Check Point
SOFTWARE TECHNOLOGIES LTD

CYBER SECURITY - KEEPING YOUR SHIP SEAWORTHY

Bill Nikolopoulos
Team Leader Security Engineering
Greece/Cyprus/Romania/Bulgaria

ONE STEP AHEAD

- MSC.1/Circ.1526 1 June 2016 (6 pages)
  - **urgent** need to raise awareness on cyber risk threats and vulnerabilities
  - high-level recommendations on maritime **cyber risk management** to safeguard shipping from **current** and **emerging cyberthreats and vulnerabilities**
  - ***maritime cyber risk*** refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being **corrupted, lost or compromised**
  - Stakeholders should take the necessary steps to **safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping**

- Risk management is fundamental to safe and secure shipping operations
- Vulnerable systems could include, but are not limited to:
  - Bridge systems;
  - Cargo handling and management systems;
  - Propulsion and machinery management and power control systems;
  - Access control systems;
  - Passenger servicing and management systems;
  - Passenger facing public networks;
  - Administrative and crew welfare systems; and
  - Communication systems.
- The distinction between information technology and operational technology systems should be considered

Deadline in place

- **IMO** makes cyber risk management onboard ships mandatory as of **1 January 2021**
- will be formalised in Chapter IX of the International Convention for the Safety of life at Sea, SOLAS, Regulations 1-6, Management for Safe Operation of Ships.

All Vessel Families are Alike

Check Point
SOFTWARE TECHNOLOGIES LTD

- Standard systems
- Build to last for years
- Common protocols in use
- Control equipment based on PLC / and or typical PC

- New trends, Vessels always online, gathering data, connected to cloud
- …

The Maersk NotPetya story

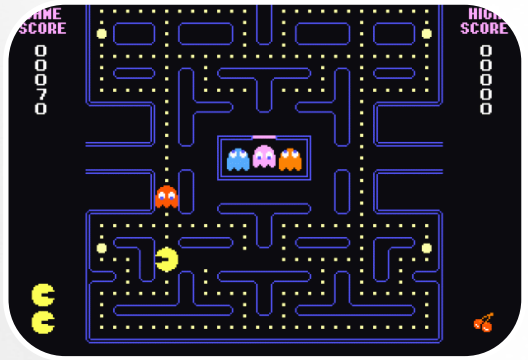
- Ransomware: The key lesson Maersk learned from battling the NotPetya attack (source zdnet.com)
  - "I remember that morning – laptops were sporadically restarting and it didn't appear to be a cyberattack at the time but very quickly the true impact became apparent," said Lewis Woodcock, head of cybersecurity compliance at Moller-Maersk, the world's largest container shipping firm.
  - "The severity for me was really taken in when walking through the offices and seeing banks and banks of screens, all black. There was a moment of disbelief, initially, at the sheer ferocity and the speed and scale of the attack and the impact it had.“

- The company was one of the most badly hit of those caught in the crossfire of NotPetya, with almost 50,000 infected endpoints and thousands of applications and servers across 600 sites in 130 countries.
- Maersk had to balance the need to continue operating – despite the lack of IT – and recovering and rebuilding networks. In many cases, it was a manual process that took days and what was described at the time as a "serious business interruption" is estimated to have cost Maersk up to $300m in losses.

Question to ask

- How many Windows XP systems are in your vessel ?
  - Have it ever been patched to at MS17-010 (Exploited WIndows SMB EternalBlue)

Why Are These Attacks Possible?



Legacy System

Default Configuration

Less/No Updates

Less/No Encryption

Policies & Procedures

Less/No Segmentation

Latency Concerns

Attack Vectors Reaching the OT Network

Removable Media

Email Phishing and Attachments

Remote Technicians

Software Vulnerabilities

Guest Networks Unprotected Sockets

Risk Methodology

- What can we use ?
- NIST SP800-30
- ISO/IEC 27005 Risk management standard
- ISO/IEC 31000 Risk management – Principles and guidelines.
- ISO/IEC 31010 Risk management – Risk assessment techniques

Scope of a Integrated Bridge System

Check Point
SOFTWARE TECHNOLOGIES LTD

Asset	ECDIS	AIS	Radar	Ballast …	Load plan software
Functions	Mapping/Route Planning/Plotting position/Tracking	Avoid collisions	Detect targets		

Risk Methodology

- Apply same concepts like in ICT (use IMO)
- Evaluation of assets
- Identify potential threat sources
- Identify vulnerabilities
- likelihood of occurrence
- Magnitude of impact
- Determine Risk

Securing Against Attack Vectors (Our controls)

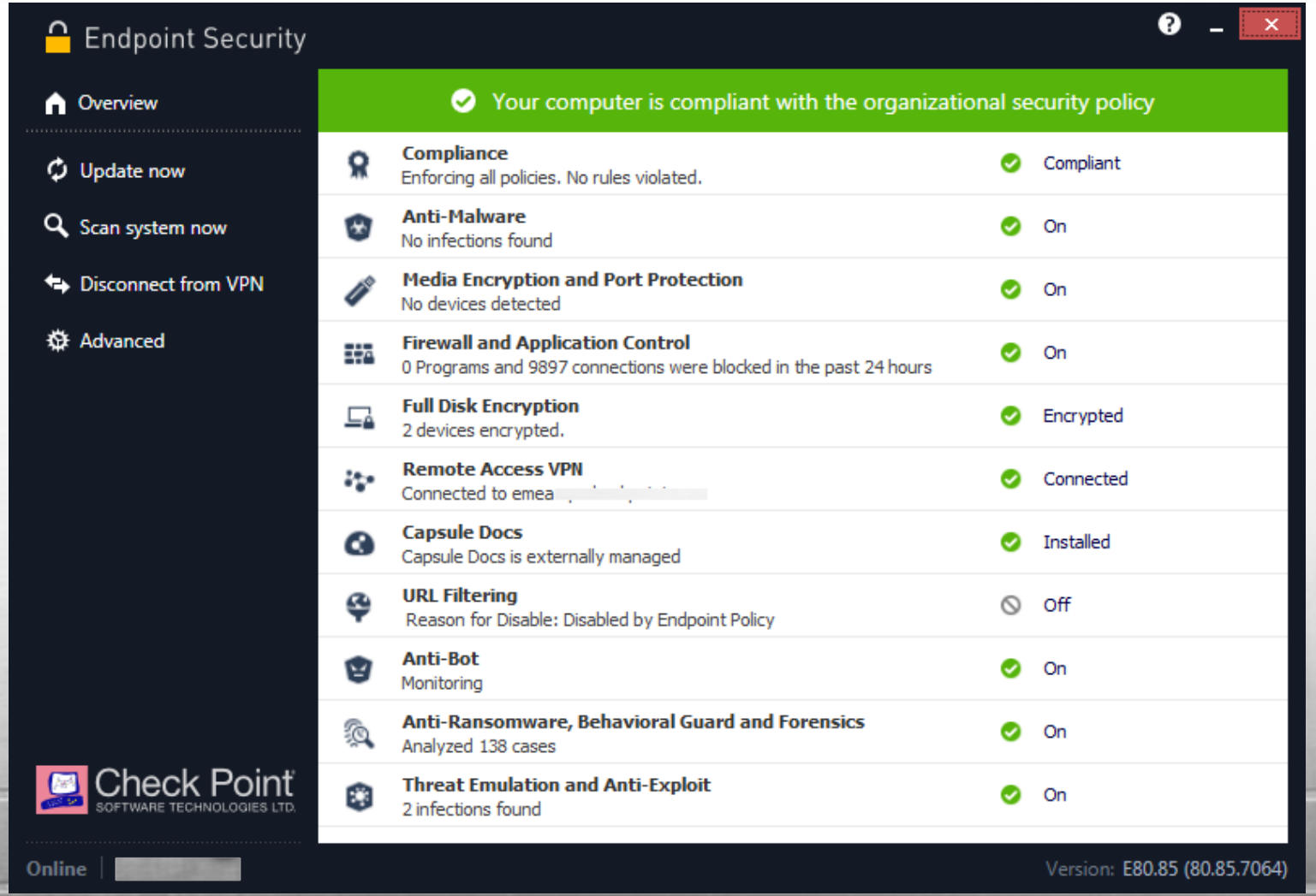
Attack Vector	Check Point solution
Removable Media	Endpoint data protection
Spear Phishing	SandBlast Emulation and Extraction
Ransomware	SandBlast Anti-Ransomware
Remote Technicians	Secured VPN Connectivity and Two Factor Authentication
Software Vulnerabilities	IPS
Virus's and BOT's	Anti Virus and Anti-Bot
Missing Boundary	Firewall and segmentation

Check Point 1200R

Purpose-Built Ruggedized Security Gateway Appliance

- **Fully** featured Check Point security gateway
- **6x1GbE ports** and firewall throughput of 2Gbps
- **Compliant** to the most rigid regulations:
  IEC 61850-3 and IEEE 1613
- **Compact fan-less** design with no moving parts; temperature range from -40°C to 75°C

Full NGAV Suite



UNIFIED MANAGEMENT

FOR BEST ROI AND OPTIMAL PROTECTION

Customized Visibility

Unified Policy

Everywhere Monitoring

Management integration With Leading SIEM systems: Q-Radar, ARCSight, Splunk And more like Predix and others

Inherent Risk Assessment

Risk	Example
An event that could negatively impact the vessel	ECDIS is being taken over remotely by an attacker

Maximum Possible Damage Per Event (Impact) X **Frequency of Risk Events (Likelihood)**

Inherent Risk

The Level of Risk

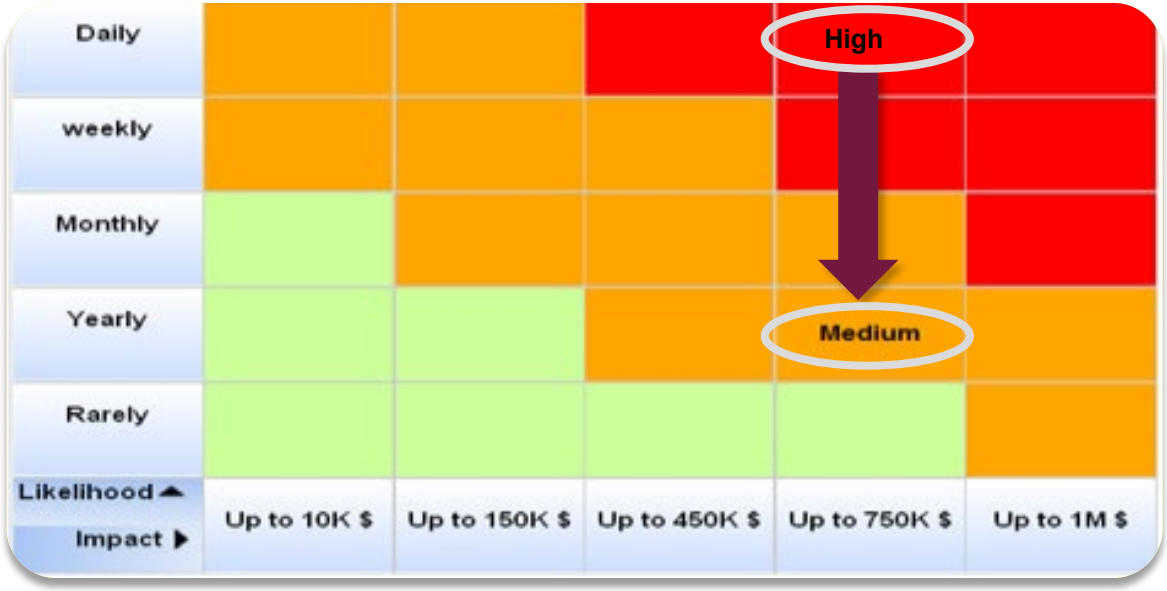
Before Controls

Are in Place

Residual Risk

Control	Example
Activity aiming to reduce the risk impact and/or likelihood	ECDIS is patched, NGAV is installed, a security device is protecting communications towards this system

Residual Risk = **Inherent Risk** – **Control Score**



Residual Risk

The Level of Risk

After Controls

Are in Place

Check Point
SOFTWARE TECHNOLOGIES LTD.

THANK YOU