Cybersecurity in Data Centers

Murat Cudi Erentürk
ISACA CISA, ISO 27001 Lead Auditor
Gandalf Consulting and Software Ltd.
What is Cybersecurity?

- Information Security
- IT Systems Security
- Physical Security
International Standards

• Certified Information Security System Professional (CISSP) Common Body of Knowledge (CBK).
• International Organization for Standardization (ISO) 27001 and 27002, version 2013
• (NIST) Risk Management Framework (RMF) and SP 800-53, 63
Threat landscape and motivations

L5 - National Actors

L4 - Industrial Espionage

L3 - Organized Crime

L2 - Hacker

L1 - Worms, Virus etc

Skill Level

Probability to encounter
Trends in Cybersecurity

Cybersecurity Effectiveness

Time

Effectiveness

~Defense Opex
~Attack Incentive

Cyber Defenses

Cyber Attacks

Defense Capex Increase
Trends in Cybersecurity

Intelligent Attacker

- 7x24 In shifts
- Attack research
- Trained professionals
Trends in Cybersecurity
Detect and Delay
Trends in Cybersecurity
Catch and Repel
Physical Security
Physical Access Control (PAC) Technologies

- Components
  - Lock Systems
  - Card readers
  - Backend Servers
# Physical Security

## Vulnerabilities and Countermeasures

<table>
<thead>
<tr>
<th>Proofed Identity</th>
<th>Physical Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Card and PIN (Identity Unknown)</td>
<td>Smart Card and PIN</td>
</tr>
<tr>
<td>Keys (Identity Unknown)</td>
<td>Access Card and Password</td>
</tr>
<tr>
<td>Ticket (Identity Unknown)</td>
<td>Password</td>
</tr>
<tr>
<td>Photo Identity Badge and PIN</td>
<td>Photo Identity Badge and password</td>
</tr>
<tr>
<td>Photo Identity Badge</td>
<td>Photo Identity Badge</td>
</tr>
</tbody>
</table>

- Restricted Cryptography
- Restricted Authentication Protocols

---

**Identity Assurance**

---

**2017 BICSI Fall Conference & Exhibition**
**September 24-28 | Las Vegas, NV**
Physical Security
Vulnerabilities and Countermeasures

Jon Doe

Visitor

1002234

2002234

Unrestricted Entry
Controlled Entry
Authorized Entry
Restricted Entry

Park Area
Level 2: Semi Private
Level 3: Private

Level 1: Semi Public
Level 0: Public

2017 BICSI Fall Conference & Exhibition
September 24-28 | Las Vegas, NV
Physical Security
Cabling Security
IT Systems Security

Network Security

Installation Cost

Maintenance Cost

Separation of Networks
IT Systems Security
Server Security Technologies
Onboard Security Chips (TPM)
• Cryptokey Generation, Storage
• Best use: Disk Encryption
IT Systems Security
Server Security Technologies

• CPU Security Features
  – Write Protect
  – NXE/XD

• Protects against buffer overflows
IT Systems Security
Firmware Security Technologies

- Provided by Device Manufacturers
- Compliments Hardware provided security
IT Systems Security
Firmware Security Technologies

UEFI Boot
[Enabled]

EFI
ubuntu (M4-CT128M4SSD3)
Ubuntu (M4-CT128M4SSD3)

Boot Device Priority
Internal HDD: M4-CT128M4SSD3
SATA HDD: ST1000LM024 HN-M101MBB
SATA ODD: HL-DT-ST DVDROM GT50N
Network Boot: Atheros Boot Agent

UEFI in PC

Firmware in Apple iOS
IT Systems Security
Firmware Security Technologies

• What to look for
  — Trusted Updates
  — Trusted Boot
  — Setup Passwords
IT Systems Security
Firmware Security Technologies

• Remote Management
  – Central Updates
  – Monitor Tampering
  – Change Passwords
IT Systems Security

Trusted Boot Sequence

- Firmware Check
- Boot Manager Check
- Operating System Check
- Driver Check
IT Systems Security
Virtualization Security Technologies

• Execution Partitions
• Virtualization assisted application whitelisting
IT Systems Security

Power Distribution Security

• UPS/PDU Security
• PoE Security
IT Systems Security
Management Systems Security

• IP Cameras, Recorders
  – Record Manipulation
  – Denial of Service

• Physical Access Control Systems
  – Unauthorized access
  – Covering tracks
IT Systems Security

Scada Systems Security in DC

- Pumps
- Compressors
- CRAC Units
- DCIM, BAS, BMS
IT Systems Security
Scada Systems Security in DC

• Separate Networks
• Disable unused services/Controllers
• Replace components that can not be secured
Cybersecurity Operations
Increased Security for Availability Classes

“Match your monitoring system security AND availability with systems you monitor”
Cybersecurity Operations
Holistic Approach
Cybersecurity Operations
Security Operations Center
Cybersecurity Operations
Minimize Operational Dependencies

- IT Systems Depends For Security
- Security Systems Depends For Operations
Cybersecurity Operations
Cybersecurity Frameworks

• NIST Risk Management Framework
  – Functions (Identify, Protect, Detect, Respond, Recover)
  – Tiers (Partial, Risk Informed, Repeatable, Adaptive)
  – Categories
What can you do?
What can you do?
Asses your cybersecurity risks

• You have physical access to critical Data Center systems
• You use a computer connected to the network
• You use Internet for communication (E-mail, Social Media)
What can you do?
Select your laptop carefully

- Use a system with TPM (preferably with v2.0)
- Use disk encryption
- Use secure boot
What can you do?
Select your laptop carefully

• All your driver updates should be downloaded from a verified and trusted location
What can you do?
Select your laptop carefully

• Use a supported and regularly updated OS AND Applications
What can you do?
Select your laptop carefully

• Use Advanced Threat Protection End Point Software
What can you do?

Use Secure Logon

- Use BIOS password
- Use Startup password
What can you do?

Use Secure Logon

- Use Multi-Factor Authentication for your laptop AND all your cloud applications
- Come up with a system for generating and remembering passwords
What can you do?

USB Devices

• Best Solution: Do NOT use USB at all, network is easier to secure

• Second best: Do not insert ANY USB device to your machine that you do not know the origin. Use your own with a known brand.
What can you do?

Daily Cyber Hygiene

- Beware where you send your password
- Do not use public Wi-fi without VPN
- Do not connect to sites if SSL is broken
- Do not leave your computer with even screen locked
What can you do?

Secure your home network

- Use proper security on your wireless/Ethernet over power network
What can you do?

Secure your home network

• Never put any device on your local network that you can’t update firmware
  – Network Printers
  – NAS Devices
  – Smart Home devices
  – Ethernet over power switches
Questions?