokud nemáte možnost se konference zúčastnit, ale přesto byste rádi získali materiály z jejího průběhu, můžete si zakoupit kompletní účastnické materiály všech přednášek.

Price / Cena	**EUR 163**	**2 990,- Kč**	**3 588,- Kč**

Payment Details / Detaily Placení

You can pay via bank transfer. We will issue your attendance confirmation and your invoice after your application has been registered. All fees are due at least one day before the beginning of the conference. Cash payment on the first conference day is possible only if agreed with the organizers in advance.

Platit můžete bankovním převodem nebo zálohovou fakturou. Po obdržení platby na náš účet Vám vystavíme daňový doklad a zašleme potvrzení účasti. Abychom Vám mohli zajistit účast, všechny poplatky musí být uhrazeny na účet organizátora nejpozději jeden den před konáním konference. Platba v den začátku konference je možná pouze po předchozí dohodě v hotovosti.

Cancellation Policy / Stornovací Podmínky

For cancellation before April 26, 2011 we will charge you a CZK 1 000 manipulation fee + 20 % VAT. For cancellations after this date you will be liable for 50 % of the conference fee + 20 % VAT, for cancellations within one week before the summit, payments will be required in full + 20 % VAT. Substitutions are possible without any additional fee.

Do 26. dubna 2011 je při zrušení účtován manipulační poplatek 1 000,- Kč + DPH 20 %. Po tomto datu je stornovací poplatek 50 % konferenčního poplatku + DPH 20 % a jeden týden před konáním konference je to 100 % + DPH 20 %. Kdykoliv máte možnost nahradit svoji účast jinou osobou bez dalšího poplatku.

Registration Form / Registrační Formulář

Please complete the registration form and return via fax, e-mail or post to:
Vyplněný registrační formulář zašlete faxem, e-mailem nebo poštou na adresu:

DSM – data security management, TATE International, s.r.o., Hořejší nábřeží 21, 150 00 Praha 5,
Telephone: / Telefon: +420 257 920 319-20, **Fax: +420 257 313 695, e-mail: dsm@dsm.tate.cz**
Alternatively you can register on-line at: / nebo využijte možnosti registrace na: **www.dsm.tate.cz/is2**

Company / Společnost ..... Industry Sector / Oblast podnikání .....

IČ ..... DIČ .....

Surname / Příjmení ..... First Name / Jméno ..... Degree / Titul .....

Position / Funkce ..... Telephone / Telefon .....

E-mail ..... Mobile ..... Fax .....

Address / Korespondenční adresa .....

.....

Postcode / PSČ ..... Country / Stát .....

Invoice Address / Fakturační adresa .....

.....

Postcode / PSČ ..... Country / Stát .....

DSM Subscriber: / Předplatitel DSM: ❑ no/ne ❑ yes/ano Subscriber number / předplatitelské číslo .....

Number of Employees / Počet zaměstnanců ❑<25 ❑26-50 ❑51-100 ❑101-200 ❑201-500 ❑501-1000 ❑>1000

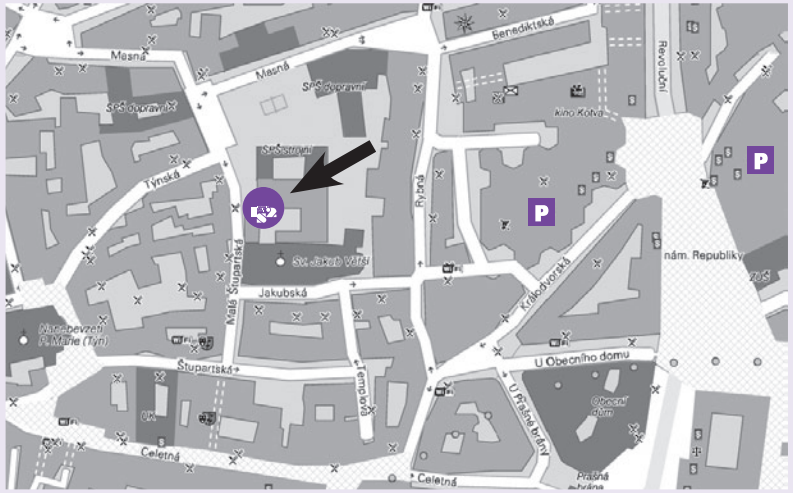
Proforma invoice request / Požaduji zálohovou fakturu yes / no ano / ne

I confirm that the registration fee CZK ..... Kč including VAT was paid to the bank account of TATE International, number 574171183/0300 at ČSOB a.s., Prague 1, ID: 25148125, Tax ID: CZ25148125.

Potvrzuji, že účastnický poplatek ve výši ..... Kč včetně DPH byl poukázán na účet TATE International, číslo 574171183/0300 u ČSOB a.s., Praha 1, IČ: 25148125, DIČ: CZ25148125.

Date / Dne ..... from bank account number / z čísla účtu .....

Date / Datum ..... Signature / Podpis .....



Conference Venue / Místo konání

The Minorite Monastery of St. James, Malá Štupartská 635/6, Praha 1

- Tram stop: Náměstí Republiky, tram Nr. 5, 8, 14, 26
- Subway B route: Náměstí Republiky

Klášter minoritů sv. Jakuba, Malá Štupartská 635/6, Praha 1

- zastávka tramvaje: Náměstí Republiky, tramvaj číslo 5, 8, 14, 26
- metro trasa B: stanice Náměstí Republiky

Loc: 50°5'18.826"N, 14°25'28.348"E

Parking / Parkování

As the monastery is located directly in a Heritage Reservation zone, the following parking spaces should be used: The underground car parks at the Kotva and Palladium shopping centres or the Hotel Marriott.

Vzhledem k poloze kláštera, který se nachází přímo v památkové rezervaci, je nutno využít následujících parkovišť: Podzemní garáže OD Kotva, OC Palladium, Hotel Marriott.

Hotel Bookings / Rezervace Ubytování

We can arrange reservations for participants from May 25th to May 26th 2011 for a special rate. Should you be interested, please, contact Mrs. Katerina Pochova (Senator Travel), e-mail: Katerina.Pochova@senatortravel.eu, phone number +420 267 090 545. Please quote the purpose of the stay: accommodation during the IS2 conference.

Pro účastníky konference můžeme rezervovat od 25. května do 26. května 2011 ubytování za speciální cenu. V případě zájmu kontaktujte, prosím, paní Kateřinu Pochovou (Senator Travel) na tel. čísle +420 267 090 545, e-mail: Katerina.Pochova@senatortravel.eu. Uveďte účel – ubytování na konferenci IS2.

Hotels / Hotely

Our hotels are located 5-10 mins walk from the Minorite Monastery of St. James.
Vzdálenost hotelů od Kláštera minoritů sv. Jakuba je 5-10 min. pěšky.

Hotel HAŠTAL* – Haštalská 1077/16, Praha 1**
single room / jednolůžkový pokoj, double room / dvoulůžkový pokoj 89 EUR/2 225,- Kč
www.hotelhastalprague.com

Hotel PÁV BEST WESTERN* – Křemencova 13, Praha 1**
single room / jednolůžkový pokoj, double room / dvoulůžkový pokoj 77 EUR/2 040,- Kč
www.hotel-pav.cz

Klášter minoritů sv. Jakuba

Na pražském Starém Městě, na rohu ulic Štupartské a Jakubské, se nachází starodávný kostel svatého Jakuba, zmiňovaný již od dvanáctého století. Chrám i klášter náleží mezi nejzajímavější pamětihodnosti Prahy, kde se snoubí architektonické styly od gotiky až po vrcholné baroko. V tomto klášteře se konala v roce 1311 (nebo 1309) korunovační hostina Jana Lucemburského a Elišky Přemyslovny. Pražský hrad byl tehdy v sutinách a nezbývalo nic jiného, než pro tuto slavnost zvolit jinou pražskou stavbu. Kolem roku 1337 se v klášteře uskutečnila druhá svatební hostina Jana Lucemburského s královnou Betricií. Později zde působil i Karel IV., který odtud, jako markrabě moravský, vydal svá privilegia Pražanům. Zároveň byl chrám sv. Jakuba roku 1374 za jeho přítomnosti slavnostně posvěcen arcibiskupem Janem Očkem z Vlašimi. Ve své konečné podobě náležel chrám sv. Jakuba k největším pražským svatyním a byl místem mnoha slavnostních obřadů, nejenom sakrálních a funerálních (v roce 1378 zde bylo na skvostném katafalku vystaveno tělo Karla IV.), ale i jevištěm velmi významných událostí politického i náboženského rázu (např. roku 1392 se zde konalo zasedání zemského soudu, v letech 1411 a 1414 se tu odbývalo jednání církevních úřadů se straníky Husovými).
Další zajímavostí na zdejších prostorech jsou překrásná gotická sklepení, která se jako jediná zachovala při velkém požáru v 17. století. Zde byla v té době uschována také soška Panny Marie, která je jinak uložena v zasklené skříni v kostele na hlavním oltáři již od 15. století. O této sošce se tradovalo, že má zázračnou moc, a proto jí lidé z celého království přinášeli velmi cenné dary a častokrát se tak stávalo, že byla socha šperky a perlami celá ověšena.

The Minorite Monastery of St. James

The ancient church of St. James, first mentioned in records in the 12th century, is situated in the Old Town of Prague, on the corner of Štupartská and Jakubská streets. Both the church and the monastery are amongst the most interesting sights of Prague, combining a blend of different architectural styles, starting with Gothic and culminating with High Baroque. These historical buildings had been closed to the public until recently, except for educational and musical activities.
In 1311 (or 1309) the coronation banquet of John of Luxembourg and Elizabeth Premyslid took place at the monastery. Prague Castle was undergoing construction work at this time, so there was no option but to choose another site in the city for the celebration. Around 1337 the monastery also hosted the second wedding reception of John of Luxembourg, this time for his marriage to Queen Beatrice. Charles IV later exercised his office as the Margrave of Moravia whilst based here, dispensing privileges to the people of Prague. He was also present when the church of St. James was consecrated in 1374 by Archbishop Jan Očko of Vlašim. In its current appearance, the church of St. James was among the largest religious sites in Prague and has been the location for many celebrations, not just for church festivals and funerals (in 1378 the body of Charles IV was laid out here on a magnificent bier), but also for important events of a political and religious nature (for example, in 1392 the provincial court met here and in 1411 and 1414 it was the site where church authorities negotiated with Hussite representatives).
The splendid Gothic cellars, which were the only original part of the church not destroyed by the great fire in the 17th century, are another place of interest. A statue of the Virgin Mary kept in a glass cabinet at the main altar of the church since the 15th century was preserved by being taken to the cellars. The statue was said to have had miraculous powers and people from around the kingdom would bring valuable gifts, often covering it entirely with jewels and pearls.

Main conference organizers / Hlavní pořadatel konference

TATE International, s.r.o.,
vydavatel časopisu DSM – data security management

In co-operation with / Ve spolupráci s

Cacio

ISACA
Trust in, and value from, information systems
Czech Republic Chapter

Address / Adresa

DSM – data security management
TATE International, s.r.o.
Hořejší nábřeží 21
150 00 Praha 5

tel.: +420 257 920 319-20
fax: +420 257 313 695
e-mail: dsm@dsm.tate.cz

http://www.dsm.tate.cz

Gold Partner / Zlatý partner

Special Partners / Speciální partneři

ANECT

ERNST & YOUNG
Quality In Everything We Do

KPMG

nextiraOne
THE COMMUNICATIONS EXPERTS

T-Systems