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

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**

<table>
<thead>
<tr>
<th>LEVEL 4</th>
<th>Business planning and logistics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Managing end-to-end supply chain. Establishing the basic plant schedule – production, material use, delivery, and shipping.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 3</th>
<th>Manufacturing Operations management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 0</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Physical devices</td>
</tr>
</tbody>
</table>

**Conventional IT Security**

- Specialized Industrial CyberSecurity
- Physical Security
Corporate IT Security is about Data protection
Industrial Security is about Process protection
Process should be continuous and only then secure
BLACKENERGY* ON UKRAINE IN 2016

23 Dec 2015: attack on Ukraine’s powergrid

100 of energy sector organizations received spear-phishing email

After this, 50 of power substations were shutdown for up to 8 hours on West and Central Ukraine. No full SCADA control until January 09 2016

In parallel, the attackers overwhelmed utility call centers with automated telephone calls, impacting the utilities’ ability to receive outage reports from customers and frustrating the response effort.

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

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

ARE THE ADVANCED RISKS REAL? (KL STUDY)

- Equipment and configuration equal to the real-world substation
- Cybersecurity settings hardened
- 4 security expert teams competing in CTF competition
- Goal: to demonstrate ways to make damage to the physical world

FIRST SHORT CQUIT IN 3 HOURS, 2 TERMINALS BRICKED
WHEN: October 2015
WHERE: Moscow
TARGET: Penetration testing 500kV substation model
THANK YOU. QUESTIONS?

MATVEY.VOYTOV@KASPERSKY.COM

KASPERSKY.COM/CIP