IT security In The Era When Everything Can Be Hacked

Kaspersky Lab’s look at the latest trends
Easy Protection Is Over

700x more threats
Businesses Struggle To Quickly Detect A Security Incident

Companies need several weeks or longer to realize that they have been attacked.

Incidents cost enterprises 2.6 times more if not detected instantly.

Incidents cost SMBs 1.6 times more if not detected instantly.

Source: Corporate IT Security Risks Report 2017
**Targeted Attacks: How To Combat Them?**

- Incident detection time is critical
- Prevention strategies won’t keep you safe
- Delays are expensive

**CREATE AN INTERNAL ENDPOINT DETECTION AND RESPONSE STRATEGY**

**TIME UNTIL COMPANIES DETECT AN ATTACK**

<table>
<thead>
<tr>
<th>Year</th>
<th>9%</th>
<th>17%</th>
<th>29%</th>
<th>19%</th>
<th>14%</th>
<th>9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Several months</td>
<td>Several weeks</td>
<td>Several days</td>
<td>Within a day</td>
<td>Within a few hours</td>
<td>Almost instant</td>
</tr>
</tbody>
</table>

- **2017**: 9% of companies detected attacks within a day, 17% within several days, 29% within several weeks, 19% within several months, 14% within a few hours, and 9% almost instantly.

*Note: Delays are expensive.*
Ransomware: Massive Outbreaks

2017:

- 11% rise in the number of people targeted with ransomware
- 23% of businesses hit by ransomware
- Over a third of those hit lost all (9%) or a significant volume of data (29%)

3 massive ransomware/wiper outbreaks

<table>
<thead>
<tr>
<th>Wannacry</th>
<th>ExPetr</th>
<th>BadRabbit</th>
<th>the use of ransomware by targeted threat actors</th>
</tr>
</thead>
</table>

Kaspersky Lab
Fighting Back: ‘No More Ransom’ Initiative

NO MORE RANSOM!

The No More Ransom project was established in July 2016 by the Dutch National Police, Europol, McAfee and Kaspersky Lab

One year on:

Over 28,000 Devices have been decrypted

More than 54 decryption tools are available

More than 100 partners

More than 26 Languages are available
DDoS: Much More Than Just A Nuisance

The average cost of a cyberattack that includes DDoS is $123,000 for smaller companies and more than $2.3 million for enterprises. 70% of companies are attacked more than once a year.
Emerging Security Challenges
Cloud: The Extended Perimeter

VIRTUALIZATION PENETRATION RATE... 75%  

- VMware: 45%
- Microsoft: 35%
- Citrix: 12%
- KVM: 8%

Agile, Reliable, Powerful, Virtualized

Microsoft Azure

Amazon Web Services
penetrate the corporate network
Cloud Security Concerns Are Rising

59% of both SMB and enterprise businesses feel that outsourcing and cloud hosted services could introduce new risks to the IT security of their business.

Incidents affecting IT infrastructure hosted by a 3rd party is one of the top-3 growing security events – with a quarter (24%) of businesses experiencing an incident over the last 12 months.

45% of those affected suffered data loss, leakage or exposure as a result of a 3rd party cloud infrastructure breach.

Source: Global IT Security Risks Survey 2017
How To Defend Your Hybrid Cloud

PRIVATE CLOUD
- Physical
- Virtual
- VDI

MANAGED HOSTING
- IaaS
- PaaS
- SaaS

PUBLIC CLOUD
- Microsoft Azure
- Amazon Web Services

Cloud Security
Finance: Wider Attack Surface

Trends

- ATMs under attack – i.e. remote administration of ATMs to extract cash
- Enterprises with Point of Sale terminals became a particular target
- 30% increase of people hit by banking Trojans
- Cryptocurrencies and blockchain-based financial systems are new targets for cybercriminals
Finding an ATM Skimmer in Vienna
Internet Of Threats

What if your perimeter includes connected smart devices?

BILLIONS OF DEVICES

YEAR

1992 1,000,000
2003 0.5 BILLION
2009 IoT INCEPTION
2012 8.7 BILLION
2013 11.2 BILLION
2014 14.4 BILLION
2015 18.2 BILLION
2016 22.9 BILLION
2017 28.4 BILLION
2018 34.8 BILLION
2019 42.1 BILLION
2020 50.1 BILLION
In 36% of cases, targeted attacks were the cause of cybersecurity incidents.

On average, ineffective cybersecurity costs industrial organizations up to $497K per year.

- 83% of respondents believe they are well-prepared to face an OT/ICS cybersecurity incident.
- Half of companies experienced between one and five IT security incidents in the past 12 months.
Percentage of industrial computers attacked, February 2018

Top countries by percentage of industrial computers attacked, February 2018

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>51.3%</td>
</tr>
<tr>
<td>Morocco</td>
<td>46.4%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>43.5%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>41.5%</td>
</tr>
<tr>
<td>Iran, Islamic Republic of</td>
<td>39.8%</td>
</tr>
<tr>
<td>India</td>
<td>34.4%</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>34.1%</td>
</tr>
<tr>
<td>China</td>
<td>34.0%</td>
</tr>
<tr>
<td>Peru</td>
<td>33.3%</td>
</tr>
<tr>
<td>Turkey</td>
<td>31.5%</td>
</tr>
<tr>
<td>Mexico</td>
<td>30.9%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>30.6%</td>
</tr>
<tr>
<td>Malaysia</td>
<td>30.1%</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>29.5%</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>27.3%</td>
</tr>
</tbody>
</table>
Geographical distribution of attacks on industrial automation systems, H2 2017 Percentage of attacked ICS computers in each country
Number of vulnerable products used in different industries (according to ICS-CERT classification) vulnerabilities published in 2017
ICS Security Framework

INDUSTRIAL AUTOMATION MODEL (ISA-95)*

- **Level 4**
  - Business planning and logistics

- **Level 3**
  - Manufacturing operations management

- **Level 1 / Level 2**
  - Batch control / Continuous control / Discrete control

- **Level 0**
  - Physical

* ISA-95 is an international standard from the International Society of Automation for developing an automated interface between enterprise and industrial control systems.
How To Stay Safe

Threat Management and Defense
Discovering and mitigating the risks associated with advanced threats and targeted attacks

Endpoint Security
The leading multi-layered endpoint protection platform, based on Next Gen cybersecurity technologies

Hybrid Cloud Security
Borderless security engineered for your hybrid cloud environment

IoT Security
All-in-one security specifically designed for IoT systems

Industrial Cybersecurity
Specialized protection for industrial control systems

Fraud Prevention
Proactive detection of cross-channel fraud in real time
Let’s Talk!