КИБЕРАТАКИ НА КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ:
АНАЛИЗ ОТДЕЛЬНЫХ ИНЦИДЕНТОВ ЗА 2015 г.

Матвей Войтов | руководитель отдела продуктового маркетинга, управление защитой критических инфраструктур | Лаборатория Касперского

CRITICAL INFRASTRUCTURE SECTORS BY STATE

- Energy
- Transport
- Water
- Food
- Communications
- Emergency Services
- Financial Services
- Government
- Health

CPNI
Centre for the Protection of National Infrastructure

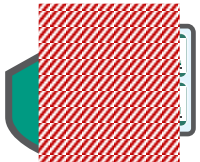
Industrial = based on Industrial Control System

- Energy
- Chemical
- Commercial Facilities
- Nuclear
- Transportation Systems
- Water and Wastewater
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Food and Agriculture
- Emergency Services
- Communications
- Financial Services
- Government Facilities
- Healthcare and Public Health
- Information Technology

WHAT SHOULD BE PROTECTED

ISA95 Model

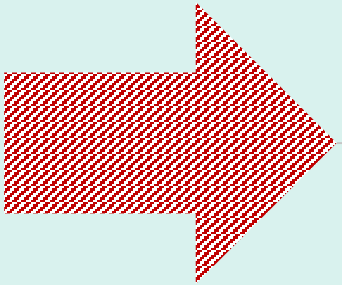
LEVEL 4
Business planning
and logistics



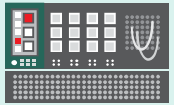
Managing end-to-end supply chain. Establishing the basic plant schedule – production, material use, delivery, and shipping.

LEVEL 3
Manufacturing
Operations management

Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process.



Monitoring, supervisory control and automated control of the production process



Sensing the production process, manipulating the production process

LEVEL 0
Physical

Physical devices

Conventional IT Security

Specialized Industrial CyberSecurity

Physical security

KASPERSKY lab

INDUSTRIAL CYBERSECURITY APPROACH

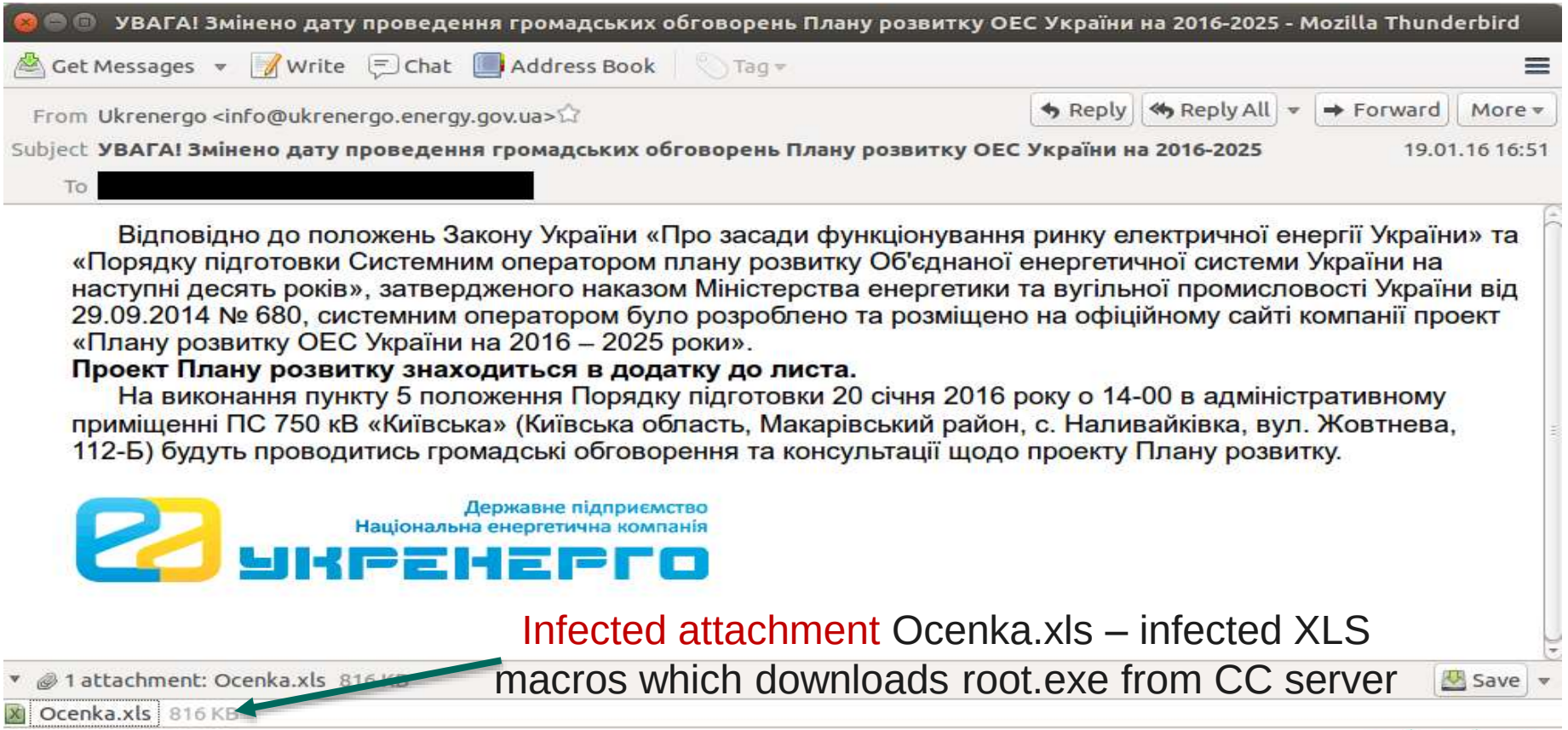
1. Availability
2. Integrity
3. Confidentiality

1. Confidentiality
2. Integrity
3. Availability

- Corporate IT Security is about Data protection
- Industrial Security is about Process protection
- Process should be continuous and only then secure

KASPERSKY lab

BLACKENERGY* ON UKRAINE IN 2016



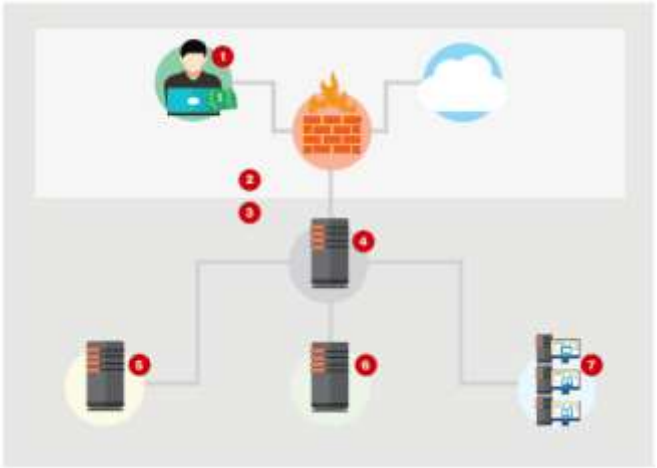
Infected attachment Ocenka.xls – infected XLS macros which downloads root.exe from CC server

*https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

KASPERSKY

WATER PLANT HACK (BY ACCIDENT)

- 2015 – water utility' control facility (Kemuri Water Company) hacked by accident*
- crucial settings that controlled the amount of chemicals used to treat tap water were changed - but hackers had no clue what they were doing
- Disaster were stopped due to secondary security measures



1. Customer access to payment system
2. External (Internet)
3. Internal (Corporate access)
4. AS400
5. PLC management
6. Finance access (PII access)
7. IT management

*http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

ARE THE ADVANCED RISKS REAL? (KL STUDY)

THANK YOU. QUESTIONS?

MATVEY.VOYTOV@KASPERSKY.COM

KASPERSKY.COM/CIP

KASPERSKY lab