PROTECTING NATIONAL CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

BEST PRACTICES RELATED TO TECHNOLOGY AND STANDARDS FROM EUROPE

BANGKOK

23.11.2015

DEFINITION OF CRITICAL INFRASTRUCTURE

US

“The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family.”

EU

“Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens.“

EXAMPLE OF ELECTRIC POWER INFRASTRUCTURE DEPENDENCIES

CRITICAL INFRASTRUCTURE
CAN ONLY BE SECURED IN
AN OVERALL CONTEXT IN
TERMS OF BUILDING BLOCKS!

THE RISE OF CYBER SECURITY RISKS

2013 CYBER RISK
UP TO 3RD POSITION
IN THE TOP FIVE!

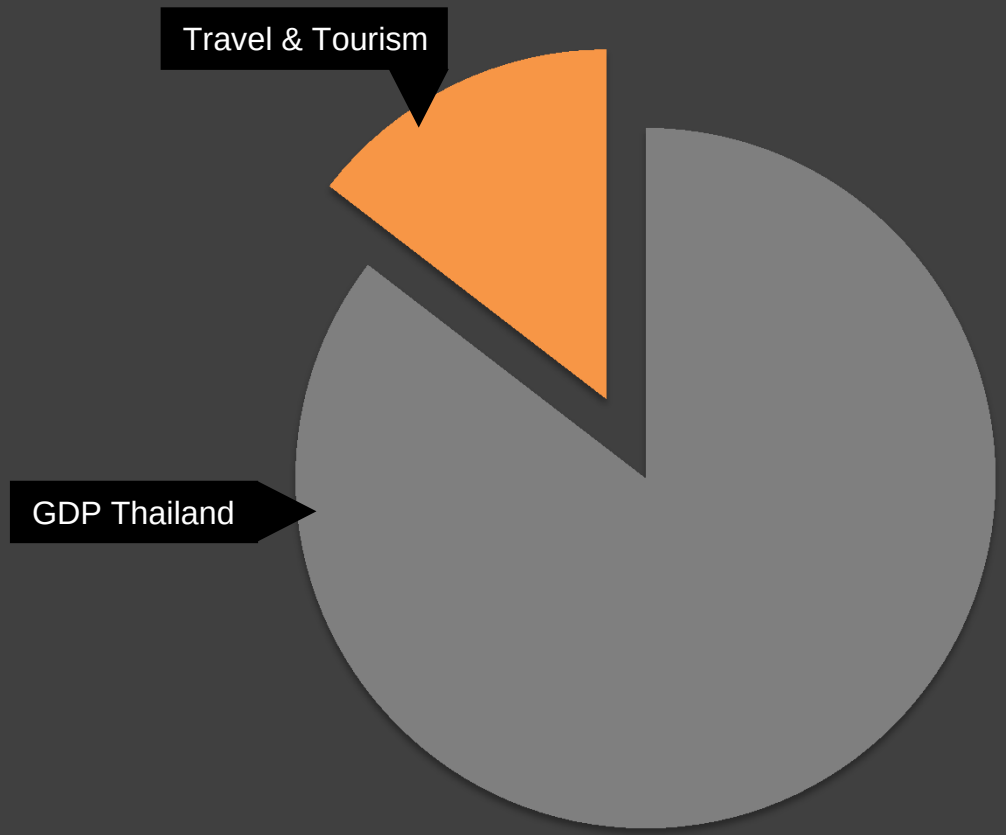
CYBER ATTACK ON THE US POWER GRID

MALWARE INFECTS ELECTRICITY GENERATION CONTROL

FORCES 50 GENERATORS TO OVERLOAD AND BURN OUT

NORTHEASTERN UNITED STATES REGIONAL GRID SUFFER SUSTAINED OUTAGE

WHY IS THE TARGET A TARGET?



387 bn USD (2013)

T&T 17% total contribution

= 66 bn USD per year!

OVERVIEW IOT PENETRATION WORLDWIDE

KOREA RANKS AMONG TOP 12 COUNTRIES

IN INTERNET PENETRATION RATE

OMISSIONS AND CONSEQUENCES

EXAMPLES OF HACKS TO DIFFERENT SECTORS

MALAYSIA AIRLINES, 26.01.2015

DOMAIN NAME SYSTEM HAS BEEN COMPROMISED

NO BOOKING POSSIBLE

IT TOOKS 24 HRS TO RECOVER

STUXNET

BORN 2007, SPOTTED JUNE 2010

“HACK OF THE CENTURY” ON URANIUM ENRICHMENT FACILITY (IRAN)

SCADA COMPROMISING

MOST COMPLEX HACK EVER SEEN

VISA & MASTERCARD, APRIL 2012

1.5 MILLION CREDIT CARD NUMBERS STOLEN

PAYMENT PROCESSORS HACKED

JAPAN TOURISM ONLINE SITE, MARCH 2015

WEBSITE WAS HIJACKED BY HACKERS

DISPLAYED A MESSAGE FROM THE ISLAMIC STATE (IS) GROUP

THE HOME DEPOT, SEPTEMBER 2014

MALWARE INFECTION OF CASH REGISTER SYSTEM

MORE THAN 2.000 STORES AFFECTED

56 MILLION CREDITCARD INFORMATIONS &

53 MILLION EMAIL-ADRESSES WERE STOLEN

62 MILLION US-DOLLAR DAMAGE

OFFICE OF PERSONNEL MANAGEMENT (OPM), APRIL 2015

MASSIVE DATA BREACH

PERSONAL DATA OF NEARLY 4 MILLION US FORMER AND CURRENT GOVERNMENT EMPLOYEES

VULNERABILITIES OF REMOTE SYSTEMS THROUGH THE EXAMPLE OF SCADA SYSTEMS

PROVIDE CONTROL OF REMOTE EQUIPMENT

ACQUIRE INFORMATION ABOUT THE STATUS OF THE REMOTE EQUIPMENT (E.G. VALVE ON/OFF)

WHY IOT IN CRITICAL INFRASTRUCTURE?

Internet of Things

Networked

Distributed

Monolithic

GENERATIONS OF SCADA SYSTEMS

1. MONOLITHIC

COMPUTING IN GENERAL CENTERED ON “MAINFRAME” SYSTEMS

EACH CENTRALIZED SYSTEM STOOD ALONE

NETWORKS WERE GENERALLY NON-EXISTENT

GENERATIONS OF SCADA SYSTEMS

2. DISTRIBUTED

DISTRIBUTE THE PROCESSING ACROSS MULTIPLE SYSTEMS

MULTIPLE STATIONS WERE CONNECTED TO LAN

SHARED INFORMATION IN REAL-TIME

GENERATIONS OF SCADA SYSTEMS

3. NETWORKED

OPENING THE SYSTEM ARCHITECTURE

UTILIZING OPEN STANDARDS AND PROTOCOLS

POSSIBLE TO DISTRIBUTE SCADA FUNCTIONALITY ACROSS WAN

GENERATIONS OF SCADA SYSTEMS

4. INTERNET OF THINGS

NETWORK OF PHYSICAL OBJECTS EMBEDDED WITH ELECTRONICS, SOFTWARE, SENSORS AND NETWORK CONNECTIVITY

OBJECTS ENABLED TO COLLECT AND EXCHANGE DATA

HONEYPOTS

RASPERRY PI WITH MOBILE CONNECTION TO THE INTERNET

SIMULATES A COMPUTER, SERVER OR INDUSTRY DEVICE

GATHERING DATA (NUMBERS OF ATTACKS, SOURCE, PROCEDURE) TO UNDERSTAND HACKERS BETTER

REGIONAL CRITICAL-INFRASTRUCTURE PROTECTION PROGRAMS

The European Programme for Critical Infrastructure Protection (EPCIP) has been laid out in EU Directives by the Commission (2006). It has proposed a list of European critical infrastructures based upon inputs by its Member States.

Each designated European Critical Infrastructures (ECI) will have to have an Operator Security Plan (OSP) covering the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures.

REGIONAL CRITICAL-INFRASTRUCTURE PROTECTION PROGRAMS

The German critical-infrastructure protection programme is coordinated by the Federal Ministry of the Interior. Some of its special agencies like the German Federal Office for Information Security or the Federal Office of Civil Protection and Disaster Assistance BBK deliver the respective content, e.g., about IT systems.

REGIONAL CRITICAL-INFRASTRUCTURE PROTECTION PROGRAMS

In the UK, the Centre for the Protection of National Infrastructure provides information, personnel and physical security advice to the businesses and organisations which make up the UK's national infrastructure, helping to reduce its vulnerability to terrorism and other threats.

It can call on resources from other government departments and agencies, including MI5, the Communications-Electronics Security Group and other Government departments responsible for national infrastructure sectors.

REGIONAL CRITICAL-INFRASTRUCTURE PROTECTION PROGRAMS

The USA has had a wide-reaching Critical Infrastructure Protection Program in place since 1996. Its Patriot Act of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

APPLICATION OF BEST PRACTICES IN EUROPE

ISO-NORMS

FIRST INTERNATIONAL STANDARD FOR IT SERVICE MANAGEMENT

DEVELOPED IN 2005, UPDATED IN 2011

RECERTIFICATION IS NEEDED EVERY 3 YEARS

ISO 20000-1 “SERVICE MANAGEMENT SYSTEM REQUIREMENTS”

“Design, transition, delivery and improvement of services that fulfill service requirements and provide value for both the customer and the service provider”

The 2011 version comprises nine sections:

- Scope
- Normative references
- Terms and definitions
- Service management system general requirements
- Design and transition of new or changed services
- Service delivery processes
- Relationship processes
- Resolution processes
- Control processes

ISO 20000

ISO 20000-2 “CODE OF PRACTICE”

“Based on the requirements, Part 2 ads best practice in terms of guiding principles and recommendations of IT Service Management-Processes”

ISO 20000

ISO 20000-3 “GUIDANCE ON SCOPE DEFINITION AND APPLICABILITY OF ISO 20000-1”

“Provides guidance on scope definition, applicability and demonstration of conformance for service providers aiming to meet the requirements of ISO 20000-1”

ISO 20000

ISO 20000-4 “PROCESS REFERENCE MODEL”

“Intended to facilitate the development of a process assessment model according to process assessment principles. Describes the concepts and terminology used for process assessment.

Describes the requirements for the conduct of an assessment and a measurement scale for assessing process capability.”

ISO 20000-5 “EXEMPLAR IMPLEMENTATION PLAN FOR ISO 20000-1 ”

“Intended to facilitate the development of a process assessment model according to process assessment principles. Describes the concepts and terminology used for process assessment.

Describes the requirements for the conduct of an assessment and a measurement scale for assessing process capability.”

ISO 20001

Information security standard that was published in 2005 and replaced in 2013
specification for an information security management system (ISMS).
Meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process.

- Scope of the standard
- How the document is referenced
- Reuse of the terms and definitions in ISO/IEC 27000
- Organizational context and stakeholders
- Information security leadership and high-level support for policy
- Planning an information security management system; risk-assessment &-treatment
- Supporting an information security management system
- Making an information security management system operational
- Reviewing the system's performance
- Corrective action

ISO 27002

Published in the mid-1990s, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO 27000-series

Provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS)

Information security standard for:

- Information technology
- Security techniques
- Code of practice for information security management

ITU RECOMMENDATIONS

ELEMENTS OF A NATIONAL CYBERSECURITY PROGRAMME (2011)

CYBERSECURITY STRATEGY OF THE EUROPEAN UNION

- Principles for cybersecurity
- Achieving cyber resilience
- Raising awareness
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)
- Develop industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote EU core values
- Coordination between NIS competent authorities/CERTs, law enforcement and defence
- EU support in case of a major cyber incident or attack

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

“NETWORK AND INFORMATION SECURITY (NIS) PLATFORM” {*DRAFT}*

“The establishment of the NIS Public-Private Platform was announced in the Cybersecurity Strategy of the European Union. It shares the same objective as the Cybersecurity Strategy (pdf) and the NIS Directive (pdf) , i.e. to foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrations in Europe. The NIS Platform will help implement the measures set out in the NIS Directive and ensure its convergent and harmonised application across the EU.

The work of the Platform will draw from international standards and best practices. The findings of the Platform will feed into Commission recommendations on cybersecurity (adopted in 2014).

THANKS FOR YOUR ATTENTION!

Cybercrime
Research Institute