4th Cyber Security & 16th International ITTE Conference
2nd edition of Future Cyber Security & Defence Conference
11th edition of Advanced Technologies in Defence & Security Exhibition

INTERNATIONAL CONFERENCE

FUTURE CRISES

Focused on developing international cooperation in cyber security

UNIQUE GATHERING PLACE FOR EXPERTS

15 – 17 October 2014

PRAGUE, CZECH REPUBLIC

www.natoexhibition.org

Přiznávám se, že nejsem odborníkem na vojenskou strategii, taktiku či pohyb na bitevním poli. Poslední zkušenost jsem získal před více než čtvrtstoletím během roční vojenské služby. Nicméně i přes zanedbatelnou bojovou zkušenost tuším, že současný kyberprostor je v mnohém podobný bitevnímu poli.

Je složitý a zranitelný. Složitá jsou zařízení (jejich software je často sestaven ze stovek miliónů řádků zdrojového kódu), komplexní je i jejich propojení a uspořádání. A zranitelnost obvykle roste se složitostí.

Ovládnutý cíl se může stát nebezpečnou zbraní. To je principem botnetů i řady cílených útoků. Řízený subjekt uvnitř dobývaného objektu je pro útočníka mimořádně cenný.

Kyberprostor je vysoce mobilní. Mobilita zařízení, jejich počet a zranitelnosti činí kyberprostor málo přehledným.

Obrana obvodu chráněného objektu nestačí. Pohyb zranitelných zařízení z nechráněných oblastí do vnitřních objektů snižují účinnost ochrany perimetru.

Spektrum útoků i zbraní je velmi široké. Musíme očekávat cílené, chirurgicky přesné útoky i útoky vedené hrubou silou.

Uživatele postižené ransomwarem (kódem sloužícím k vydírání) můžeme přirovnat k válečným zajatcům. A boty (pěšáky botnetu) si můžeme představit jako zběhy, byť nevědomé.

I metody útoků se v mnoha fázích podobají. Po průzkumu terénu následuje příprava, vyzbrojení, přiblížení k cíli, proniknutí a vlastní akce, často řízená na dálku.

A mohli bychom pokračovat v hledání dále.

Jistě, přes četné podobnosti existují i určité rozdíly. Kyberprostor je velmi rozsáhlý. Už dnes se v něm nachází přes 13 miliard zařízení a jejich počet rychle roste. V kyberprostoru jsou útoky snadno opakovatelné, zbraně (a ostatně i cíle) prakticky neomezeně replikovatelné. Rychlost šíření útoku v kyberprostoru je mnohem vyšší než v poli. Snaha o destrukci cíle nebývá hlavní snahou útočníka. V kyberprostoru se většinou se bráníme pasivně. Připravíme se a čekáme. Poté, co útok odrazíme, čekáme na další. Asi bychom našli další odlišnosti.

Před zmíněné rozdíly bych zdůraznil jednu podstatnou podobnost.

Vzhledem ke složitosti prostředí a propracovaným zbraním útočníků nemůžeme očekávat, že nás útok nezasáhne a nepoškodí. Musíme si udržovat přehled, být připravení a akceschopní ve všech fázích – před útokem, kdy se snažíme snížit pravděpodobnost jeho úspěchu, během útoku, kdy se snažíme případný průnik zachytit a omezit jeho dopad, i po jeho ukončení, kdy se snažíme zacelit zranění a obnovit činnost.

Na tomto principu jsou postaveny moderní bezpečnostní technologie, chránící firemní informační systémy.

Vzhledem k tomu, že kyberprostor se v mnohém podobá bitevnímu poli, uvažuje řada odborníků o tom, zda by firmy neměly převzít při obraně sítě vojenské strategie a postupy (viz např. [1], [2]).

Věřím, že konference Future Crises může takové myšlenky rozvinout a přispět i k posílení obranyschopnosti podniků a snížit tak přirozené výhody, které dnes útočníci mají.

Ivo Němeček, acting general manager, Cisco Systems

I admit I am no expert when it comes to military strategy, tactics, or battlefield logistics. My last military experience dates back to my mandatory year with the Czech Army and is more than quarter of a century old. Despite my minor military experience, I believe that today's cyberspace is in many ways similar to a battlefield.

It's complicated and vulnerable. Devices are complicated (their software often consisting of millions of lines of source code), their layout and connectivity are often even more complicated.

A controlled target may become a dangerous weapon. That's the principle of botnets and targeted attacks. A controlled subject on the inside of an entity being attacked is very valuable for the attacker.

The cyber space is highly mobile. Mobility of devices, as well as their number and vulnerability make cyber space very difficult to understand.

A perimeter protection is no longer sufficient. Movement of vulnerable devices from unprotected areas into inside environment impairs the efficiency of perimeter protection.

The range of attacks and weapons available is very wide. We must expect targeted, surgically-accurate attacks, as well as brute force attacks.

Users subjected to ransomware may be likened to prisoners of war. Bots, the foot-soldiers of botnets, can be visualised as deserters, albeit unaware.

Methods of attack on the battlefield and in cyber space are also similar. After reconnaissance come preparation, armament, approach, penetration and the action itself, often remotely-controlled. And the parallels do not end here.

Still, there are some differences. The cyber space is very large. Already today, it contains 13 billion devices, and the number is growing fast. Cyber-attacks are easy to repeat, the weapons (and the targets) replicable without limits. Propagation rate of a cyber-attack is much higher than that on a battlefield. Destruction of target is often not the attacker's main objective. Cyber defence is usually passive. We prepare and we wait. After we push back an attack, we wait for the next one. Further differences could be found...

Despite the above differences, I would like to emphasize one important similarity.

Given the complexity of the environment and the sophistication of the attackers' weaponry, we can't expect not to be attacked or emerge intact when we are. We must maintain awareness, be prepared and in readiness at all times – before an attack, when we are trying to limit the probability of its success, during an attack, when we are trying to intercept the eventual penetration and limit its impact and after an attack, when we are trying to heal the wounds and re-establish operations.

This is the principle behind modern security technologies protecting enterprise information systems.

Given the similarities between the cyber space and the battlefield, many professionals are considering the use of military strategy and processes in protecting the enterprise cyber environment (see [1], [2]).

I hope the Future Crises Conference develops such thoughts and contributes to the defence of enterprises and organisations by limiting the natural advantages attackers have today.

Ivo Němeček, Acting General Manager, Cisco Systems

Reference
[1] Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D."Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
[2] Treat cyberspace like a battlefield, Michael Kassner
http://www.techrepublic.com/article/treat-cyberspace-like-a-battlefield/
[3] Addressing the Full Attack Continuum, Cisco White Paper
http://www.cisco.com/web/learning/le21/le34/assets/events/i/gartner_BDA_Whitepaper.pdf
[4] Cisco Annual Security Report
http://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html

Známé závislosti na vodě, potravinách, energii, postupně doplňujeme a zaměňujeme za závislost na technologiích, na fungování kybernetického světa. Závislými se ale nestáváme jenom my, jako fyzické či právnické osoby, závislým se stává celý náš způsob života, naše ekonomicko sociální hodnoty. Proto musí reprezentace společnosti diskutovat a stanovit, kde je hranice mezi svobodou jednotlivce a potřebou chránit zájmy a hodnoty společnosti jako celku. Hledá se kompromis a řešení rizik přinášených asymetrickými kybernetickými hrozbami. Setkání bezpečnostních odborníků z celého světa na konferenci Future Crises 2014 je platformou, kde se bude hledat tento kompromis. Přijďte hledat s námi.

Josef Strelec, Prezident ČP AFCEA

The well-known dependencies on water, food and energies are gradually complemented and replaced by dependencies on technologies and functioning of the cybernetic world. However, it is not just us, i.e. individuals or legal entities, that become dependent; it is also our entire way of life and our economic and social values. This is why representatives of the society must discuss and determine the borderline between individual freedoms and the need to protect the whole society's interests and values. A compromise and a solution of risks resulting from asymmetric cybernetic threats are being sought. The meeting of security experts from the whole world at the Future Crises 2014 Conference is a platform where the compromise will also be looked for. Come to look with us.

Josef Strelec, President AFCEA Czech Chapter

Czech Chapter AFCEA

Non-profit association
for communication, electronics and information systems in armed and security forces

Who we are

Czech Chapter of the Armed Forces Communications & Electronics Association (AFCEA) is a non-profit and educational organization whose mission is to create a professional forum for the management of ethical and effective dialogue between experts representing the membership and representatives of the armed and power ministries, government and academia of the Czech Republic.

AFCEA Czech chapter focuses its attention to promoting the development of information and communication technologies of the armed forces as one of the most important tools for defense of the universally recognized moral values of the democratic world. AFCEA Czech chapter was established on 5 May 1993.

Czech chapter is managed by a board of thirteen members. The head of the board is the chapter president. Current chapter president is Mr. Josef Strelec. The board consists additionally of three vice-presidents, secretary of the chapter, secretary of the program vice president, a treasurer and six board members.

Czech chapter currently has two honorary vice-presidents, who are Army General Vlastimil Picek, Chief of the General Staff of the Czech Armed Forces and Brigadier General Jan Kaše, Director, Department of Communication and Information Systems of the Ministry of Defence.

International significance

AFCEA was founded in 1946 in the United States based on the efforts of members of the U.S. Air Force Signal Corps to create an independent professional forum dealing with issues of communication, electronics and information systems not only in the armed and security forces.

Currently the association has more than 35,000 individual and more than 2,000 corporate members in more than 130 offices worldwide.

AFCEA International Headquarters are located in Fairfax, Virginia, USA. European management – AFCEA Europe has headquarters in Brussels, Belgium.

Significant activities

Czech Chapter regularly organizes conferences and seminars in the field of information and communication technology and security aspects. Since 1993, we have held more than 50 international conferences and more than 100 seminars and club events.

Among our most important events is the annual International Conference ITTE held since 1998. Czech chapter is also the co-organizer of professional events accompanying the International Exhibition of Defence and Security Technologies IDET and exhibition & conference Future Soldiers.

Since 2004 we organize professional events in the working group Digitization of Warfield and from 2010 seminars and professional events in the Cyber Security Working Group.

AFCEA Czech chapter has signed a cooperation agreement with the General Staff of the Czech Armed Forces, with the Police Academy of the Czech Republic in Prague and with the University of Defence in Brno.

Dolnoměcholupská 1418/12, 102 00 Prague 10, Czech Republic
phone: +420 606 764 616
www.afcea.cz

Industry's First
Threat-Focused NGFW

ASA with FirePOWER Services

#1 Cisco Security announcement of the year!

World's most widely deployed, enterprise-class ASA stateful firewall

Threat focused – Industry-leading next-generation IPS (NGIPS)

Identity-Policy Control & VPN

URL Filtering

Best in class high availability with clustering

Advanced Malware Protection

Unmatched visibility and automation with FireSIGHT management

Comprehensive Visibility and Control

Mobility and cloud drive productivity but introduce risk with emerging threats. To protect your assets, you must see the users, applications, devices, and threats on your network and what they are doing. With next-generation security services, ASA 5500-X firewalls protect your business, regardless of size, against multivector threats across the entire attack continuum.

Feature and Capabilities

Multilayered Threat Protection

Cisco ASA 5500-X Series Next-Generation Firewalls help you to balance security effectiveness with productivity. This solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, including:

- Granular visibility and control
- Robust web security onsite or in the cloud
- Comprehensive intrusion prevention system (IPS) to protect against known threats
- Protection from malware and emerging threats
- World's most widely deployed ASA firewall with highly secure Cisco AnyConnect remote access

Wide Range of Sizes and Form Factors

Protect networks of all sizes with MultiScale performance and a wide range of form factors. Cisco ASA 5500-X Series Next-Generation Firewalls are available as:

- Scalable, standalone appliances for branch offices, midsize businesses securing the Internet edge, and enterprise data centers
- High-performance blades that integrate with the Cisco Catalyst 6500 Series Switches
- Virtual instances to provide enterprise-class security for private and public clouds

Proven, Enterprise-Class Platform

All Cisco ASA 5500-X Series Next-Generation Firewalls are powered by Cisco Adaptive Security Appliance (ASA) Software, with enterprise-class stateful inspection and next-generation firewall capabilities. ASA software can be configured with the following capabilities:

- Integration with other essential network security technologies
- Enhanced user ID awareness from Cisco TrustSec security group tags, and Identity-Based Firewall
- Up to 640 Gbps of throughput by clustering up to 16 ASA 5585-X appliances
- High availability for high-resiliency applications
- Robust next-generation security with Cisco ASA with FirePOWER Services or ASA Next-Generation Firewall Services

CONFERENCE AGENDA

Conference Hall VHII

1st day - Wednesday 10/15/2014 (DEFENCE & SECURITY DAY)

10:00 - 13:30 CONFERENCE REGISTRATION OPEN

13:30 - 15:10 **Session 1 – Opening session**
Chairman: Mr. Petr JIRÁSEK, Chairman, Czech Cyber Security Working Group (CZE)
Future threats, future cyber forces, military cooperation and future challenges.

13:35 - 13:55 **Keynote speech: Future threats and necessary military capabilities in the coming years**
GENERAL Petr PAVEL, Chief, General Staff of the Czech Armed Forces (CZE)

13:55 - 14:20 **Keynote speech: Future cyber forces, military cooperation and future challenges**
MGEN. Thomas FRANZ, Deputy Chief of Staff, CIS and Cyber Defence, SHAPE (GER)

14:20 - 14:45 **Security Policy and Military Strategy in a Dynamically Evolving International Environment: "How to Respond to Future Threats and Challenges?"**
LTGEN. (Ret.) Kurt HERRMANN, President of the Clausewitz-Society (GER)

14:45 - 15:05 **Czech Law on Cyber – experiences from legislation process**
Mr. Tomáš KLADÍVKO, Member of Parliament, Czech Parliament (CZE)
Q&A period

15:10 - 15:40 NETWORKING COFFEE BREAK

15:40 - 17:30 **Session 2 – Defence session**
Chairman: LTCOL. (Ret.) Robert KOSLA, Regional Director, Public Safety, National Security, Defense, Microsoft Central and Eastern Europe HQ (POL)
Cyber Defence Strategy now and in the future. How to buy cyber technologies? The ability of armed forces to respond to security crisis of the 21st century

15:40 - 16:00 **Keynote speech: Definition of the role and tasks of National Armaments Office in the following years and the specifics of the acquisition process in cyber defence**
Mr. Tomáš DVOŘÁČEK, Deputy Director, National Armaments Office (CZE)

16:00 - 16:30 **Building and Perspective use of the armed forces in a global context - ability of the armed forces to respond to security crises in the 21st century**
BGEN. (Ret.) František MIČÁNEK, Director, Centre for Security & Military Strategic Studies, Defence University of Brno (CZE)

16:30 - 16:50 **The aspects of security and national sovereignty tactical communications**
Mr. Pavel ŠALANDA, General Manager Rohde & Schwarz – Praha, Member of AOBP (CZE)

16:50 - 17:10 **Tactical IP Radios in Battlefields** Mr. Michala REMPER, Cisco Systems Czech Republic (CZE)
Q&A period

17:25 - 17:30 **Closing remarks**
Mr. Petr JIRÁSEK, Chairman, Czech Cyber Security Working Group (CZE)

2nd day - Thursday 10/16/2014 (SECURITY DAY)

09:30 - 10:40 **Session 3 – Crisis Management session**
Chairman: BGen. (Ret.) Leif KÜLLER, Senior Advisor, Secana AB
Crisis management as a way to cope with threats and disasters.

09:30 - 09:35 **Welcome**
Mr. Jaroslav PEJČOCH, Vice-Chairman, Czech Cyber Security Working Group (CZE)

09:35 - 10:00 **New challenges in ensuring the civil protection in the coming years**
Mr. Bohuslav CHALUPA, Member of Parliament, Deputy Chairman of the Defense Committee and Chairman of the Permanent Commission for Control of Military Intelligence (CZE)

10:00 - 10:20 **Keynote speech: What we have learned in past 20 years and what is ahead**
BGEN. Miloš SVOBODA, General Directorate, Fire Rescue Service of the Czech Republic (CZE)

10:20 - 10:40 **Keynote speech: Risk Management in Cyber – lessons learned**
LTGEN. (Ret.) Robert SHEA, USMC, President AFCEA International (USA)

10:40 - 11:10 NETWORKING COFFEE BREAK

11:10 - 13:10 **Session 4 – Future Threats & Security Trends**
Chairman: Col. (Rtd.) John DOODY, Strategic Cyber Security Adviser (GBR)
What we may expect in a future? How to prepare for it?

11:10 - 11:35 **Keynote speech: How to keep up with future threats New Threats, New Risks and New Opportunities require Worldwide Collaboration with Dedicated People as a Key Factor solving these Challenges and establishing Relevant Education and Communication across borders.**
K. Harald DRAGER, President TIEMS (NOR)

11:35 - 11:55 **2014 Security Report**
Mr. Daniel ŠAFÁŘ, Country Manager, CZR Region, Check Point Technologies (CZE)

11:55 - 12:15 **Blackout – a New Situation for City or Prague – Exercise 2014**
Mr. Josef JURÁNEK, City of Prague (CZE)

12:15 - 12:35 **Droughts in Europe?**
Mr. Filip CHUCHMA, Czech Hydro meteorological Institute (CZE)

12:35 - 12:55 **Protection against advanced malware**
Mr. Ivo NĚMEČEK, CTO, Mr. Jiří TESAŘ, Cyber Expert, CISCO Systems (CZE)
Q&A period

13:10 - 13:40 NETWORKING COFFEE BREAK

13:40 - 15:30 **Session 5 – Critical Infrastructure Protection**
Chairman: Dr. Oldřich KRULÍK, Vice dean, Faculty of Security Management, Police Academy of the Czech Republic in Prague
Our critical infrastructure is more and more critical for our daily life and sustainability of our civilization.

13:40 - 14:00 **New perspectives on critical infrastructure in terms of future threats**
COL. Daniel MIKLÓS, General Directorate, Fire Rescue Service of the Czech Republic (CZE)

14:00 - 14:20 **Critical infrastructure protection – lessons learned, future threats & challenges**
Mr. Tudor GHEORGHITA and Mr. Alexandru BUHUS, Cyber Security Specialist, Romanian Secret Service (ROM

14:20 - 14:40 **Adopting a role of the Critical Infrastructure Subject: Burdens, Problems, Challenges, Benefits**
Mr. Tomáš KLAČER, MERO ČR (CZE)

14:40 - 15:00 **Status of critical information infrastructure identification in the Czech Republic**
Daniel P. BAGGE, National Cyber Security Centre (CZE)

15:00 - 15:20 **How Integration between Various Security Solutions Can Catch Targeted and Advanced Persistent Threats**
Mr. Ján KVASNIČKA, Territory Account Manager, Symantec (SVK)
Q&A period

15:30 - 16:00 NETWORKING COFFEE BREAK

16:00 - 18:00 **Session 6 – Security**
Chairman: LTCOL. Kamil HALOUZKA, Ph.D., Communication and Information Systems Department, University of Defense, Brno (CZE)
What are the future security concepts, trends, challenges and technologies? What kind of security threats we have to expect?

16:00 - 16:20 **Maintaining BLOS communications using latest technologies**
Mr. Steff TAYLOR, Head of Business Development, Spectra Group (GBR)

16:20 - 16:40 **Non-nuclear EMP as unavoidable considered risk in CIS risk management process**
Mr. Adnan KULOVAC, Head of CIS security department, National Security Authority of Bosnia and Herzegovina (BIH)

16:40 - 17:00 **How to manage your data erasure challenges**
Mr. Daniel DYER, Vice President of Global Operations, Tabernus (GBR)

17:00 - 17:20 **Security-as-a-Service and other alternatives to cyber security**
Mr. Tomáš PLUHAŘÍK, Manager, PwC (CZE)

17:20 - 17:45 **Future Threats and expected security solutions – technological trends**
Dr. Robert D CHILDS (COL. Ret.), President of iCLEAR, LLC, former Chancellor, National defense University iCollege (USA)
Q&A period

17:55 - 18:00 **Closing remarks**
Mr. Jaroslav PEJČOCH, Vice-chairman, Czech Cyber Security Working Group (CZE)

3rd day - Friday 10/17/2014 (CYBER SECURITY DAY)

10:00 - 11:40 **Session 7 – Cyber Security Visions & Challenges**
Chairman: Mr. Petr JIRÁSEK, Chairman, Czech Cyber Security Working Group (CZE)
What goals are ahead in cyber security? What future vision we have to declare?

10:00 - 10:25 **Keynote speech: New Cyber Security Strategy of the Czech Republic**
Mr. Dušan NAVRÁTIL, Director, National Security Authority (CZE)

10:25 - 10:45 **Keynote speech: International cooperation in cyber security**
Mr. Mihály ZALA, President, National Security Authority (HUN)

10:45 - 11:05 **Cyber Security – The human element and the best practices**
LTCOL. Paulo Almeida ARAÚJO, National Security Authority (PRT)

11:05 - 11:25 **Are National Doctrines effective for Cyber Defense and should NSA's stay behind security trends?**
LTCOL. (Ret) Robert KOSLA, Regional Director Public Safety & National Security, Microsoft Central & Eastern Europe (POL)
Q&A period

11:40 - 12:30 NETWORKING COFFEE BREAK

12:30 - 14:00 **Session 8 – Cyber education and cooperation**
Chairman: MGen. (Ret.) Frans J.H. PICAVET, Former Director NC3 Staff, General Manager NCOC2 (NGL)
How many cyber experts and well trained end-users we will need? What core skills they will need? How we will educate them quickly and effectively?

12:30 - 13:05 **Keynote speech: Cybersecurity Education, Training, and Workforce Development in the US: The Federal View and National Impact**
Dr. Robert D CHILDS (COL. Ret.), President of iCLEAR, LLC, former Chancellor, National defense University iCollege (USA)

13:05 - 13:30 **Cyber Security Education in the Czech Republic**
Mr. Vladimír ROHEL, Director National Cyber Security Centre (CZE)

13:30 - 13:45 **Need of synergy in education in the field of cyber security and internet safety**
Dr. Šárka SOUDKOVÁ, Ph.D., Manager for Cyber Security, National Centre for Secure Internet (CZE)
Q&A period

14:00 - 14:30 NETWORKING COFFEE BREAK

14:30 - 16:40 **Session 9 – Security trends & solutions**
Chairman: Air Commodore (Rtd.) Bruce WYNN, Cyber Expert, Member of Cyber Committee AFCEA International (GBR)
What are the current security trends? Are current security solutions ready for future threats? Do we need standardization for security solutions?

14:30 - 14:55 **Examining Active Cyber Defence in Deterrence and Conflict Escalation**
Col. (ret.) Jeffrey L. CATON, USAF, President, Kepler Strategies LLC (USA)

14:55 - 15:15 **How to fulfill the cyber-security law compliance and gain more security intelligence?**
Mr. Petr HNĚVKOVSKÝ, ArcSight Specialist, Hewlett-Packard (CZE)

15:15 - 15:35 **Mobility versus Security – How to meet security demands and user expectations**
Mr. Holger KALNISCHKIES, Secunet (GER)

15:35 - 15:55 **The databases vulnerabilities and protection of sensitive data**
Mr. Michal LUKANIČ, Oracle DB Specialist Sefira & Mr. Jan STRNAD, Presales Engineer McAfee, Intel (CZE)

15:55 - 16:20 **Keynote speech: Future threats, expected solutions and potential business opportunities**
MGen. (Ret.) Frans J.H. PICAVET, Former Director NC3 Staff, General Manager NCOC2 (NGL)
Q&A period

16:35 - 16:40 **Closing remarks**
Mr. Petr JIRÁSEK, Chairman, Czech Cyber Security Working Group (CZE)

LIVE DEMONSTRATIONS

Wednesday 10/15/2014

11:30 - 11:40
Demonstration of Cyber attack for VIP "Phishing attack"
CIRC Ministry of Defence live demo stand 214

15:00 - 15:10
Demonstration of Cyber attack for VIP "Phishing attack"
CIRC Ministry of Defence live demo stand 214

15:30 - 15:50
Demonstration of Cyber attack for Managers "Phishing attack" Demonstration of attack, detection, analysis Q&A, discussion
Masaryk University live demo stand 212

15:50 - 16:10
Demonstration of Cyber attack for Managers "Wi-Fi – Nothing is Free"Demonstration of attack, detection, analysis Q&A, discussion
CIRC Ministry of Defence live demo stand 214

Thursday 10/16/2014

10:20 - 10:40
Demonstration of Cyber attack for Managers "Phishing attack" Demonstration of attack, detection, analysis Q&A, discussion
CIRC Ministry of Defence live demo stand 214

11:10 - 11:30
Demonstration of Cyber attack for Managers "Phishing attack" Demonstration of attack, detection, analysis Q&A, discussion
Masaryk University live demo stand 212

15:10 - 15:30
Demonstration of Cyber attack for Managers "Wi-Fi – Nothing is Free" Demonstration of attack, detection, analysis Q&A, discussion
CIRC Ministry of Defence live demo stand 214

Friday 10/17/2014

11:05 - 11:25
Demonstration of Cyber attack for Managers "Phishing attack" Demonstration of attack, detection, analysis Communication, cooperation, sharing information among other CIRT teams Q&A, discussion
Masaryk University live demo stand 212
National Centrum of Cyber Security

13:30 - 13:50
Demonstration of Cyber attack for Managers "Wi-Fi – Nothing is Free"Demonstration of attack, detection, analysis Communication, cooperation, sharing information among other CIRT teams Q&A, discussion
CIRC Ministry of Defence live demo stand 214
National Centrum of Cyber Security

PROGRAMME COMMITTEE

Col. (Ret.) John Doody
FBCS FCMI CITP IISP
MIOD, Strategic Cyber Security Advisor, UK

Col. (Ret.) Ladislav Kollárik
Vice-president, AFCEA Slovak chapter

Assoc. Prof. Marcel Harakaľ, Ph.D.
Vice-rector, Armed Forces Academy, Slovakia

Mr. Jaroslav Pejčoch
Member, Coordination Committee, ICT Union, Czech Republic

LtCol. Petr Hrůza, Ph.D.
University of Defence, Czech Republic

Assoc. Prof. Josef Požár, Ph.D.
Dean, Faculty of Security Management, Police Academy, Prague

Col. Ivan Ilavský
Commander, J6, General Staff of the Slovak Armed Froces

Mr. Vladimír Rohel
Director, National Center of Cyber Security, Czech Republic

BGen. Jan Kaše
Director, CIS Dept., General Staff of the Czech Armed Forces

LtCol. Richard Složil
Director, CIRC, Ministry of Defence, Czech Republic

PROGRAMME COMMITTEE

LtCol. (Ret.) Josef Strelec
President, AFCEA Czech chapter

MGen. (Ret.) Klaus-Peter Treche
General Manager, AFCEA Europe

Mr. Aleš Špidla
Vice-President, Czech Institute of Information Security Managers

Mr. Josef Veselý, Ph.D.
Security Director, Ministry of Interior, Czech Republic

CONFERENCE SPEAKERS

Mr. Dušan Navrátil
Director, Czech National Security Authority

Mr. Mihály Zala
President, National Security Authority

Gen. Petr Pavel M.A.
Chief of the General Staff of Armed Forces; General Staff of Armed Forces

BGen. Miloš Svoboda
General Directorate, Fire Rescue

MGen. Thomas Franz
Deputy Chief of Staff, CIS and Cyber Defence, SHAPE

Mr. Tomáš Dvořáček
Deputy Director, National Armaments Office, Ministry of Defence

Lt.Gen. (Ret.) Robert M. Shea
Executive Vice President, Strategic Solutions, Smartronix Inc.

MGen. (Ret.) Ir. Frans J. H. Picavet
Former Director NC3 Staff, General Manager NCOC2

Mr. Petr Jirásek
Chairman; AFCEA Czech Cyber Security Working Group

LtCol. (Ret.) Josef Strelec
President, AFCEA Czech chapter

CONFERENCE SPEAKERS

LtGen. (Ret.) Kurt Herrmann
President of the Clausewitz-Society

Air Commodore (Ret.) Bruce Wynn
OBE, Cyber Expert, Member of AFCEA International Cyber Committee

BGen. (Ret.) František Mičánek
Director, Centre for Security and Military Strategic Studies

Mr. Vladimír Rohel
Director, National Center of Cyber Security

Mr. Bohuslav Chalupa
Vice-Chairman of the Defence Committee, Member of Parliament

Mr. K. Harald Drager
President TIEMS

Mr. Tomáš Kladivko
Senator, Czech Parliament (CZE)

Mr. Jaroslav Pejčoch
Member, Coordination Committee, ICT Union

Mr. Adnan Kulovac M.Sc.
Head of INFOSEC - CIS security department, Ministry of Security

Mr. Jeffrey Caton
President, Kepler Strategies LLC

CONFERENCE SPEAKERS

Col. (Ret.) John Doody
FBCS FCMI CITP IISP
MIOD, Strategic Cyber Security Advisor

PhDr. Šárka Soudková Ph.D.
Manager for Cyber Security, National Centre for Secure Internet

Col. Daniel Miklós
General Directorate Fire Rescue

LtCol. Kamil Halouzka Ph.D.
Communication and Information System Department, University of Defense, Brno

LtCol. (Ret.) Robert Kosla
Regional Director, Public Safety, National Security, Defence, Microsoft Central and Estern Europe HQ

BGen. (Ret.) Leif KÜLLER
Senior Advisor, Secana AB

Mr. Alexandru Buhus
Cyber Expert, Romanian Secret Service

Mr. Holger Kalnischkies
Senior Business Development Manager, Secunet Security Networks AG

Mr. Tudor Gheorghita
Cyber Expert, Romanian Secret Service

Dr. Oldřich Krulík
Vice dean, Faculty of Security Management, Police Academy of the Czech Republic

CONFERENCE SPEAKERS

Mr. Filip Chuchma
Czech Hydrometeorological Institute

Mr. Michal Lukanič
Oracle DB Specialist, Sefira

Mr. Josef Juránek
Director of Security and Crisis Management, Prague City Hall

Mr. Daniel P. Bagge
National Cyber Security Centre

Mr. Jan Strnad
Presales Engineer McAfee, Intel

Mr. Tomáš Klačer
ICT development and ISMS, Mero Czech Republic

Col. (Ret.) Robert D. Childs
President of iCLEARIlc, former Chancellor, National defense University iCollege

Mr. Steff Taylor
Head of Business Development, Spectra Group (UK) Ltd

Lt.Col. Paulo Jorge Antunes de Almeida Araújo
Adviser, National Cybersecurity Centre

Mr. Jiří Tesař
Cyber Expert, CISCO Systems Inc.

CONFERENCE SPEAKERS

Mr. Ivo Němeček
Acting General Director,
CISCO Systems Inc.

Mr. Ján Kvasnička
Territory Account Manager,
Symantec

Mr. Petr Hněvkovský
Senior Security Consultant,
HP Enterprise Security,
Hewlett-Packard

Mr. Daniel Dyer
Vice President of Global
Operations, Tabernus

Mr. Pavel Šalanda
General Manager,
Rohde & Schwarz

Mr. Tomáš Pluhařík
IT QA Manager, PwC

Mr. Daniel Šafář
Country Manager CZR
Region, Check Point
Software Technologies

Mr. Michala Remper
CISCO Systems Inc.

Alphabetical Exhibitors' Directory
Hall VHII

ALEF NULA, a.s.

U Plynárny 1002/97, 101 00 Praha 10
tel.: +420/225 090 111, fax: +420/225 090 112
e-mail: CZ-Sales@alef.com
www.alefnula.cz
Czech Republic

ALEF NULA, member of ALEF Group, provides comprehensive services in the field of information and communication technologies. Since 1994, the company has been a leading supplier of Cisco Systems solutions. The ALEF NULA Company pride themselves on a broad technological base and top technical experts. The combination of technological facilities, experts and the status of Cisco Certified Learning Partner provides a wide base, which makes it possible for ALEF NULA to offer their customers the best platform for providing high level of support and developing their services. Not only in the Czech Republic but also at the level of EMEA, partners as well as the manufacturer appreciate the unique possibility of combining theoretical knowledge gained in the Cisco training activities with practical knowledge resulting from the completed projects. All this is evidenced by the company's dominant market position, Cisco Worldwide Top Innovator award, and the status of Cisco Gold Partner.

Stand: 206

AFCEA Czech Chapter (ARMED FORCES COMMUNICATIONS & ELECTRONICS ASSOCIATION)

Budova Servodata, Dolnoměcholupská 1418/12, 102 00 Praha 10
tel.: +420/606 764 616, fax: +420/296 813 310
e-mail: prezident@afcea.cz
www.afcea.cz
Czech Republic

AFCEA Czech Chapter is a non-profit and educational organization whose mission is to create a professional forum for the management of ethical and effective dialogue between experts representing the membership and representatives of the armed and power ministries, government and academia of the Czech Republic.

Stand: 210

CISCO SYSTEMS (Czech Republic) s. r. o.

Millenium Plaza Building, V Celnici 10, 110 00 Praha 1
tel.: +420/221 435 111
www.cisco.com/cz
Czech Republic

CISCO is the worldwide leader in networking and changes the way people connect, communicate and cooperate. Since the very beginning of the company's existence, it focuses all efforts to answer to customers' specific needs. Cisco is one of the largest global IT companies and a dominating player in the field of network elements. Apart from networking technologies, Cisco develops and offers its own teamwork systems or multifunctional systems allowing to transmit data, voice and video with centralized web management and administration. More than 90 % of all internet data passes through Cisco products. Last year, Cisco successfully combined their experience with cyber safety with newly acquired technologies called Cognitive Threat Analytics, represented by the Czech company Cognitive Security, as well as with Advanced Malware Protection (AMP), originally developed by Sourcefire. This allows us to provide protection for every phase of a cyber-attack: before, during and after. The newest feature in Cisco security solutions is a new generation of firewalls combining time-proven firewall technologies with new generation Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) technologies.

Stand: 203

DEFENCE AND SECURITY INDUSTRY ASSOCIATION (DSIA)

Washingtonova 25, 110 00 Praha 1
tel.: +420/224 235 320, fax: +420/224 235 319
e-mail: info@aobp.cz
www.aobp.cz
Czech Republic

DSIA is an interest association of more than 100 corporate bodies dealing with military and security material and services.

HEWLETT PACKARD

Vyskočilova 1/1410, 140 21 Praha 4
tel.: +420/261 307 111
e-mail: info.cz@hp.com
www.hpenterprisesecurity.com
Czech Republic

Today's organizations are facing the most aggressive threat environment in the history of information technology. Emerging computing trends have greatly increased productivity and business agility—but at the same time, have introduced a host of new risks. Actionable security intelligence is critical to protecting your organization from this rising tide of security threats. HP is a leading provider of security intelligence and compliance solutions for enterprises that want to mitigate risk and defend against today's most advanced threats. Based on market-leading products from ArcSight, Atalla, Fortify and TippingPoint, HP Enterprise Security Products enables organizations to take a proactive approach to security, integrating information correlation, application analysis and network-level defense. HP Security Research strengthens this portfolio of solutions through innovative research, delivering actionable security intelligence while providing insight into the future of security and the most critical threats facing organizations today. More information about HP Enterprise Security Products is available at http://www.hpenterprisesecurity.com.

Stand: 201

CHECK POINT SOFTWARE TECHNOLOGIES s.r.o.

Pobřežní 3/620, 186 00 Praha 8
tel.: +420/222 311 495
e-mail: info_ee@checkpoint.com
www.checkpoint.com
Czech Republic

CHECK POINT SOFTWARE TECHNOLOGIES Ltd. (www.checkpoint.com), the worldwide leader in securing the Internet, provides customers with uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to develop new innovations based on the Software Blade Architecture, providing customers with flexible and simple solutions that can be fully customized to meet the exact security needs of any organization. Check Point is the only vendor to go beyond technology and define security as a business process. Check Point 3D Security uniquely combines policy, people and enforcement for greater protection of information assets and helps organizations implement a blueprint for security that aligns with business needs. Customers include tens of thousands of organizations of all sizes, including all Fortune and Global 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

Stand: 205

ICT Network News / AVERIA LTD.

Pod Kotlaskou 558/3, 180 00 Praha 8
tel.: +420/773 626 874
e-mail: smolnik@averia.cz, events@averia.cz
averia.cz
Czech Republic

ICT Network News - Landing page of our community collects the latest and the best of all of our media. This page is a guidepost of our community for both new and existing readers. Applications such as Event Calendar, Jobs in ICT or ICT-TV completes the practical landing page and give more reasons for visiting.

Stand: 209

ICT UNIE z. s.

K červenému dvoru 25a/3269, 130 00 Praha 3
tel.: +420/222 582 880
e-mail: ictu@ictu.cz
www.ictu.cz
Czech Republic

ICT UNIE is a professional association of companies active in the field of information technology and electronic communication. Its goal is to increase the awareness of the importance of adopting and making use of modern information technology in our society. This includes creating an optimal setting for the development of public electronic communication networks in the Czech Republic, as the networks' development is a necessary step towards establishing an information society.

MASARYK UNIVERSITY

Žerotínovo náměstí 9, 602 00 Brno-město
tel.: +420/549 492 100, fax: +420/541 212 747
e-mail: info@ics.muni.cz
www.muni.cz
Czech Republic

MASARYK UNIVERSITY is the second largest university in the Czech Republic. Research and development in the area of cyber security is pursued at the Institute of Computer Science in cooperation with the Faculty of Informatics, the Faculty of Law, and other public institutions and business partners.

Stand: 212-213

McAfee Ireland Ltd.

Building 2000, City Gate, Mahon, Cork
e-mail: CZ+SK: Alena_Reznickova@McAfee.com
www.intelsecurity.com
Ireland

McAfee is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and businesses of all sizes from the latest malware and emerging online threats. Our solutions are designed to work together, integrating antimalware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve Internet security, and help businesses achieve operational efficiencies. Backed by an award-winning research team, McAfee security technologies use a unique, predictive capability that is powered by McAfee Global Threat Intelligence — enabling home users and businesses to stay one step ahead of online threats.

MICROSOFT s.r.o.

BB Centrum, budova Alpha, Vyskočilova 1461/2a, 140 00 Praha 4
tel.: z ČR volejte na číslo (from Czech Republic call):
841 300 300*
mimo ČR volejte (outside of Czech Republic call):
+420 261 197 665
* Hovor bude účtován podle tarifu Vašeho operátora za volání na pevné linky v rámci ČR
e-mail: velkespolecnosti@microsoft.com
www.microsoft.cz
Czech Republic

Founded in 1975, MICROSOFT is the worldwide leader in software, services, and solutions that help people and businesses realize their full potential. The Czech subsidiary of Microsoft Corporation was founded in 1992. Biljana Weber is the company's general manager. Microsoft provides broad support for charitable projects in Czech Republic. The PCs Against Barriers project was launched in 1996 on the initiative of the Charter 77 Foundation and Microsoft and that support continues to this day. The project aims to help disabled individuals succeed not only in everyday life, but also in the labor market. Microsoft's charitable activities are covered by the Microsoft Unlimited Potential global initiative. This program focuses on forming partnerships around the world with public education centers that organize training courses on information technology and solutions. Grants from the program are designed to provide training in community and special education centers, where people can learn how to work with computers.

POLICE ACADEMY of the Czech Republic in Prague

Lhotecká 559/7, 143 01 Praha 4
tel.: +420/974 828 501, fax: +420/974 827 273
e-mail: polac@polac.cz
www.polac.cz
Czech Republic

POLICE ACADEMY of the Czech Republic in Prague is a state college of the university type, closely associated with the Ministry of Interior of the Czech Republic. The school offers bachelor (Bc.), master (Mgr.) and doctoral programmes (PhD., Ph.D.), as well as the possibility of habilitation (doc.). The school is divided into the Faculty of Security Management and the Faculty of Security and Law. The school is open not only to the police offices but also for the wider public.

Stand: 211

PricewaterhouseCoopers Česká republika, s.r.o.

Hvězdova 1734/2c, 140 00 Praha 4
tel.: +420/251 151 111, fax: +420/251 156 111
www.pwc.com/cz
Czech Republic

Risk assurance department of PwC focuses on identification of risk areas of our clients and using proven methodologies and deep industry knowledge, we help organizations to integrate a security infrastructure (people, processes and technology) and implement standardized and secure processes. With a comprehensive view of security, organizations obtain a realistic picture of their weaknesses and can proactively take action to protect information assets.

RITTAL CZECH, s.r.o.

Ke Zdibsku 182, 250 66 Zdiby u Prahy
tel.: +420/234 099 000, fax: +420/234 099 099
e-mail: info@rittal.cz
www.rittal.cz
Czech Republic

RITTAL CZECH, s.r.o. is a daughter company of Rittal GmbH & Co. KG, a leading global provider of solutions for industrial enclosures, power distribution, climate control and IT infrastructure, plus software and services. The company's broad portfolio includes complete solutions for modular and energy-efficient data centres: from innovative security concepts for data systems to physical data and system security for IT infrastructures. Founded in 1961, Rittal is now active worldwide with 11 production sites, 64 subsidiaries and 40 agencies. With 10,000 employees worldwide, Rittal is the largest company in the owner-operated Friedhelm Loh Group, based in Haiger, Germany. The entire group employs more than 11,500 people and generated revenues of about € 2.2 billion in 2013. Further information at www.rittal.com and www.friedhelm-loh-group.com.

Stand: 208

secunet

Kronprinzenstrasse 30, 45128 Essen
tel.: +49/201 5454 – 0
e-mail: info@secunet.com
www.secunet.com
Germany

secunet is one of the leading German IT security providers with a wide range of products and solutions. Highly sensible information deserve the highest level of protection – secunet's flagship product line SINA comprises Gateways, Line Encryptors, Management and various mobile Clients suitable for use in the Defence Sector.

Stand: 207

SEFIRA spol. s r. o.

Antala Staška 2027/77, 140 00 Praha 4
tel.: +420/222 558 111
e-mail: sales@sefira.cz
www.sefira.cz
Czech Republic

SEFIRA - is a stable supplier of IT solutions and services. They focus on supplying enterprise solutions, development of specialized information systems, security of enterprise applications (mobile security, authentication, PKI, database security), and provision of services in the areas of systems integration, and design and implementation of enterprise infrastructure. They are the author and supplier of a solution for the management and archival of electronic documents, OBELISK Archive, and a provider of a service for verifying the validity of digital certificates, CertReview. SEFIRA has customers in finance, insurance, energy, industry and public administration.

SIMAC TECHNIK ČR, a.s.

Radlická 740/113c, 158 00 Praha 5
tel.: +420/283 061 281
e-mail: sales@simac.cz;
www.simac.cz
Czech Republic

SIMAC TECHNIK ČR is a technology independent system integrator providing Services in the ICT environment. System integration provided by Simac Technik ČR involves comprehensive solutions of customers' needs, which integrate infrastructure, security, management and applications, primarily with regard to the functioning of systems, instead of delivering third-party products.
SERVICES AND SOLUTIONS
For all of the following services and solutions we provide comprehensive analysis of the current status, design, consulting, implementation and operation of the solution, followed by technical assistance under the project methodology standards PMI and ITIL best practices.

- Communication infrastructure
- Mobile data solutions and wireless networks
- Data center and virtualization
- ICT security
- Solutions and collaboration tools
- Management and monitoring
- Customer Technical Support ICT

Stand: 204

SPECTRA GROUP

Bridge Court Barn, Kingstone, HR2 9ES Herefordshire
tel.: +44/845 2600 444
e-mail: enquiries@spectra-group.co.uk
www.spectra-group.co.uk
United Kingdom

SPECTRA GROUP (UK) is a leading provider of voice and data services in areas where either none exist or where high intensity conflicts, natural disasters, pandemics or terrorist attacks may have destroyed existing networks.

STALWARTS s.r.o.

Holušická 2221/3, 148 00 Praha 11
tel.: +420/723 642 881
e-mail: info@stalwarts.eu
www.stalwarts.eu
Czech Republic

STALWARTS s.r.o. is a global sales and distribution representative for SilentPocket® a U.S. manufacturer of top of the range shielding devices for mobile phones, tablets and credit cards. More information at www.stalwarts.eu.

Stand: 200

SYMANTEC GmbH ČR&SR

REGUS Zlatý Anděl, Nádražní 344/23, 150 00 Praha 5
tel.: +420/234 234 761
e-mail: Kristina_hasonova@symantec.com
www.symantec.cz
Czech Republic

SYMANTEC protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world.

TABERNUS EUROPE Ltd

Unit 8, Waterside Court, Albany Street, NP20 5NT Newport, South Wales
tel.: Sales: Call: +44/1639 505 731, fax: Support: tel: +44/1639 505 731
e-mail: eusales@tabernus.com
www.tabernus.com
United Kingdom

TABERNUS is a leading provider of data erasure software and hardware products used by companies of all sizes to completely remove all data from hard drive storage devices. Tabernus has been formally certified for government use to securely erase protectively marked data after independent testing carried out by QinetiQ, a British global defence technology company under contract to the Government's Communications-Electronics Security Group (CESG). Tabernus partners include the OEM, Defence, Public/Private Sector, Health Care and IT Recycling and Disposal sectors. Tabernus Data Erasure software is one of only a few companies that offer a full suite of products for the erasure of everything from PC's and laptops, through to Enterprise Storage shelves, mobile phones and Tablets.

stand: 202

UNIVERSITY OF DEFENCE

Kounicova 65, 662 10 Brno
tel.: +420/973 442 554, fax: +420/541 211 269
e-mail: vladimir.sidla@unob.cz
www.unob.cz
Czech Republic

The UNIVERSITY OF DEFENCE is responsible for education of military professionals and other experts engaged in national security and defence.

stand: 211A

Kybernetická bezpečnost v éře Internet of Everything

Doba neškodných virů typu Kuchař a Sušenka je dávno minulostí. Dnešní svět kybernetického zločinu už dávno není světem obrýlených uhrovitých mladíčků, kteří chtějí všem okolo dokázat, jak jsou dobří. Dnešní útočníci jsou profesionálové každým coulem.

Svět informačních a komunikačních technologií se mění. Nástup Internet of Everything znamená, že do sítě nejsou už připojeny pouze počítače či notebooky, ale celá řada dalších zařízení. Ať již jde o datové sklady, nositelnou elektroniku nebo třeba chytré semafory či systémy řízení dopravy. Cílený kybernetický útok tak může znamenat přímé ohrožení nejen systémů jedné firmy, ale dokonce funkcí a bezpečnosti celých států. Loňský výzkum americké neziskové organizace CSIS (Center for Strategic and International Studies) odhadl, že kybernetické útoky připraví celosvětovou ekonomiku ročně o 500 miliard amerických dolarů.

Kyberzločin záležitostí profesionálů

Dříve používaný systém ochrany proti kybernetickým útokům založený na vzorcích škodlivých kódů dávno nedostačuje. Kybernetické útoky dnešní doby jsou založené na využití nedokumentovaných hrozeb, se kterými si běžné firewally či antivirové programy nemohou poradit. Svědčí o tom i výsledky průzkumu Cisco Midyear Security Report ze srpna 2014, který ukázal, že v 70 procentech firem byly zjištěny stopy po tak zvaném botnetu. To je škodlivý kód, díky němuž je útočník schopen převzít kontrolu nad napadeným počítačem a zneužít ho k provádění dalších útoků či jiným činnostem. Ve více než 90 procentech firem byl zaznamenán provoz směřující na servery, na nichž se vyskytuje malware.

Největší část útoků připadá v současné době na útoky typu exploit. Ty jsou totiž mířeny na konkrétní známé slabiny operačního systému nebo aplikace, s cílem získat přístup k napadenému počítači. Prostředí pro vytváření nebezpečných kódu lze přitom získat pouhým nákupem balíčku (exploit kit). Výsledný exploit lze šířit pomocí odkazů v mailu, ale také odkazy či skrytým přesměrováním na stránkách některých serverů.

Právě možnost koupě exploitu, že kybernetický zločin se již dnes stal svébytným „průmyslovým odvětvím“, které je do značné míry profesionálním. Již zmiňovaný výzkum ukázal, že když byl loni zatčen tvůrce jednoho z nejpopulárnějších kitů (Blackhole Exploit Kit), poklesl počet podobných balíčků meziročně o 87 procent. Na druhou stranu se ale zvýšila jejich rozmanitost. Kit dokázal určit bezpečnostní slabiny zejména v programech Adobe Acrobat a v jazyce Java, a následně je využít pro provedení útoku. Podle některých zdrojů mohly útoky založené na Blackhole Exploit Kit až za 80 procent napadení odhalených bezpečnostními programy.

Ochrana dříve, než útok začne

Vzhledem k proměně bezpečnostního prostředí se technologie společnosti Cisco snaží zaměřit především na ochranu před novým typem hrozeb. V dnešním světě se není možné začít bránit až v okamžiku vypuknutí útoku. Moderní forma ochrany proti kybernetickému ohrožení se proto musí zaměřit na všechny fáze útoku: před ním, během něj a po něm. Ve fázi „před“ je třeba posilovat IT prostředí firmy nebo organizace, řídit přístup do sítě a nasadit takové systémy, které odhalí přicházející útok co možná nejdříve. Ve fázi „během“ je klíčové probíhající útok identifikovat a co nejrychleji zastavit. Ve fázi „po“ přicházejí ke slovu technologie, které pomohou zjistit dopad útoku a napravit vzniklé škody. Vzhledem k nepřetržité povaze útoků ovšem často neexistuje ostrá hranice mezi těmito fázemi, protože fáze různých útoků se mohou překrývat.

Schopnost bránit se tak zvaným útokům prvního dne je založena na kontinuální analýze, behaviorálním modelování a detekci anomálií v běžném provozu sítě. Tímto způsobem jsou identifikovány škodlivé aktivity a zkracuje se čas vedoucí k odhalení hrozeb působících uvnitř sítě. Po loňské akvizici české společnosti Cognitive Security se v portfoliu Cisco spojily dřívější zkušenosti z oboru kybernetické bezpečnosti s přínosy technologie Cognitive Threat Analytics, a také Advanced Malware Protection (AMP), které bylo původně vyvinuto firmou Sourcefire.

Obě technologie kombinují moderní postupy, aby identifikovaly a zneškodnily útoky v jakékoliv jejich fázi. Mezi tyto postupy patří zjišťování reputace souborů – kde dochází k analýze souborů probíhajících sítí a uživateli je poskytnuta informace o tom, jaké soubory byly na základě nastavení zablokovány, sandboxing – který pomáhá v izolovaném prostředí sledovat a pochopit chování malwaru a retrospektivní analýzu souborů, jejíž pomocí se řeší situace, kdy jsou soubory, které již prošly perimetrem, považovány za hrozbu.

Nejnovější obranný val

Všechny požadavky na moderní ochranu sítě splňuje i nejnovější přírůstek do rodiny bezpečnostních zařízení společnosti Cisco. Nová generace firewallů řady Cisco ASA sérií 5500-X a Cisco ASA 5585 – X zcela mění dosavadní zvyklosti. Dříve dokázaly firewally ochránit síť jen před známými hrozbami. Nová generace firewallů Cisco ale kombinuje osvědčené firewallové technologie s novou generací technologií Intrusion Prevention System (IPS) a Advanced Malware Protection (AMP) založených na platformě SourceFire.

V souladu s aktuálními požadavky tak mohou nabídnout kontextovou a dynamickou analýzu bezpečnostních hrozeb, a umožňují ochránit sítě v každé fázi kybernetického útoku. Kombinace Cisco Adaptive Security Appliance se službami FirePOWER totiž poskytuje adaptivní několikavrstvou ochranu. To umožňuje rozšířit možnosti ochrany sítí za hranice toho, co bylo dosud možné očekávat od běžných firewallů. Vůbec poprvé si totiž díky technologiím FirePOWER umí firewall poradit s hrozbami nultého dne, tedy s novými a dosud nepopsanými útoky, na které nelze předem připravit bezpečnostní politiky.

Check Point SOFTWARE TECHNOLOGIES LTD.

Revolutionary Software-defined Protection architecture

Check Point Software Technologies introduced this year Software-defined Protection (SDP), a revolutionary security architecture that can protect organizations in today's fast-evolving IT and threat landscape. Software-defined Protection offers modern security today that can effectively protect against tomorrow's threats, through a design that is modular, agile and most importantly, secure.

SDP is a three-layer security architecture comprised of enforcement, control and management layers. This framework decouples the control layer from the enforcement layer, enabling robust and highly-reliable enforcement points that obtain real-time protection updates from a software-based control layer. SDP converts threat intelligence into immediate protections and is managed by a modular and open management structure.

"The threat landscape has become far more sophisticated while at the same time, enterprise IT environments have grown in complexity. Enterprises are looking for advice on how they can become more secure, but in a way that is manageable and simple to use. SDP is today's security architecture for tomorrow's threats; it is simple, flexible and can robustly convert threat intelligence into real-time protections," said Amnon Bar-Lev, president at Check Point Software Technologies.

"Check Point's new Software-defined Protection is a sound blueprint to architecting security that just makes a lot of practical sense," said Dan Meyer, vice president of technology at Carmel Partners. "Security attacks have changed radically over the years, and SDP represents a very smart shift forward in protecting organizations of all sizes in a pragmatic, modular and secure approach."

"By offering a security architecture driven by function, threat and need, Check Point's Software-defined Protection architectural blueprint can help IT better redesign their enterprise security network to accommodate both today's IT borderless environment and the dynamic threat landscape," said Charles Kolodgy, research vice president with IDC Security Products team.

"There are a multitude of point security products that are reactive and tactical in nature rather than architecturally oriented. We developed the Software-defined Protection in response to this gap and to give organizations an agile and secure security infrastructure," concluded Bar-Lev.

Additional Resources:

- For read the full report on Check Point's Software-defined Protection security architecture, visit:/http://www.checkpoint.com/sdp/check_point_spd_white_paper.pdf
- For more information on how to utilize the SDP methodology in your organization, visit:http://www.checkpoint.com/sdp/

DSIA

Tactical Systems Section of the Defence and Security Industry Association (DSIA) was established in November 2012 to prepare systemic solution of tactical communication for the Armed forces of the Czech Republic. Its goal is to:

- provide compatibility of legacy systems with existing systems
- maintain continuity of systemic integration with regard to information security of these systems and protection of classified information
- exploit national and European industry potential
- utilize potential of future development of these systems
- provide cryptographic independency and sovereignty of the Czech Republic and its military

Expert work within the Section is provided by five companies (ROHDE & SCHWARZ - Praha, DICOM, PRAMACOM HT, INTV, ICZ), furthermore, other experts from DSIA member companies are invited for consultations if needed.

Based on a requirement of the Chief of the General Staff, the Section prepared for the high profile representatives of the Czech armed forces a practical demonstration of a hybrid systemic concept of communication. The demonstration took place at the Prague Airport Kbely on the 31st October 2013. A proposal of the system was completed in September 2014.

Nowadays, experts from the Section are working on so called White Paper on the whole concept with the aim to finish the document and present it to wide public in November 2014 during MilDay of the Section 2014.

Establishment of the Section was unequivocally useful step to synchronize knowledge and expertise of the Czech defence industry which is strongly connected with Europe. This synergy has been already transformed into concrete projects which have high export potential.

Symantec™

Slovak Government Authority Secures Public Finances with Symantec

The security of the Slovakian Rebublic's public finances is safely in the hands of Symantec. DataCentrum, which IT processing services associated with the country's state budgets, treasury, and tax, standardized on an integrated portfolio of Symantec endpoint security and encryption technologies almost a decade ago. The solution protects critical government fiscal information, mitigates new risks, and lowers the cost of government IT infrastructure security.

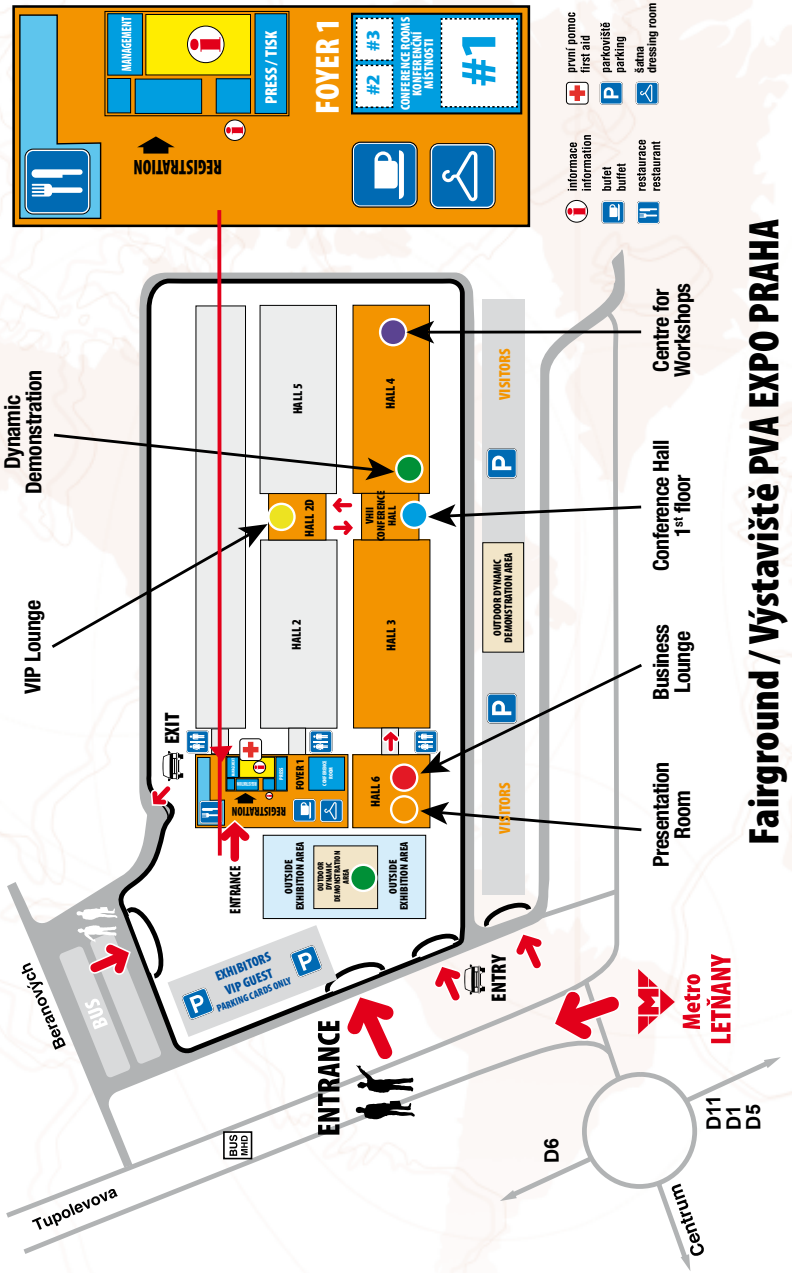
Budget management in Bratislava

Occupying both banks of the Danube River and as the only national capital to border two independent countries (Austria and Hungary), Bratislava is the political and economic hub of Slovakia. The city is also home to a key government institute: DataCentrum. This organization is the information center for the Ministry of Finance of Slovak Republic, processing data associated with state budgets, state treasury, tax, and customs affairs.

As a key government department in Central Europe, DataCentrum operates strict rules governing threat management. However, it is a continual struggle for the organization to keep up with changes in the threat landscape, maintain adequate visibility of the IT infrastructure, and manage alerts. To this end, the organization standardized almost a decade ago on Symantec solutions.

As the chief operating officer of DataCentrum, Peter Cichra is at the forefront of safeguarding the public finances data. "DataCentrum—together with the Ministry of Finance itself—is constantly evolving and new infrastructure trends, such as mobility, virtualization and cloud-based solutions, can open up new avenues for attacks. With Symantec, DataCentrum benefits from 'edge-to-endpoint' visibility across the Slovak infrastructure. This mitigates new risks and protects our critical information."

For Cichra, one of the most important benefits of standardizing on Symantec is the knowledge that the government organization is partnering with a global leader in data security. "The breadth of the Symantec portfolio, market leadership, and the gradual evolution of the Symantec technology is what stands Symantec apart from other vendors," he says. "With such a strong security solution stack, Symantec is gathering huge amounts of threat data that cascades down into improved protection for customers like DataCentrum."



Fairground / Výstaviště PVA EXPO PRAHA

Hall VHII

general partner

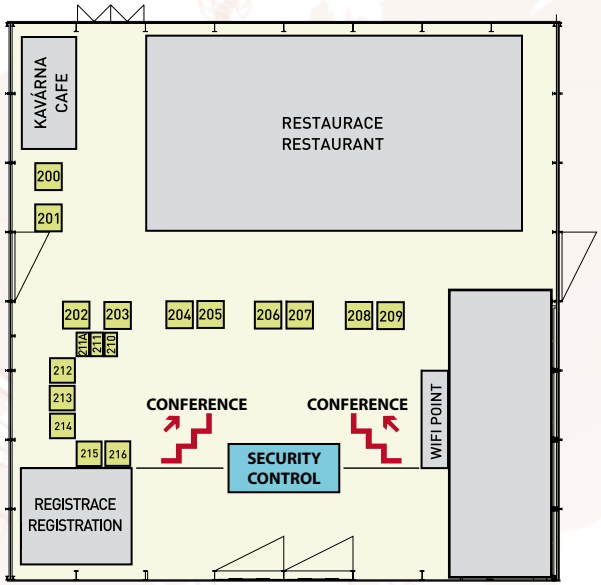
LOM PRAHA

general partner of conference

CISCO

Check Point SOFTWARE TECHNOLOGIES LTD.

Cyber Pavillion Sponzor



INFORMATION

EXECUTIVE GUARANTOR
AFCEA Czech Cyber Security Working Group

IN CO-OPERATION WITH
AFCEA Czech Chapter
National Security Authority of the Czech Republic
National Centre of Cyber Security of the Czech Republic
Police Academy of the Czech Republic in Prague
Armed Forces Academy of General Milan R. Štefánik, Slovakia
University of Defence in Brno, Czech Republic

Contact for Conference Programme and Speakers:
Mr. Petr Jirásek
Program Committee Chairman
petr.jirasek@cybersecurity.cz
+420 603 245 240

Contact for Exhibitors, Partners and Participants:
Mrs. Martina Navrátilová
Exhibition & Conference Manager
martina@natoexhibition.org
+420 277 010 665
GSM +420 602 221 864

EMERGENCY CALL
112

TAXI
We recommend using the contracted company HALOTAXI, which is able to offer the negotiated price for Future Forces Exhibition & Conference guests - 24 CZK/km – **do not forget use the phrase „FUTURE FORCES" for this special rate** Payment in CZK, EUR or credit card possible.

Phone numbers:
+420 2 4411 4411, +420 602 177 292,
+420 603 845 825, +420 776 11 44 11