CORSO: Security

DOCENTI: Walter ARRIGHETTI (Ph.D., 2007); Alessandro CIANI (Master, 2017); Michela IEZZI (Ph.D., 2013); Marco PERICÒ (Master, 2018).
EMAIL: walter.arrighetti@uniroma2.eu
alessandro.ciani@uniroma2.eu
michela.iezzi@uniroma2.eu
marco.perico@uniroma2.eu

DESCRIZIONE DEL CORSO

Lo scenario *Big Data* offre molti vantaggi per la collettività, ma anche sfide tecnologiche, organizzative e normative, legate al trattamento di dati che devono essere disponibili, sempre e ovunque.
In questo cambiamento di paradigma, in cui si "dissolvono nel Cloud" concetti quali reti di calcolatori, identità, privacy degli utenti e persino il dato stesso, sono anche nate nuove opportunità di attacco da parte di diversi attori della minaccia *cyber*.
Dopo una parte introduttiva sulle tecnologie, i protocolli e i metodi della sicurezza informatica, gli studenti del corso di Security saranno calati nello scenario evolutivo della minaccia *cyber* con particolare riferimento alla *data science* e acquisiranno conoscenze sulle principali tipologie di attacco ai dati e sui relativi metodi di difesa ricorrendo al metodo scientifico, alla tecnologia, ma anche agli strumenti normativi e alla corretta sensibilizzazione degli individui.

OBIETTIVI DI APPRENDIMENTO

- ✓ Fornire il *know-how* su tecnologie, protocolli e soluzioni di sicurezza.
- ✓ Fornire delle conoscenze pratiche degli attacchi informatici e delle relative difese tramite attività di laboratorio e pratiche su software e strumenti di sicurezza.
- ✓ Evidenziare alcune sfide specifiche che emergono negli scenari di *Big Data* e fornire alcuni suggerimenti sulle metodologie e strumenti emergenti per affrontare tali sfide.

METODOLOGIA

Didattica frontale; laboratori di tipo dimostrativo (in cui il docente mostra alcune operazioni su componenti software, siti web o macchine virtuali e gli studenti possono seguire da remoto e in alcuni casi replicare sui propri PC quello che fa il docente).

VALUTAZIONE

Valutazione mediante prova finale scritta.

PROGRAMMA

- Introduction
  1. The Triad of Security (and Cybersecurity).
  2. The Cloud paradigms: IaaS, PaaS, SaaS.
  3. Basic taxonomy: threat, vulnerability, risk, exploit, etc.
  4. Examples of threats: virus, malware, spyware, trojan, RAT, APT, zero-day.
  5. Classification of hacker types.
  6. Cybersecurity related teaming: SOC, NOC, CSIRT, CERT.

7. Elements of computer networking.

- Cyber-attacks
  1. Definition of cyber-attack.
  2. Techniques and tactics.
  3. Common attack types; the OWASP Top 10.
  4. Large scale attack examples: DDoS (distributed denial-of-service) and ransomware.
  5. Social engineering based attacks.
- Security controls
  1. Risk (RA) and vulnerability (VA) assessments.
  2. Security processes: event monitoring, incident handling, vulnerability management.
  3. Network vulnerability scanning, penetration testing (PT) and the CVSS index.
  4. Cyber-defence systems: firewall, WAF, IDS/IPS, SIEM, anti-malware, anti-DDOS).
  5. Red- and purple-team testing.
- Cryptography: from theory to hands on data
  1. Basic cryptography and cryptanalytics.
  2. Elements of quantum cryptography and quantum key distribution (QKD).
  3. Digital trust concepts: from certification authorities to non-repudiation.
  4. Digital trust internals: digital certificates' and secrets' management.
  5. Applied cryptography: e-signatures and e-seals; payment cards; secure authentication; internet browsing.
  6. Applied cryptography: electronic ID, EUDI wallet, self-sovereign identity and digital twins
- "Big Data" Cybersecurity
  1. Sublimation of network perimeter and cyber risk concepts into the Cloud.
  2. Data security with respect to owners/custodians, sovereignty, delocalisation, colocation.
  3. Structured, demi-structured and unstructured data.
  4. Big Data characteristics: velocity, volume, value, variety and veracity.
  5. Data anonymity (*DB*-anonymity).
- Privacy-enhancing techniques (PETs) for Data Science.
  1. Privacy-enhancing technologies (PETs) and privacy by design.
  2. Homomorphic, attribute- and identity-based encryption.
  3. Secure multi-party computation and private set intersection.
  4. Secure federated learning.
  5. Differential privacy.
  6. Synthetic data.
  7. Zero-Knowledge Proof (ZKP).
- Cyber threat intelligence (CTI).
  1. The differences between data, information, and intelligence.
  2. The intelligence cycle.
  3. Intelligence sources and CTI models.
  4. Exploiting surface, deep and dark web for information gathering.
  5. Big data analysis techniques for proactive threat detection
- Cyber laws in EU and Italy.
  1. Cybersecurity Act.
  2. NIS2 Directive.

3. eIDAS Regulations.
4. The next-to-be EU laws: Data Act, AI Act, Cyber Resilience Act, Chips Act.
5. The Italian security perimeter; the Cloud and Cybersecurity Strategies.

MATERIALE DIDATTICO

Ai discenti saranno fornite le *slide* del corso, da usarsi esclusivamente per le finalità del Master.