NEWSLETTER

Vienna, January 2018

energypact foundation

THE FIRST WOMAN CYBER FORUM

OUTSTANDING GROUP OF SPEAKERS, MENTORS AND PARTICIPANTS GATHERED IN LEVERAGING THEIR EXPERIENCE AND KNOWLEDGE

EDITORIAL

The first and the last step behind all of us! The first step towards female integration into cyber area has been made, with the first Women`s Cyber Forum: Launching Careers in Cyber Space that held at the Diplomatic Academy of Vienna, gathering more than 90 speakers and participants. And the very last step from us, is actually what is in front of you – this issue of Newsletter; our last addressing to you in existing format. From 2018, we will have an honor to introduce our new and more comprehensive publication – Energypact Review.
Beside getting informed about our Women Cyber Forum event, in this issue of Newsletter, you will be able to read more about women`s participation into cyber area, as well as the news digest and announcement for the forthcoming Vienna Cyber Security Week 2018.

Enjoy reading!

energypact

WOMEN'S CYBER FORUM 2017

Launching Careers In Cyber Space

Information sharing - Networking - Mentoring

November 6, 2017
Vienna

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

With the support of

CSP AUSTRIA

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

IN THIS ISSUE:

THE FIRST WOMEN`S CYBER FORUM HAS BEEN HELD!

Very high level of interest shown for the ever first "Women`s Cyber Forum: Launching Careers in Cyber Space", which has been held within the premises of the Diplomatic Academy of Vienna on 06 November.

The rapid expansion of the cyber security sector offers one of the fastest growing areas of opportunity for professionals seeking to enhance or diversify their career. A 2016 Forbes article reported that there were over one million cyber security job openings in 2016, rising to 6 million lobally by 2019; by then we will witness a shortfall of 1.5 million specialists. Reports, however, also show that women comprise only 11 percent of the global information security workforce.
This is an unsatisfactory and unstainable model. Cyber security is not merely a technical, but a societal and business challenge that requires a diverse set of disciplines and skillsets that includes traditional areas such as computer science but also increasingly requires strong competences in criminology, psychology, business, law, and political science.
The Energypact Foundation, in its mission to build awareness and promote cyber security, conducted a one day seminar focused on information sharing, networking and mentoring for women professionals seeking opportunities in cyber security. The goal of this seminar was to create a forum for information sharing, networking and mentoring: to raise awareness about the importance of cyber security as a career choice for young women in particular.

WOMEN'S CYBER FORUM AT A GLANCE

- 70 PARTICIPANTS FROM 9 COUNTRIES
- 16 SPEAKERS
- 5 SESSIONS (3 REGULAR & 2 SPECIAL ONES)
- MENTORING & NETWORKING RECEPTION

Most of presentations exposed in the event, are available at the following link:
https://www.energypact.org/presentations/

For more detailed information about the event, as well as for the Agenda, please consult the following link:
www.energypact.org/womencyberforum

Networking & Mentoring Session
at the first Women`s Cyber Forum 2017

With 90 speakers and participants, this very first edition of the Forum gathered representatives of business, academia, NGO sector, junior professionals and students interested in persuing career in cyber space. Since its inception, the EnergyPact Foundation has engaged the international energy community through activities aimed at raising the global awareness on issues related to energy development and sustainability. These activities have included coordination and sponsorship of multiple international conferences for information exchange and confidence building.

In its often cited research, Cisco reported that in 2013, 80 “things” per second were connecting to the internet and estimated that by 2020, more than 250 things will connect each second to the internet for a combined total of over 50 billion things.Furthermore, this connectivity will not just power traditional IT components, but will drive critical infrastructure including energy, transportation, agriculture, and finance. It is hard to imagine a sector not being impacted. Unfortunately, while this technology migration provides tremendous benefit, it also comes with risk of attack from a variety of threat actors.

One of the most challenging issues we face as a global community is the ever increasing need for expertise in IT and computer security. While tremendous needs exist, recent workforce reports indicate that women comprise of only 11 percent of the global information security workforce. The current situation fails to take leverage a wealth of talent, talent that is desperately needed. Talent however is not just needed in traditional IT and computer security disciplines, but today’s environment requires strong computer security knowledge across a multitude of competencies to address the far reaching influence and impact of computers.

> ***Vienna School of International Studies was founded in 1754 by a strong and visionary woman – the Habsburg Empress Maria Theresia. And I dare say that Maria Theresia would approve of your approach to empower women by launching careers in cyber space.***
>
> Susanne Keppler-Schlesinger, Deputy Director,
> Diplomatic Academy of Vienna

We are grateful to our sponsors: the Austrian Institute of Technology - AIT, and Cybersecurity Platform - CSP: Austria for actively supporting our event.

STARTING A CAREER IN CYBERSECURITY

Colleen Glenn, Idaho National Laboratory

With a projected workforce shortage of 1.8 million by 2021, there have never been more opportunities or a greater need for women to join the field of cybersecurity. Yet a recent study found that women comprise only 11% of the current global information security workforce. Encouraging more women to consider careers in cyber is a challenge employers must address and undertake quickly in order to meet future labor demands. This means attracting talent from backgrounds beyond computer science and engineering–such law, business, and social sciences, among others. Still, women who have already developed an interest in cybersecurity may find that the cyber career path is not clearly defined, or are unsure where to begin. For those thinking about starting or transitioning into a career in cyber, there are a number of ways to prepare.

First, do your research. Fundamentals of information technology (IT) are a good start to understanding needs and practices in cybersecurity. A basic understanding of system architecture and administration, hardware and software, networking, and general digital literacy (computer and internet use) are useful. An additional topic to consider exploring is operational technology (OT), the hardware and software responsible for controlling real-world, physical processes and that also require cybersecurity considerations. Also, keeping up with news and trends in cybersecurity such as emerging cyber threats, vulnerabilities, new technologies, etc. may be helpful to gain a better understanding of the cyber landscape.

Take advantage of available (and often free) resources. To learn about IT fundamentals or to supplement and build a cyber skill set, many resources can be found online, often free. Educational platforms such as *Coursera* and *edX* offer cybersecurity, IT, and computer science courses. Interactive platforms like *Codeacademy* teach a number of different programming languages. Organizations such as the National Institute of Standards and Technology (NIST) and the SANS Institute offer numerous publications related to cybersecurity. The US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) hosts a Virtual Learning Portal for those interested in learning about OT cybersecurity. Learning IT and cyber skills can also be fun: games such as CheckiO and apps like Py teach users basic coding techniques.

Ask questions. If your school, workplace, or social circle include cybersecurity professionals, engage with them about their experience and career paths. Academic and professional lectures and conferences related to cybersecurity are often open to the public and offer great opportunities for questions and discussion with cyber experts. Further, events such as the recent **Women's Cyber Forum 2017** organized by the Energypact Foundation are held particularly to encourage women's endeavors in cyber.

Get involved. Another way to engage with the cyber community is to join a professional association or group. Organizations such as Women in IT Security (WITSEC), the Women's Society of Cyberjutsu, and Women in Cybersecurity (WiCyS) among others offer women from all backgrounds an opportunity to network with female professionals, discuss issues, list jobs, and share experience.

These are just some examples of ways to build the knowledge and skills needed for a successful cyber career. Of course, soft skills such as oral and written communication, good teamwork, and problem-solving abilities are also critical for jobs in the cyber field. Whether embarking upon a new opportunity or transitioning to another role in cyber, continuously seeking more information and the perspectives of cyber professionals are always good practices to stay current and involved in the field of cybersecurity.

THE CYBERSECURITY CHALLENGES AND SOLUTIONS IN THE ENERGY SECTOR

Piotr Ciepiela
Executive Director, OT/ IoT Security leader for EY EMEIA

Jacek Walaszczyk
OT/ IoT Security Expert at EY EMEIA Advisory Center

IMPACT OF CYBER THREATS ON THE SECURITY OF THE ENERGY SECTOR

Digital reality, which is crucial for both our society and the economy, is highly dependent on applications, systems, and other IT solutions. With the increasing dependence on information technology, the number and "attractiveness" of cyberattacks also increase, which can result in extensive damage not only in the digital world, but also in the physical infrastructure and people's businesses' and the state's assets. Attacks carried out in virtual world - unlike their traditional counterparts - are characterized by:

Relatively low cost & "convenience" of execution - in the vast majority of cases, they require only a computer, Internet connection and knowledge (they are not subject to limitations resulting from differences in the geographic location of the attacker and the target);

Lower risk for the perpetrators - mainly due to lack of physical threat to the attackers;

High repeatability - assuming that the attacker will prepare specially crafted malicious software in order to perform the attack, he can easily replicate it, and then attack different target again after minor adjustments.

While in the past the cyberattacks were mostly connected with potential losses in the digital space, nowadays outcome of these types of attacks can be actual losses in physical assets. As a result of digital attacks, not only sensitive data, intellectual property and know-how are becoming threatened, but also material wealth, and even health and human life - these types of attacks have taken the term cyber-physical.

The specificity of cyber-physical incidents is that they are carried out by persons with extensive knowledge of industrial control systems and are preceded by the phase of the reconnaissance of the production environment (mostly unnoticed). The purpose of this initial phase is to identify the architecture of OT environment and all potential vulnerabilities and, as a result, to develop a specific scenario for the attack.

The abnormal operation of OT components is usually caused by changes in the setting of set points, bypassing of the interlocks, by the forcing of the control signals, communication disruptive etc.

Advanced Metering Infrastructure (AMI) infrastructure is very good example of technology which become more and more popular in energy sector but which is not free from vulnerabilities and weaknesses. Based on our experience in testing of AMI devices we can say that knowledgeable hacker is able to modify configuration settings of these devices or perform Denial of Service attack resulting financial loses of Electricity suppliers depending only on attack scale.

The response to increasingly advanced attacks in the OT environment is a new trend in the security area, namely the advanced security solution dedicated to industrial world.

Recently, security in OT area was mainly based on properly designed network segmentation and perimeter security, most commonly deployed in the form of a firewall between the IT layer and OT. At present, we may see numerous new security solutions dedicated to the OT environment like Industrial Firewalls and Intrusion Detection Systems (IDS) supporting OT specific protocols.

These solutions, developed over the last few years, have capabilities to analyze industrial protocols and has greatly enhanced the ability to monitor the security of industrial control systems.

The biggest challenge nowadays for OT security monitoring area is to optimize the existing solutions on the market to ensure the compatibility of the particular components, to gather the optimum amount of information, and to ensure that security personnel responsible for incident handling have an effective and supportive tool in the process.

It should be noted that the technology layer is only one of the security areas. Without adequately developed organization and process layers, regulating the area of security incident management, management of OT environment security becomes very ineffective. Response for this needs is another trend in OT security – Security Operational Center (SOC) dedicated to OT environment – the unit in organization responsible for monitoring and incidents handling. Rapid development of technology and ongoing changes to IT / OT integration increase the risk of cyber attacks on critical industrial processes. Hence, there is a need for a comprehensive approach to security covering all of its areas, therefore SOCs dedicated to OT covering organization, processes and technology is one of biggest challenges in cybersecurity world.

THE FUTURE OF CITIES IS SMART

Dr. Sigrid Schefer-Wenzl and Dr. Igor Miladinovic
Computer Science and Digital Communications, FH Campus Wien

In recent years we have noticed an immerse success of connected devices in both, consumer and business market segments and across multiple industries. These devices together with the corresponding networks are also called Internet of Things (IoT). All predictions on the amount of IoT devices show in the same direction – a massive growth of the number of IoT devices in the next years resulting in multiple tens of billions connected devices by 2020 (e.g. in [1] Gartner Inc. predicts 20,797 million of IoT devices in 2020).

On the other side, the administration of public resources and services in the majority of cities today does not reach the optimal level. One of the reasons for that is a lack of transparency of the needs for and usage of these resources and services. Without this transparency, a targeted and tailored optimization of city administration is not possible. Data from various sources, such as sensors, cameras or vehicles, need to be collected, analysed and evaluated in order to gain the current state of these resources and services. The aim of smart cities IoT concepts is to improve the quality of public administration by continuous measurements of city data and adapting behaviour of people and things accordingly [2, 3].

A precondition for a smart city is an open IoT architecture enabling all public services to use a common infrastructure exchanging data for cross-optimization [4]. Figure 1 shows a possible smart city IoT architecture based on an IoT architecture we presented in [5].

At the street layer, sensors, devices and networking components collect data, connected either directly or via an IoT gateway. Examples are magnetic sensors, video cameras or lighting controllers.

The city layer is composed of network routers and switches building an IP network adjusted to the size of the city data that need to be transported. At the data center layer, sensor data are processed and made available for the application layer. The key technology in the data center layer is the cloud providing a secure, scalable, elastic, and reliable data processing infrastructure. The application layer provides control and visibility of the collected data according to the specific needs of each user type. There exist several use cases where IoT concepts can be successfully integrated into smart cities.

One example is smart parking. Ineffective parking management is a constant challenge in cities around the world. It contributes to pollution, causes frustration and increases traffic incidents. Parking sensors including in-ground magnetic sensors, video-based sensors and radar sensors may be connected over IoT gateways and indicating availability of parking spaces. An application shows the parking availability on smart phones where an action, for example booking, can be taken. The application can support drivers with disabilities to locate suitable parking spots. Furthermore, city operators can monitor and analyse the city parking situation, parking officers can take real-time actions on parking time violation, citizens can find available parking spots and use online payment.

A layered IoT architecture is a precondition for successful IoT deployments. There exist several examples of pilot smart city projects around the world. However, all of them are focusing on specific public services. In the future, it will be necessary to leverage IoT infrastructure across all public services – to really make our cities smart.

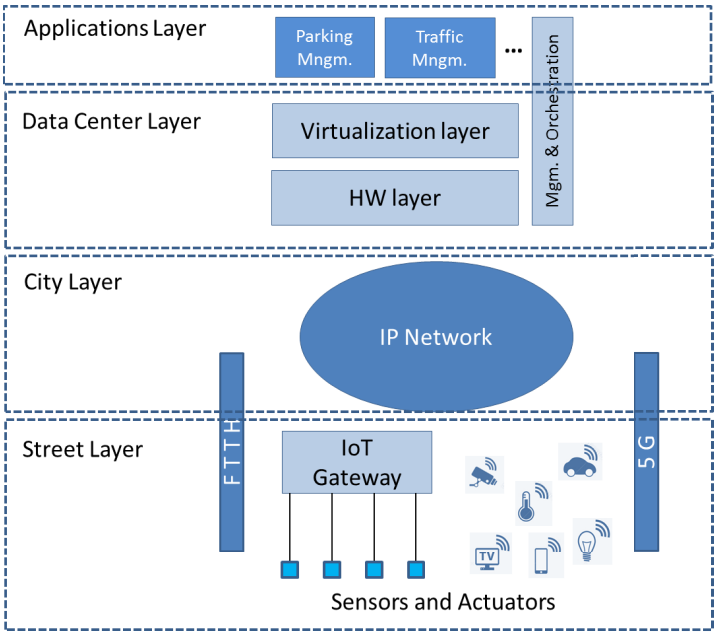

Figure 1: Smart City IoT Layered Architecture

REFERENCES

[1] Gartner Inc., "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015," http://www.gartner.com/newsroom/id/3165317, Nov. 2015.

[2] Andrea Zanella et al., "Internet of Things for Smart Cities", IEEE Internet of Things Journal, Vol. 1, No. 1 Feb. 2014.

[3] Ejaz Ahmed et al., "Internet of Things Based Smart Environments: Stat of the Art, Taxonomy and Open Research Challenges" IEEE Wireless Communications, Oct. 2016.

[4] David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton, Jerome Henry, "IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things", Cisco, Jun. 2017.

[5] Igor Miladinovic and Sigrid Schefer-Wenzl, "A Highly Scalable IoT Architecture through Network Function Virtualization" in VLIoT 2017, International Workshop on Very Large Internet of Things, Munich, Germany, Aug. 2017.

CYBER SECURITY NEWS DIGEST

CYBER SECURITY FIRMS TURN TO ARTIFICIAL INTELLIGENCE AS HACKING THREATS RISE

Cyber security companies are turning to artificial intelligence and machine learning tools to ward off growing number of attacks on networks, Finland-based internet security firm F-Secure said. As the world is fast moving towards Internet of Things and connected devices, deployment of artificial intelligence (AI) has become inevitable for cyber security firms to analyse huge amount of data to save networks from infiltration attempts, F-Secure's Security Advisor Sean Sullivan said. Networks are persistently exposed to threats like malware, phishing, password breaches and denial of service attacks. On a daily basis, F-Secure Labs on an average receives sample data of 500,000 files from its customers that include 10,000 malware variants and 60,000 malicious URLs for analysis and protection, Sullivan said.

More info: http://profit.ndtv.com/news/tech-media-telecom/article-cyber-security-firms-turn-to-artificial-intelligence-as-hacking-threats-rise-1780119

OMAN ON TOP IN CYBER SECURITY READINESS IN ARAB WORLD

Oman has emerged first in the Arab world, and fourth in the world, for cyber security, according to the latest Global Cyber Security Index (GCI) published by the International Telecommunications Union (ITU), the United Nations' specialised agency for information and communication technologies. The Sultanate secured its high rank in the index, which measure each nation's level of cyber security preparedness, through its focus on the five main pillars of cyber security — legal, technical, organisational, capacity building and cooperation — according to Engineer Badar Ali Al Salehi, Director General of Oman National CERT (Computer Emergency Readiness Team).

More info: http://gulfnews.com/news/gulf/oman/oman-on-top-in-cyber-security-readiness-in-arab-world-1.2130299

HIGH-SPEED DATA ENCRYPTION COULD BE THE SOLUTION TO FUTURE CYBER SECURITY THREATS

In a bid to fight against the future cyber threats, scientists have developed a new system with high-speed encryption properties that drives quantum computers to create theoretically hack-proof forms of data encryption. Representative image. The novel system is capable of creating and distributing encryption codes at megabit-per-second rates, which is five to 10 times faster than existing methods and on par with current internet speeds when running several systems in parallel.

More info: http://www.firstpost.com/tech/news-analysis/high-speed-data-encryption-could-be-the-solution-to-future-cyber-security-threats-4228379.html

RUSSIA TO LAUNCH 'INDEPENDENT INTERNET' FOR BRICS NATIONS - REPORT

The Russian Security Council has asked the country's government to develop an independent internet infrastructure for BRICS nations, which would continue to work in the event of global internet malfunctions. Russia won't disconnect from global internet, works on cyber security – Kremlin The initiative was discussed at the October meeting of the Security Council, which is Russia's top consultative body on national security. President Vladimir Putin personally set a deadline of August 1, 2018 for the completion of the task, the RBC news agency reported. While discussing the issue, members of the council noted that "the increased capabilities of western nations to conduct offensive operations in the informational space as well as the increased readiness to exercise these capabilities pose a serious threat to Russia's security."

More info: https://www.rt.com/politics/411156-russia-to-launch-independent-internet/

WKO AUSSENWIRTSCHAFT AUSTRIA

CSP AUSTRIA

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

energypact

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

International Multistakeholder Conference, Training & Exhibition

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

SECURITY & DIPLOMACY
29 - 30 January

TECHGATE

ENERGY, TECHNOLOGY & SECURITY
31 January - 02 February

With the support of

ITU

OSCE

IEC

BUNDESKANZLERAMT ÖSTERREICH

EUROPE INTEGRATION FOREIGN AFFAIRS
FEDERAL MINISTRY
REPUBLIC OF AUSTRIA

FEDERAL MINISTRY OF DEFENCE AND SPORTS

BM.I REPUBLIC OF AUSTRIA
FEDERAL MINISTRY OF THE INTERIOR

bmvit
Federal Ministry
for Transport,
Innovation and Technology

With courtesy of

DIGITAL CITY WIEN

OMV

KPMG

KURATORIUM SICHERES ÖSTERREICH

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

International Multistakeholder Conference, Training & Exhibition

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

SECURITY & DIPLOMACY
29 - 30 January

TECHGATE

ENERGY, TECHNOLOGY & SECURITY
31 January - 02 February

SECURITY & DIPLOMACY		ENERGY, TECHNOLOGY & SECURITY		
DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
CYBERSECURITY FOR CRITICAL (ENERGY) INFRASTRUCTURE: A GLOBAL CHALLENGE	**SAFEGUARDING CRITICAL ENERGY INFRASTRUCTURE IN THE CONTEXT OF REGIONAL AND GLOBAL SECURITY: STRATEGIC AND DIPLOMATIC ASPECTS**	**TRENDS IN TECHNOLOGY AND CYBER SECURITY**	**SECURING ENERGY ECONOMY: OIL, GAS, ELECTRICITY & NUCLEAR**	**SECURING SMART CITIES AND EMERGING TECHNOLOGIES**
Official opening	Session 1: Operational considerations for responding to the threat of cyber-attacks on critical energy infrastructure	Cyber Range Tutorial: Concept, Demonstration, Exercises, Training and the Cyber Research Project	Session 1: Emerging and Future Threats to Digitalized Energy Systems	Session 1: Making Smart Cities Cyber Secure
Session 1: Implementing the EU Strategy for Safe, Open and Secure Cyberspace	Session 2: Reducing the Risks of Conflict Stemming from the Use of Cyber-Capabilities	Cyber Security Cluster Austria (CSCA) Day 2018: Exhibition on leading-edge cybersecurity technologies	Session 2: Cybersecurity Standards in Critical Energy Infrastructure	Session 2: Austrian IoT Safety & Security light house initiatives
Session 2: Cyber-Threats to Critical Energy Infrastructure	Session 3: Cyber-Diplomacy: Developing Capacity and Trust Between States	Reception of the organizers of the CSCA Day 2018	Session 3: Cybersecurity & Resilience in Transport Infrastructure	Session 3: The Promise and Challenge of New Technologies
			Session 4: Public sector, industry, and research cooperation in cybersecurity	Concluding Statements
Diplomatic Academy of Vienna 15A Favoritenstraße, 1040 Vienna U1 Taubstummengasse		Tech Gate Vienna 1 Donau-City-Straße, 1220 Vienna U1 Kaisermühlen VIC		

The second edition of Vienna Cybersecurity Week will be held in Vienna, from 29 January to 02 February 2018. This annual event aims to engage with key national and international stakeholders in dialogue and cooperation in the field of cybersecurity for critical infrastructure with a focus on the energy sector. A five-day event will offer a unique forum for both governmental and non-governmental partners to delve into substantive debates over the protection of critical energy infrastructure, combating cybercrime, cyber-diplomacy and the future of technologic development in the energy sector.

energypact foundation

VISION

An international collaborative community of technologically and risk informed leadership, researchers, implementers, and stakeholders for the development, sustainability, and security of energy production, transmission, and delivery addressing today's challenges and tomorrow's needs.

MISSION

The Energypact Foundation has directed its efforts toward three mission areas:

AWARENESS:

Promoting dialogue and international co-operation on security issues for the energy sector.

TRAINING:

Establishing the Industrial Control Systems Security Centre (ICS Security Centre) in Vienna, Austria and regional training centres around the world for providing human resource development activities for leadership, management and employees.

RESEARCH:

Nurturing a collaborative research network for the energy sector.

energypact foundation

Become a Collaborating Member of the Vienna Project

Energypact Foundation
viennaproject@energypact.org
www.energypact.org