NEWSLETTER

Vienna, June 2017

energypact foundation

"SOME GOVERNMENTS SAY WE DON'T HAVE CYBERCRIME IN OUR COUNTRY, WE DON'T SEE ANY THREAT HERE"

IN WAKE OF 'WANNACRY' ATTACKS, UN CYBERSECURITY EXPERT DISCUSSES INTERNET SAFETY

by Paulina Kubiak, UN News Centre

"Some governments say we don't have cybercrime in our country, we don't see any threat here"

19 May 2017 – A United Nations cybersecurity expert says that cybercrime is ultimately preventable, and that the internet – even the hidden so-called ***'dark net'*** – has very good elements to it.

That may seem difficult to believe for people in the 150 countries hit by the ***'WannaCry'*** ransomware, some of whom have had to pay hundreds of dollars in digital currency, Bitcoin, to get back photos of their families and other files on their laptops, or the families unable to board a train in Germany or see a doctor in the United Kingdom.

"Law enforcement and diplomats have been warning people of ransomware for some time, but this is really the first time that we've seen an attack of this size," said Neil Walsh, Chief of Cyber and Emerging Crime at the UN Office on Drugs and Crime (UNODC).

Last Friday's attack was due to a strain of Windows ransomware – which like the name suggests, encrypts files and holds them ransom. It entered individual systems as a compressed zip file through a security loophole in the Windows operating systems, and went on to scramble information in hundreds of thousands of machines belonging to hospitals, banks and other organizations around the world.

Mr. Walsh told UN News that the attack attributes its success to the fact that the operating systems used by those companies were old and did not have a security patch.

His advice boils down to clicking yes to software updates, using an up-to-date antivirus system, and backing up data into a device separate from the computer.

"If you weren't expecting an attachment from someone, or it looks strange, don't open it," Mr. Walsh added.

Headquartered in Vienna, and with teams in Guatemala, El Salvador, Tunisia and Thailand, Mr. Walsh's role is to help create an inter-governmental response to cybercrime. That involves, in part, public outreach about internet risk, including to children and their parents, and working with police, prosecutors and judges around the world to improve how cases are investigated and tried.

Despite the increased number of cybercrimes in the past several years, some governments do not understand cyber risk, he said.

"It still never fails to amaze me that some governments say we don't have cybercrime in our country, we don't see any threat here," Mr. Walsh noted. "***And technically that means that they don't have the capability to identify, to look for and to respond to it. So my role, and the role of my people, is to help governments understand that and to help them put strategies in place to minimize that risk to them."***

His teams also work with victims, to make sure that they have avenues to report crimes to the police, and sometimes seeking redress from a non-governmental organization or charity.

"There's no such thing as a victimless crime, and that's the same in cyberspace as in crime committed in the physical world," he added.

For integral part of the text, visit the UN News Centre at: http://www.un.org/apps/news/story.asp?NewsID=56796#.WTGPBPnyjIX

RANSOMWARE AND THE ENERGY SECTOR

Energypact believes that the changing threat coupled with the integration of new technologies, must continue to be focal point of discussion and research.

Ransomware has made the news again with the immergence of the WannaCry Ransomware worm on 12 May. Over 230,000 computers in 150 countries have been infected including critical infrastructure most notably healthcare providers, but also utilities and manufacturing sites have been impacted. [1]. These attacks appear to be of a criminal nature, indiscriminate and not targeted against specific infrastructure.

The ransomware exploits vulnerability in the SMB of Windows operating systems where it encrypts selected files of the infected systems and appends .WCRY to the end of the file name. The ransom is $300USD that is required to be paid in Bitcoins.

Ransomware is not new having first appeared in 1989 at a World Health Organization (WHO) conference were the AIDS Trojan was distributed via infected diskettes to conference attendees. [2] Ransomware denies the availability of information and/or resources via one of two mechanisms: by locking user access out of a device or by the encryption of files on a device. Ransomware targets all types of operating systems.

While the WannaCry targeted primarily IT systems, what is the concern for the energy sector? First, while the energy sector relies on IT systems and COTS in operational systems, a recent research paper also shows the potential vulnerability of industrial control systems (ICS), namely PLCs, to a ransomware attack. [3] Given the rise in ransomware attacks, it is not unrealistic to believe that criminal elements will not turn to targeting ICS directly.

Second, the frequency of cyber-attacks targeting of the energy sector has grown and this trend can be anticipated to continue as more and more ICS components become digitally based. Third, the targeting of the energy sector by criminal elements for extortion is not new. In 2008, Tom Donahue, a senior Central Intelligence Agency (CIA) analyst reported that cyber-attack had compromised multiple electrical utilities outside of the US resulting in power outages while demanding extortion payments.[4]

Finally, the nature of operational technologies (OT) introduces restraints that may require addition consideration and mitigation strategies. WannaCry exploits a vulnerability, CVE-2017-0144, in the SMB of Windows operating systems. Microsoft addressed the vulnerability in MS17-010 releasing an associated patch. OT, especially ICS, may not have the flexibility for rapid patching. The patch was released in March 2017 with the Wannacry Ransomware becoming prominent in the middle of May 2017. Patched systems were immune to the attack.

A few closing thoughts. Computer security is a process and not an endpoint. The line between IT and OT continues to blur and non-targeted attacks as well as targeted attacks against either can have adverse consequences. Energypact continues to build computer security awareness and promote discussion of the new challenges facing both the IT and OT environments of the energy sector, but like security, awareness in a continual process. Additional research is needed too. Proven security controls and practices in IT may not be applicable or may need additional mitigation considerations for OT environments. Energypact as reflected in its core mission fully believes that the changing threat coupled with the integration of new technologies, must continue to be focal point of discussion and research; essential for risk informed decision making on cyber security of the energy sector.

References:

[1] https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#542e46d3425c

[2] http://www.csoonline.com/article/3095956/data-breach/the-history-of-ransomware.html#slide21

[3] http://www.cap.gatech.edu/plcransomware.pdf

[4] http://www.nbcnews.com/id/22734229/ns/technology_and_science-security/t/cia-hackers-demanding-cash-disrupted-power/

ENERGYPACT PRESENCE AT MAJOR CYBER EVENTS

INTERNATIONAL CONFERENCE "CRITICAL INFRASTRUCTURE PROTECTION CIP, FORUM" 2 ND EDITION

BUCHAREST, ROMANIA

The fourth industrial revolution. New challenges for critical infrastructure

CRITICAL INFRASTRUCTURE PROTECTION FORUM

ROMANIAN PARLIAMENT PALACE
BUCHAREST / ROMANIA
APRIL 26, 2017
2ND EDITION

OPEN PLATFORM FOR IDEAS, SECURITY AND RESILIENCE

Romanian Parliament Palace

The 2017 edition of the forum was organized Under The Patronage of The Prime-Minister of Romania.

CIP FORUM

Organised by Idea Factory Think Tank, the 2nd edition of the International Conference CIP Forum 2017 took place in Bucharest, at the Palace of the Parliament, on April 26th, 2017.

The event represented a platform for dialogue with experts, business professionals, academia, local and central public administration, and civil society at the highest levels. Ministers, state secretaries, ambassadors met with industry and acadamy leaders to share their views on the challenges of critical infrastructure protection centered around the phenomena and movements generated by Industry 4.0: smart grid & network in the field of energy, smart city, blockchain and new risks and threats to critical infrastructure.

The presentations took note of the fact that the vital services of the society, provided by critical infrastructures - in the new digital age - of the ***"smart"*** type, will be dependent on new smart, fast and super-sophisticated technologies, but also very vulnerable to the same extent. Thus, ***"smart infrastructure"*** will be part of the ***"smart society"***, and their protection and security will be achieved through complex policies, strategies and technologies. Societal security will be directly dependent on critical infrastructures (with particular reference to cybernetics), state and non-state actors being part of a system that will develop into other co-ordinates, through rapid computerization and full change of the power paradigm for the labour market.

The criticality of these thoughts was well reflected by the success of the conference that was attended by more than 500 guests representing 125 institutions from 29 countries. The conference benefited from 57 speakers representing ministries, public authorities and private institutions, under the aegis of 10 universities and research institutes with expertise in the field.

DASICON 2017 ORGANISED BY THE OSCE

Organised by the OSCE in Vienna, two panels of the DASICON 2017 conference dealt with cybersecurity and energy security on March 4th, 2017. The conference had roughly 400 participants and more than 45000 people reached the event on livestream.

"SEEING AND UNDERSTANDING CYBER SECURITY"

An exhibition of state-of-the-art security technologies

The AIT Austrian Institute of Technology was presenting internationally cutting-edge technologies that have been developed for global companies within national and international research programs on May 30th in Vienna.

The event was rounded off by a top-class panel discussion, entitled: **"Austrian security technologies between the poles of domestic market vs. global market".**

The interconnectedness of all our technical systems offers enormous advantages. At the same time, however, it makes us a glass person who is increasingly dependent on this process. Complex systems are created which are hardly understood by humans anymore and data sets which can no longer be processed by individual persons. This results in a great demand for new tools to master this complexity and dynamism.

in cooperation with:

FUTURE EVENTS

HACK2017 ISTANBUL ORGANISED BY THE UITSEC

Organised by UITSEC (Universal IT Security Company), Hack Istanbul 2017 will be held in Istanbul, Turkey on 7-8 December 2017 as an international cyber security conference including project-based and CTF (capture the flag) style competitions. The conference will have a dedicated panel on energy cybersecurity.

VIENNA CYBER SECURITY WEEK 2018

Advanced Announcement

29 January - 02 February

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

January 29 - 30

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.

January 31 - February 01

International Multi-Stakeholder Conference

TECHNOLOGIES AND BUSINESS ENABLERS FOR DEVELOPING RESILIENCE IN CYBERSPACE

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

February 02

Building Awareness

CYBERSPACE AND ENERGY SECURITY TRAINING

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

January 29 - February 02

Supporting Knowledge

CYBERSPACE TECHNOLOGY DEMONSTRATION AND EXHIBITION

Exhibitors and experts during the week will promote awareness building, through demonstration and discussion 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

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