EUROCC ITALY
HPC Competence Center

bi-rex
Big Data Innovation & Research Excellence

CORSO
CyberSecurity Futura
Executive program

Iscriviti al corso

Presentazione

Il corso di Cyber-security Futura si propone di fornire le conoscenze principali riguardanti la cyber-security sia per quanto riguarda i principi che le metodologie alla base della sicurezza dei sistemi informatici e delle reti di telecomunicazioni, dal punto di vista tecnico ma anche organizzativo.

Destinatari:

Imprenditori, IT manager, programmatori, integratori di sistemi, responsabili sicurezza, qualità e organizzazione, responsabili del personale.

Obiettivi:

- Introdurre i principali problemi della cyber-security;
- Apprendere i concetti di base e la metodologia tipica di questo settore;
- Essere in grado di individuare le principali problematiche di sicurezza dei propri sistemi;
- Essere in grado di valutare criticamente le soluzioni presenti sul mercato;
- Permettere di individuare i maggiori trend di evoluzione della cyber-security;
- Individuare gli aspetti più rilevanti dal punto di vista normativo e relativamente all'AI.

Docenti

- Stefano Ferretti, Professore Associato UniUrb;
- Gabriele D'Angelo, Ricercatore confermato, Dipartimento di Informatica - Scienza e Ingegneria UNIBO;
- Francesco Meoni, Responsabile Linea Pilota BI-REX.

MODULO 1, online:
20 e 24 settembre, ore 9:00 - 12:30

Introduzione alla sicurezza informatica

- Concetti e principi di base della sicurezza informatica;
- Casi di studio: analisi iniziale di alcuni esempi tratti dall'attualità;
- Terminologia essenziale del mondo della sicurezza;
- Il concetto di vulnerabilità informatica: definizione per mezzo dell'analisi di alcuni esempi notevoli;
- Principi e meccanismi fondamentali per la progettazione (e l'implementazione) di un sistema "ragionevolmente sicuro";
- La sicurezza come processo;
- Non solo tecnica;
- La mitigazione delle minacce e la corretta gestione delle vulnerabilità che non possono essere eliminate.

MODULO 2, online:
27 settembre e 1 ottobre, ore 9:00-12:30

Strumenti e meccanismi di base per la protezione dei sistemi

- Meccanismi di autenticazione tra innovazione e limiti
- Meccanismi di autorizzazione: chi può accedere a cosa?
- Breve introduzione ai meccanismi crittografici e breve discussione di alcuni utilizzi pratici
- Esercitazione: “giochiamo” con l’infrastruttura di rete Bi-Rex e con la linea pilota. Sono sicure o vulnerabili?
- Esercitazione: esempio pratico di attacco ai protocolli HTTP/HTTPS;
- Qual è il livello di sicurezza dei sistemi attualmente in commercio?

MODULO 3, online:
3 e 11 ottobre, ore 9:00-12:30

Attacchi, contromisure e prospettive future

- Ransomware: presente e futuro dei meccanismi di estorsione;
- Internet of Things;
- Case histories: pompe per insulina, il mercato delle vulnerabilità;
- Cloud computing
- Industria 4.0: breve analisi di sicurezza dei sistemi produttivi connessi a Internet;
- I rischi delle politiche BYOD (bring your own device) e la loro gestione corretta;
- Firewall e antivirus: cosa sono esattamente?
- Alcuni cenni di sicurezza delle reti (sia cablate ma soprattutto wireless)

MODULO 4, online:
17 e 21 ottobre

17 ottobre, ore 9:00-12:30

21 ottobre, ore 9:00-13:00, Stefano Ferretti;
ore 14:00-17:30, Gabriele D'Angelo

Aspetti normativi della CyberSecurity, Intelligenza Artificiale

- Introduzione al "Regolamento Europeo in materia di protezione dei dati personali (GDPR UE 2016/679)";
- Come può un'impresa che ha a disposizione un budget (piuttosto) limitato, migliorare il proprio livello di sicurezza?
    - Alcuni punti di partenza:
        - Laboratorio Nazionale di Cyber Security (CINI)
        - libro Bianco sulla Cyber Security;
        - framework Nazionale per la Cybersecurity (15 Controlli Essenziali per la Cybersecurity).
    - Aspetti normativi:
        - "Misure per un livello comune elevato di cibersicurezza nell'Unione" (NIS-2)
        - "Cyber Resilience Act" (CRA)
        - "Artificial Intelligence Act" (AI Act)
        - Certificazioni: ISO 27001
        - AI e CyberSecurity:
        - Attacchi al Machine Learning
        - Data poisoning
        - Uso del ML per identificare outlier e soggetti anomali
        - Difesa e Attacchi AI-driven
        - Etica e privacy nell'AI

Co-funded by the European Union. This work has received funding from the European High Performance Computing Joint Undertaking (JU) and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia under grant agreement No 101101903.