Publication date : 01/03/2024

Course : Ransomware, understanding the threat

Preventing attacks and remedying incidents

Seminar - 2d - 14h00 - Ref. RAN

Price : 2170 CHF E.T.

Nouvelle édition

Hardly a day goes by without the media alerting us to a new ransomware attack on a hospital, local authority or company. Between January 2022 and June 2023, ANSSI dealt with 187 cyberattacks targeting local authorities alone. In just a few years, ransomware has become the world's No. 1 cybercrime scourge. This training course will help you understand the mechanisms behind ransomware attacks. It will also show you how to protect yourself against ransomware attacks and how best to manage a crisis of this type.

Teaching objectives

At the end of the training, the participant will be able to:

- Understanding the ransomware threat and how cybercriminals operate
- Discover the ransomware ecosystem (RaaS, affiliates, IAB...)
- Identify the main security measures to protect against them
- Best practices for ensuring your company's cyber resilience
- Managing a large-scale cyber crisis linked to a ransomware attack

Intended audience

CISOs, CIOs, architects, developers, project managers, pre-sales representatives, system and network administrators.

Prerequisites

General computer knowledge is recommended.

Course schedule

PARTICIPANTS

CISOs, CIOs, architects, developers, project managers, pre-sales representatives, system and network administrators.

PREREQUISITES

General computer knowledge is recommended.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant’s academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they’ve developed.

1 Understanding the ransomware threat

- The main ransomware programs and their evolution from AIDS/PC Cyborg (1989) to the present day.
- Evolution of the threat: from simple to quadruple extortion.
- Typology of companies affected.
- The 10 myths of ransomware.
- The motivations of cybercriminals (money is not always the goal...).
- Who are the major groups of cybercriminals specializing in this field?
- The cybercriminal ecosystem (RaaS Group, affiliates, IAB, BPHS, dark web).
- Anonymity and cybercriminals' modus operandi.
- The Ransomware as a Service (RaaS) business model.
- Trends in the number of attacks over the last 3 years.

2 The impact of cyber attacks on businesses

- What are the direct and indirect costs of a cyber attack?
- What is the average/median ransom amount? How is it calculated?
- Can we negotiate? What room for maneuver is there? Other benefits of negotiation.
- Should ransoms be paid? Is the ANSSI position still applicable?
- How do you recover data after payment?
- The debate in France surrounding the assumption of ransoms by insurers and LOPMI 2023.

3 Legal aspects

- The main French laws on cybercrime and cybersecurity.
- Regulatory obligations in terms of data protection.
- What are the penalties for cybercriminals?
- The judicial treatment of cybercrime in France, Europe and the rest of the world.
- How the global fight against cybercrime is organized: the Budapest Convention and MLAT.
- How effective are investigations and prosecutions outside France?

Storyboarding workshops

Examples of cybercriminal arrests.

4 Anatomy of a modern ransomware attack

- Description of a "Big Game Hunting" attack.
- The kill chain: from initial access to extortion.
- Analysis of tactics, techniques and procedures (TTP) using the MITRE ATT&CK framework.
- The high-profile WannaCry and NotPetya cyberattacks.
- Attacks on OIV (Colonial Pipeline), supplier (Kaseya) or hospital (CHSF Corbeil-Essonnes).

Storyboarding workshops

Some famous cyberattacks and feedback.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

5 Initial access to the information system

- Identify your company's attack surface.
- The 9 techniques used to obtain initial access.
- Social engineering attacks (spear phishing, deepfake phishing...).
- Remote access issues (RDP and VPN).
- The main software vulnerabilities exploited by ransomware (CVE, CVSS and EPSS).
- Attacks via the supply chain.

6 Identify the main security solutions

- Why and how to raise user awareness?
- How EPP solutions compare with traditional antimalware.
- Understand the role and complementarity of EPP, EDR, NDR and XDR solutions.
- Reinforcing Active Directory (AD) security.
- Network segmentation and the application of the Zero Trust principle to AD and backups.
- Vulnerability scanning and patch management.
- Managing ransomware risk via the supply chain.
- What are the most effective safety measures?
- Evaluation of the ROM (operating efficiency/ease of use ratio) of the main security solutions.

7 Ensuring your company's cyber resilience

- Perform a Business Impact Analysis specific to the ransomware threat.
- Business continuity plans (BCP) and disaster recovery plans (DRP).
- Why is the 3-2-1 safeguard rule no longer sufficient?
- Secure backups (encryption, immutability, offline mode).
- Cyber insurance contracts (guarantees, costs, exclusions and limits).

8 Managing a ransomware crisis

- Organization of the crisis unit.
- The main stages in a ransomware crisis.
- Internal and external communication: what level of transparency?
- Secrecy of the investigation and application of article 11 of the CPP.
- The main mistakes to avoid in managing a ransomware crisis.
- Crisis closure and Retex.

Dates and locations

REMOTE CLASS
2026 : 9 Apr., 2 June, 17 Sep., 3 Dec.