EU NIS directive and NIS-Law – What now?

The Network and Information System Safety Act, coming into effect in May 2018, will create new frameworks for organizational and technical information security. Operators of services that are of high importance due to their provision of public services, companies, public security and national defense institutions are the target group as a cyber security incident would lead to supply bottlenecks and threats. The breakout session discusses the impact of the new act.

Chair:
FH-Prof. DI Robert Kolmhofer
Head of Department Secure Information Systems / Member of the ITC board of advisors
University of Applied Sciences, Hagenberg, Austria / ITC Upper Austria

Coordination:
Dr. Tanja Spennlingwimmer
Head of Department Investors and Location Management
Business Upper Austria, Linz, Austria

Opening Session, Welcome and Introduction
01:00 p.m. – 01:10 p.m. Dr. Michael Strugl
Deputy Governor, State of Upper Austria

01:10 p.m. – 01:30 p.m. Impulse statement:
Critical infrastructure operation as a challenge for international digital services / cloud providers
Dr. Gerhard Eschelbeck
Vice President / CISO, google Inc. CA, USA

NIS legal/compliance
01:30 p.m. - 02:00 p.m. NIS-G compliance in national and EU context
Dipl.-Ing. Pia Hoschek, BSc
Sektion I, Abteilung I/8 – Cyber Security, GovCERT und NIS Büro
Bundeskanzleramt Österreich

02:00 p.m. - 02:10 p.m. Discussion
2018 Alpbach Technology Symposium  
Breakout Session 6  
Friday, August 24, 2018, from 1.00 p.m.  
Alpbach Secondary School (Hauptschule Alpbach)

---

**NIS technical challenges**

02:10 p.m. - 02:50 p.m.  
**NIS certification and auditing of network and information processing infrastructure important for national defence units**  
Obst.dG. Mag. Walter Unger  
Director Cyber Defence Unit - AbwA  
BMLVS, Austria

02:50 p.m. – 03:20 p.m.  
**IT security measure determination according to the state of the art**  
Tomasz Lawicki  
Head TeleTrusT Arbeitskreis „Stand der Technik“  
AC Schwerhoff / TeleTrusT, Berlin, Germany

03:20 p.m. - 03:50 p.m.  
**NIS practical implications for power grid operators**  
Thomas Pfeiffer MSc  
CISO  
LINZ STROM Netz GmbH, Linz, Austria

03:50 p.m. - 04:00 p.m.  
**Discussion**

04:00 p.m. – 04:20 p.m.  
**Coffee Break**

---

**NIS research**

04:20 p.m. - 04:50 p.m.  
**Security Research in the context of NIS**  
Dr. Edgar Weippl  
Research Director  
SBA Research, Vienna, Austria

04:50 p.m. - 05:00 p.m.  
**Discussion**
Dr. Gerhard Eschelbeck  
Vice President / CISO, google Inc. CA, USA

Impulse statement
Abstract

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. For this reason, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 (NIS Directive) is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the European Union. The NIS Directive foresees the attainment of a common high level of network and information security and thus upscaling capacities (e.g. national cybersecurity capabilities), cooperation (cross border collaboration) and risk management practices as well as incident reporting obligations across the EU Member States.
Obst.dG. Mag. Walter Unger  
Director Cyber Defence Unit - AbwA  
BMLVS, Austria

Abstract

Critical infrastructure protection: NIS Act - what now?

States depend on their strategic infrastructures. The increasing penetration and support of networked information and communication technology (ICT) systems in all areas of society leads to vital dependencies on their functioning. Cyber-attacks against strategic infrastructures, e.g. against power supply, GPS/GALILEO or other essential ICT infrastructures would be particularly threatening, as they could be launched surprisingly without warning.

To keep the damage caused by large-scale cyber attacks as small as possible, it is necessary to permanently operate a high degree of security measures for critical infrastructures. The accreditation process is an effective preventive measure. This process accompanies the entire life cycle of digital infrastructures and ensures that only high-quality, optimally secured ICT systems are introduced into organisations.
Abstract

The legislation calls for the "state of the art" in the context of IT security. Current examples are the European General Data Protection Regulation (GDPR) and the European NIS Directive (NIS). But what does the legislation exactly understand by the term "state of the art" is not further defined. In the event, the speaker assigns the term "state of the art" factually and provides a methodical approach to determine it.
Thomas Pfeiffer MSc
CISO
LINZ STROM Netz GmbH, Linz, Austria

Abstract

What would modern life be like without energy? What to do when being hacked?

For more than one hundred years, companies in the energy industry have been proving their ability to deal successfully with natural disasters, such as storms and flooding. The energy sector was gearing up by establishing an own Austrian energy computer emergency response team (AEC), in order to mitigate attacks from cyberspace. So, how will we be able to react rapidly to changes in the organizational process beforehand, and with which technical methods can we prevent the critical infrastructure against these enemies?
Dr. Edgar Weippl  
Research Director  
SBA Research, Vienna, Austria  

Abstract  

Power plants and many other industrial plants are an integral part of Austria’s critical infrastructure. As systems become increasingly automated and networked and complicated software systems control entire systems, IT security is playing an increasingly important role. Previous attacks have mostly exploited existing vulnerabilities, future attackers will strive to intervene in the development process to build in vulnerabilities themselves.