NEWSLETTER

Vienna, July/August 2017

energypact foundation

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

energypact foundation

VIENNA CYBER SECURITY WEEK 2018

Protecting Critical Energy Infrastructure

Intergovernmental & Multistakeholder Conferences – Training – Technology Exhibition

CSP AUSTRIA

29 January - 02 February

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

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Jointly organized by the Austrian and international governmental and non-governmental partners and the Energypact Foundation. This centrepiece annual event aims at engaging with key national and international stakeholders in dialogue and cooperation in the field of cyber security for critical infrastructure with focus on the energy sector.

SAVE THE DATE

Intergovernmental Strategic Conference

A STRATEGY FOR CYBERSPACE AND ENERGY SECURITY

State level information exchange forum for discussion on strategies and good practices in advancing the security of cyberspace and critical energy infrastructure.

International Multistakeholder Conference

TECHNOLOGIES AND BUSINESS ENABLERS FOR DEVELOPING RESILIENCE IN CYBERSPACE

Technology driven discussion on research and state of the art technologies and their practical implementation for building cyber resilience.

Building Awareness

CYBERSPACE AND ENERGY SECURITY TRAINING

Computer Security training will be provided during the week to build awareness of the cyber threats, the associated risks and to sound programmatic elements for cyber protection and mitigation.

Supporting Knowledge

INTERNATIONAL CYBERSPACE TECHNOLOGY EXHIBITION

Austrian and other international exhibitors and experts will promote awareness building, through demonstration of commercial and research technologies to enhance cyber security and their application within the energy sector.

Should you have an interest in presenting or event sponsorship, please contact: viennaproject@energypact.org

BEGINNINGS OF A CYBER HOT SUMMER

The WannaCry and Petya ransomware attacks against critical infrastructures in May and June 2017 highlight the dynamic nature of cyber security challenges in the power sector. This edition of the Energypact newsletter provides industry perspective on cyber security from Mr Jordan Georgiev, former CEO of Bulgarian Energy Holding. Ms Kamilla Csomai, CEO of MAVIR Hungarian Independent Transmission Operator Company Ltd., discusses the 4th industrial revolution for power transmission operators. Mr Walter Wutzl, Siemens AG Oesterreich, provides an overview of computer security projects initiated to secure energy systems in Austria. Finally, Mr Szabolcs Hallai discusses information sharing initiatives occurring within the energy sector in Hungary.

Enjoy reading!

CYBER SECURITY IN THE ENERGY SECTOR: CHANCES AND CHALLENGES

Jordan Georgiev, former CEO of Bulgarian Energy Holding

We all benefit from a digital, global and interconnected economy. Digitalization is the major trend of the recent years, brings new business models and convenience to everyday life and unlocks enormous economic potential across all industries.

Energy companies, being traditionally late adopters of cutting-edge information technology are cautiously exploring those new digitalization opportunities. New technologies are used to control energy production, monitor demand and consumption and exchange data, thus pushing the physical operational and digital information technology (OT and IT) of an energy company to become more interconnected and reliant upon each other. This interdependency tremendously increases the efficiency of the energy company operations and helps them cope with the challenge of increasing number of connected market participants. But those benefits to energy companies come with a price tag of increased vulnerability and exposure to cyber-attacks – cyber security incidents increase in frequency, impact and complexity. ENISA, the European Union Agency for Network and Information Security ranks the energy sector in having the second highest cost per cyber security incident and together with the financial services sector also suffers the strongest economic impact due to cybercrime. A cyber security incident in the energy sector does not only impact the company under attack, but can trigger economic or financial disruptions across other sectors, threaten the health and lives of the population and cripple the defense capability of a country as a whole. A cyber-attack is not only resulting in loss of data or IT systems, but can also physically damage critical assets and result in unrecoverable environmental damage.

There are several challenges in respect to cyber security an energy company is facing today. On one hand, every energy company is part of the larger, national or international energy sector. In this respect, the chain is as strong, as its weakest link. But a company in this sector is not alone in its efforts to prevent and fight cyber threats – other market participants are facing similar challenges. The European Directive on Security of Network and Information Systems (NIS-Directive) sets out minimum security and notification requirements for operators of essential services, including energy companies. It not only promotes the cooperation between member states, but also strengthens the national cyber security capacity by introducing the Computer Security Incidence Response Teams (CSIRTs) and encourages the sharing of incident information. This information exchange will help to create the "big picture" of threats and vulnerabilities and support the timely deployment of adequate preventive and counter-measures against cyber-attacks. As a next step, the creation of guidelines for cyber risk assessment and a scheme for "pricing" of security investments should further encourage energy companies to boost investments in securing their infrastructure.

On a corporate level, few other challenges are worth mentioning. First, the energy companies were mainly focused on two main areas: safety for their customers and employees and maintaining high

reliability and quality of supply. Until recently, cyber threats were not considered a threat to those areas. As a result, metrics for efficacy of cyber security measures are underdeveloped or even non-existent. Most utilities have well-developed methodology to mitigate traditional risks and it could be applied also to cyber security risks, in order to provide better understanding and argumentation for future investments. Security should become integral part of the overall risk management strategy of every energy enterprise. Centralized oversight over all security aspects should be introduced with the appointment of a Chief Security Officer (CSO), who should have ultimate control and responsibility for securing IT and OT across all lines of business. A second large challenge is the increasing complexity of OT and IT landscapes and their interconnectedness. The traditional role of the IT department as "order-taker" of the business is not sufficient anymore. The regulators and consumers demand "security by design". The earlier IT and cyber security thinking is involved in every project, product and service an energy company is planning, the better is the outcome for security, manageability and acceptance. The constant collaboration between business lines and IT should be promoted heavily, starting from the corporate strategy creation, where IT strategy should become an integral part and going all the way through third-party technology selection to deployment of infrastructure assets. Here, on top of the physical, the digital security should come up front. This is the new world of Internet of Things (IoT), where IoT security demands more from a company, than IT security alone.

And last, but not least – the human factor. In 2016, the ICS-CERT Incident Response team completed work on 290 incidents in the US, where the energy sector accounted for around 20% of those incidents. Spear-phishing represented 26% of the total incidents, making it the leading access vector for cyber-attacks. Segmentation of sensitive systems and information is crucial, but sometimes convenience of users overshadows security considerations. Therefore it is crucial for an energy company to constantly adapt its security guidelines to respond to emerging threats and keep the awareness level of its employees in the matter of cyber security on the highest level possible. Obviously, this is valid for all organizations, but we still tend to forget the obvious.

[1] The cost of incidents affecting CIIs, August 2016, ENISA
[2] Directive (EU) 2016/1148 of the European Parliament and of the Council, July 2016
[3] ICS-CERT Year in Review, 2016

THE CYBER SECURITY CHALLENGES OF THE 4TH INDUSTRIAL REVOLUTION FROM THE TSOS' PERSPECTIVE

Kamilla Csomai, CEO of MAVIR Hungarian Independent Transmission Operator Company Ltd., member of the board of the European Network of Transmission Service Operators

We live in the age of the 4th industrial revolution. By 2020, at least 50 billion devices ranging from cars to coffee machines will be connected to the internet generating approximately 75 trillion gigabytes of data.

From 150 000 in 2015, there will be at least 18 million Battery Electric Vehicles (BEVs) in Europe by 2020 as charging becomes more widely available and cities invest in smart & clean mobility based on European Enviroment Agency report. In electricity, all consumers should by then be equipped with smart meters. The sheer numbers clearly demonstrate that the electricity transmission networks and their operators need to digitally link the different networks to gain in efficiency and service as well as develop an extra layer of dataflow allowing new ways of consuming and producing energy.

These challenges accelerate the speed of digitalisation in the electricity sector that make electric utilities increasingly vulnerable to cyber-attacks. By now, the utility systems have adopted a growing number of digital control, operation, metering and resource management systems that became more interconnected and complex.

In addition, the widespread connection of solar, wind and other distributed energy resources with two-way digital controls also led to new cyber security vulnerabilities. Last but not least, the collection and dissemination of large amounts of energy production and consumption data raised national security and privacy concerns over the ownership and management of these critical data.

To tackle these challenges, transmission service operators need to apply a strategical approach with a comprehensive set of actions ranging from cyber security and data protection policies through collaborations to technological measures.

The European Network of Transmission Service Operators (ENTSO-E), gathering 43 transmission system operators from 36 European countries, realised this need for action and on June 20th, 2017 signed a memorandum of understanding (MoU) with the European Network for Cyber Security (ENCS) to develop state of the art cyber security regulation, practices & standards for the electricity transmission system.

Under the MoU, ENCS and ENTSO-E will share expertise and resources: ENCS providing ENTSO-E with technical information and support on cyber security issues while ENTSO-E will give ENCS insights into the European transmission system and the particular challenges faced by its operators. This closer collaboration agreement results from a series of hacking and security training programmes organised by ENCS in which ENTSO-E and its members participated.

CURRENT DEVELOPMENTS AND TECHNOLOGICAL SOLUTIONS FOR CYBER SECURITY IN POWER GRIDS

Walter Wutzl, Head of Digital Grid Automation Products Siemens Austria

Power utilities are becoming more and more dependent upon automation and process networks. At the same time, necessary interconnectivity via internet and other partner networks increases potential vulnerability to cyber dangers of hacking, manipulation and/or destructive intervention of process networks. Another issue for consideration is the longer system lifetime of 10-20 years, creating a situation where the majority of any utility's equipment is from 5 to 10 years old, and 100% replacement is neither commercially nor technically feasible. Recent cyber-attacks have demonstrated the scope of such dangers and their serious impact upon the business activities of energy-dependent companies, especially power utilites.

There are defined approaches to improve cyber security in the electricity sector, e.g. from the organization of German Utilities (BDEW) and North American Electric Reliability Corporation (NERC), which have issued stringent guidelines and requirements to achieve cyber security for power utilities.
Many product suppliers have implemented security features already, but standards and secure products alone are not enough to ensure secure networks.
A systematic approach is needed; therefore, Siemens has undertaken research/ pilot projects and joint developments with utilities, universities and governmental organizations for approaches to ensure secure energy systems.
These projects and developments apply strategies for network segmentation (e.g. office, control center and substation zones), secured data transmission and maintenance issues that constitute a layered defense, which, in turn, can be designed into a new substation and /or grid control system architecture, but these features can be integrated as security upgrades into existing systems, as well.
One example of such pilots is the Secure Substation Project with a leading Austrian power utility, set in a carefully-selected section of the grid, where power generation and distribution assets interact with a heterogeneous system of automation, protection and remote control products. The pilot project was based upon general guidelines issued by BDEW and "Austria's Energy" (OE) that provide references to applicable harmonized technical standards.

Our pilot project was specifically designed to realize the complete BDEW requirements on a small section of the grid and to perform a commercial evaluation of the risk mitigation benefits against total cost, in order to define an optimum result for the utility partner. It improved the security of the installed base, using systematic analysis of installed equipment and systems, building upon and expanding existing security measures.
In this pilot project, together with the utility, we implemented sound technical solutions with acceptable investments in time, effort and equipment. These goals were successfully achieved while maintaining compatibility with existing systems and their functionality.

THE POWER OF TRUST

Szabolcs Hallai – Founder and manager of IT Business Consulting Hungary

In the antique world real history was made, when the ancient Greek city-states developed during the Archaic period as the ancestor of city, state, and citizenship and persisted though with decreasing influence well into Roman times. The term polis, which in archaic Greece meant "city", changed with the development of the governance center in the city to signify "state", which included its surrounding villages. Finally, with the emergence of a notion of citizenship among landowners, it came to describe the entire body of citizens. The best form of government of the polis for Plato is the one that ***leads to the common good.*** *

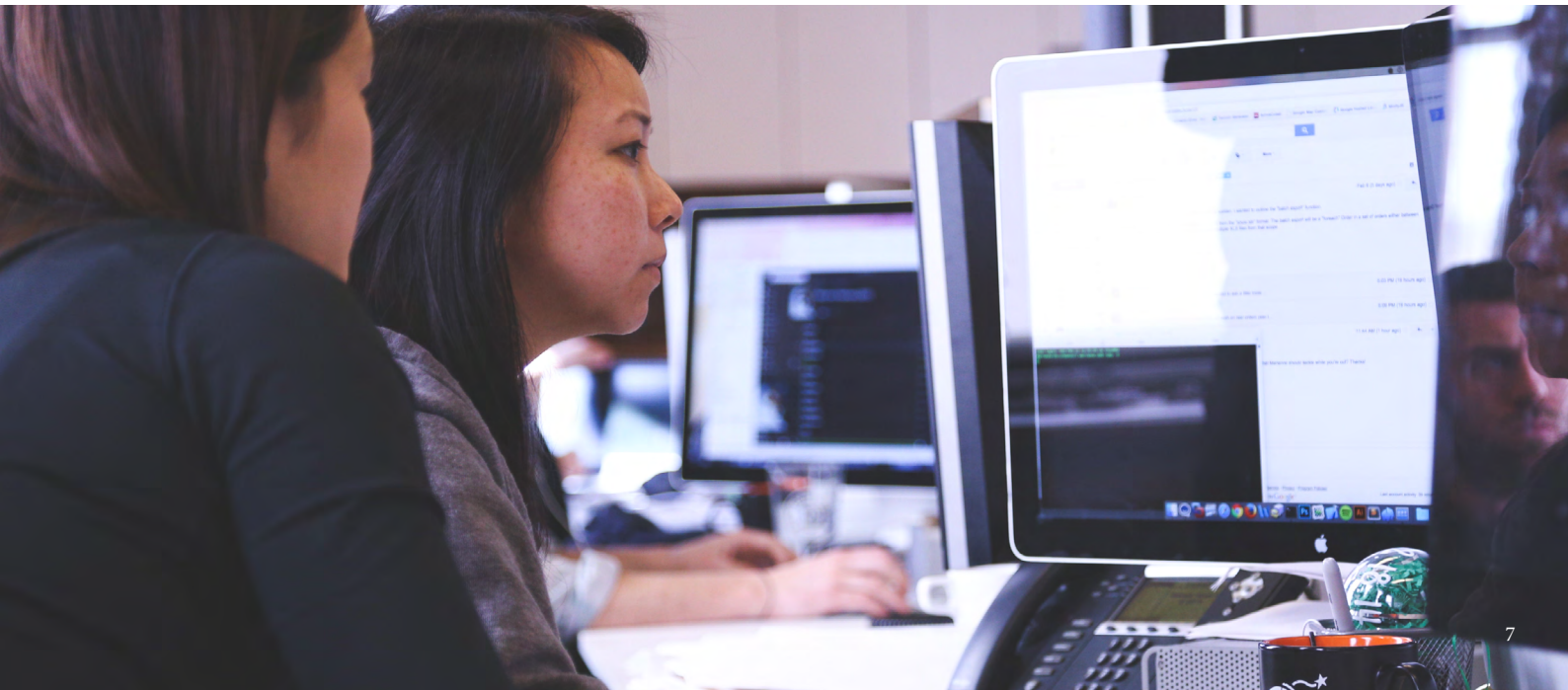
Nowadays it seems that working in cyber security domain is an endless tread wheel of fighting against systemic vulnerabilities and human data leakage. During this fight against processes and zero-day threats the professionals often forget to look around, take a deep breath and start to collaborate with companions in distress. We, the cyber professionals in energy sector, are not alone in our efforts and can start to organize and help each other to achieve results that ***leads to the common good***.

In 2014 within Hungary's energy sector, a new initiative began called the Hungarian Energy Security Forum. In the beginning it was no more than a group of CISO's and CSO's from the big power grid contributors siting around a table discussing everyday challenges. We took a notice of a rare Trojan infecting only in SCADA environments or watch a shot of transformer-tower fire put out by local fire brigade. After a period of time, however, we noticed that the chain of trust had been built and was growing not only with new Hungarian participants but of those from Slovenia and Croatia. In 2015, the Hungarian Energy Agency sponsored the Hungarian Energy Security Forum (HESF) to declare a new Hungarian Cyber security Strategy for Energy Sector. In the strategy declared the need for cooperation and the development of Information Sharing and Analysis Center for Energy Sector or e-ISAC to provide a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector that hopefully will ***lead to the common good***.

In 2017 Q1 and Q2 the e-ISAC.hu was developed and made ready for beta testing. It collects feeds of threats from more than 50 sources including major ICS CERTs and big ITSEC vendors. The format was planned to provide full anonymity for those members who do want to share information about their incidents but without disclosing themselves. We are planning to have segregated forums for each sector (power, gas, water, other utilities) and for the invitation only VIP HESF. Sponsored by the Hungarian Energy and Public Utility Regulatory Authority, the e-ISAC will provide comprehensive information from Hungarian, EU and USA governmental agencies (GOVCERT, LRLIBEK, NEIH, ENISA, NIST, EU-ISAC, CERTs etc.) not only for big grid contributors but also for small and medium energy companies with limited IT resources. If only one more threat will be recognized yearly and then every year the double of the previous period, and wiped out by the help of e-ISAC this will provide more security for the energy supply and ***lead to the common good.***

After the introduction to more than 4000 licensees of Hungarian Energy and Public Utility Regulatory Authority in November 2017, the e-ISAC plans to include members from neighbouring countries (Austria, Slovenia, Croatia…) as well as to invite agencies/organizations specialised in fighting cyber-attacks (USA Department of Homeland Security, ENISA, CEER, ACER, CyberPol etc.) thus providing that extra edge for our members. Energy stakeholders in Hungary believe that e-ISAC and the chain of trust built around it will actually lead to the common good.

*Source: Wikipedia



CYBER SECURITY NEWS DIGEST FOR SUMMER 2017

EU AGREES TO JOINT SANCTIONS ON CYBER-ATTACKS

The EU has agreed to use a "cyber diplomacy toolbox" against hackers targeting member states. The move comes amid concern hackers may seek to influence German elections in September. EU foreign ministers meeting in Luxembourg said in a statement that the bloc would use a "cyber diplomacy toolbox" to respond to malicious cyber activities targeting computer systems.
"A joint EU response to malicious cybera ctivities would be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity," foreign ministers said in a statement. So-called restrictive measures typically target individuals, groups, companies or governments with travel bans, asset freezes and restrictions on doing business.

More info: https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#65ff52117abd

PETYA AND NOTPETYA, ANOTHER MASSIVE RANSOMWARE OUTBREAK GOING GLOBAL FAST

Ukraine's government, National Bank, its transportation services and largest power companies are bearing the brunt of what appears to be a massive ransomware outbreak that's fast spreading across the world and hitting a significant number of critical infrastructure providers, e.g. Danish shipping and energy company Maersk, U.S. pharmaceuticals company Merck.

More info: http://www.dw.com/en/eu-agrees-to-joint-sanctions-on-cyberattacks/a-39314085

ESTONIA BUOYS CYBER SECURITY WITH WORLD'S FIRST DATA EMBASSY

To protect itself from cyber-attacks, Estonia is about to open a "data embassy" outside its borders. The "embassy," in Betzdorf, Luxembourg, will safeguard what Estonian society depends on - its online data and infrastructure. It is there, in a high-security, "Tier-4" data centre where Estonia's most critical, confidential data will be stored. Under a bilateral agreement between the Estonian and Luxembourg governments expected to be signed within weeks, the Estonian data will receive the type of protection and immunity given "regular" embassies under the Vienna Convention, the 1961 international treaty that defines diplomatic relations between independent countries. That means that officials from the host country, in this case Luxembourg, will be barred from accessing the data.

More info: http://www.dw.com/en/estonia-buoys-cyber-security-with-worlds-first-data-embassy/a-39168011

SENATORS SAY CYBER SECURITY SHOULD BE TOP PRIORITY FOR AUTONOMOUS VEHICLES

The U.S. Senate Commerce, Science, and Transportation Committee released bipartisan principles for AV legislation. The document states that cyber security must be included 'from the very beginning of their development,' and that "Legislation must address the connectivity of self-driving vehicles and potential cyber security vulnerabilities before they compromise safe.

More info: http://www.securityweek.com/senators-say-cybersecurity-should-be-top-priority-autonomous-vehicles

JAPANESE HONDA FACTORY HIT WITH WANNACRY RANSOMWARE, HALTS PRODUCTION

A Honda plant in Sayama, Japan was forced to halt domestic production for a day in June after its network was hit with WannaCry ransomware. The plant has a daily output of around 1,000 vehicles and produces models including the Accord sedan, Odyssey Minivan and Step Wagon compact multipurpose vehicle. Researchers said the loss in productivity in just one day most likely took a toll on the auto manufacturer.

More info: https://www.scmagazine.com/wannacry-attacks-halts-honda-production/article/670273/

ENERGYPACT ANNOUNCEMENTS

1. Energypact Diplomatic Café
The Energypact Foundation will initiate a monthly diplomatic round table forum to promote discussion and information exchange on international and national cyber security issues relevant to the energy sector. The format of a small group lunch and a guest speaker will commence in Fall 2017 in Vienna, Austria. Discussion will focus on different topics each month and participation will be drawn from the diplomatic and technical leadership from the state missions and embassies and international organizations based in Vienna.

2. Cyber Security Forum: Launching Careers in Cyber Space
In its mission to promote awareness and encourage human capacity development in cyber security professions, Energypact Foundation is developing a seminar promoting professional careers in cyber security, with a focus on opportunities for women professional. The seminar is designed for young professional women (and men) with an interest in cyber security issues. Desired attendees include women and male allies already engaged or considering careers in cyber security, including university students and faculty, industry professionals, members of the government, and professional organizations. The seminar is planned for Q4 2017.

3. Hale and Farewell
The Energypact Foundation completes its relocation to Vienna. Energypact would like to thank Mr Ferenc Suba for his outstanding contributions while serving as the acting Executive Director during this transition period. Mr Suba is pursuing new career interests and will continue to provide technical advisory support to Energypact. From September 2017, Mr Alexandre Dimitrijevic, the president of Energypact Foundation will assume the role of Executive Director.

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