ITM SYSTEMS
INTELLIGENT TECHNOLOGY MANAGEMENT

8
Hours daily

4
Days

None
Pre-requisites

Protect Yourself Against Ransomware

What is Ransomware?

A ransomware attack involves malicious software that is downloaded onto a victim's device, and then used to encrypt the victim's information. Hackers that initiate these attacks threaten to block access to the files until a ransom is paid. Ransomware attacks are becoming increasingly wide-spread these days; the most common ways for the software to be installed on a victim's device is through phishing emails, malicious adverts on websites, and questionable apps and programs.

Who is at risk?

Prominent target groups of ransomware attacks are critical infrastructure establishments, state organizations, major enterprises, as well as small-to-medium businesses that don't have a strong cyber security protection implemented. Any company or organization depending on daily access to critical data should be most worried about ransomware.

Objectives

By the end of the training participants will be able to:

- Identify existing weaknesses in the processes, infrastructure and human behavior of the organizations;
- Handle cyber security incidents from both the technical and managerial perspectives;
- Possess the knowledge to evaluate different solutions available on the market to support the protection of the organization;
- And most importantly, they will experience in real-time the life-cycle of various attacks, with considerable in-depth exploration of ransomware.

How is a ransomware attack originated? How easily can hackers access your network? How to prevent ransomware attacks and how to respond to them once they have occurred? What is the best protection against ransomware?

All these and more require a fundamental understanding of hackers' state-of-mind, the vulnerabilities of corporate systems and the best practices of handling security incidents.

The following training course was especially designed for IT and security teams to equip them with an in-depth understanding of the security threat landscape affecting their organization, and the corresponding mitigation methods.

Course Outline

Day 1: Introduction to Cyber Security

01 Cyber Security Basics

- Malware
- Viruses
- Trojans
- Phishing – case studies
- Keyloggers
- MiTM attacks explained
- The Anti-Virus and how it works + demo
- OSI model – the 8th layer

02 Hacking with Linux

- Linux as an OS
- Linux Command Line
- Scripting with Grep, Sed and Awk

03 Password Security

- Password complexity
- Demo: how your password can be hacked
- Online vs. offline password hacking methods
- Brute-Force attack methods
- Password attacks mitigation for enterprise

04 Browsing risks

- Demo: JavaScript attacks
- SQL injection
- XSS
- RFI and LFI
- Email phishing + demo (spam mail simulation)
- Social engineering + demo (setting your own phishing pages)

Day 2: Hands-On Session

01 Virtualization

- Bridged vs NAT explained from the hacker's point of view
- Isolating your virtual machine
- Configuring Virtual Machines for lab environment

02 Introduction to Advanced Persistent Threats

- Introduction to the post-exploitation phase
- Pivoting through the enterprise networks

03 Introduction to Metasploit Framework

- Auxiliary + demo
- Exploits + demo

04 Trojans

- Msfvenom as creation tool
- Bind
- Reverse
- HTTPS
- Advantages vs. limitations of Trojan kinds
- Demos lab

05 Wi-Fi

- How Wi-Fi works
- WEP security weaknesses
- Breaking WEP, WPA, WPA2 methods

06 Security monitoring: IDS and IPS

Day 3: The Ransomware

01 Introduction to Ransomware

- What is Ransomware?
- Ransomware attack vectors
- How ransomware can affect your organization?
- Ransomware extensions

02 Types of Ransomware

- Locker
- Crypto
- Hybrid

03 Delivery Channels

- Malware advertisement
- Phishing emails
- Downloaders
- Ransomware-as-a-Service

04 Ransomware Attacks

- Case study: popular Ransomware attacks
- Targets of Ransomware
- Payment: should you pay or not?

Day 4: Response and Report

01 Prevention

- Backup and recovery
- Network share access security
- Email and executable controls security
- Security endpoints

02 Response

- Ransomware analysis methodology
- Harding your enterprise system
- Separate networks
- Scanning the organization network

03 Report

- How to write a Ransomware attack report?
- Extend your report
- To whom should you report?

ITM SYSTEMS
INTELLIGENT TECHNOLOGY MANAGEMENT