START4.0

CENTRO DI COMPETENZA PER LA SICUREZZA E L'OTTIMIZZAZIONE DELLE INFRASTRUTTURE STRATEGICHE

punto impresa digitale

Camera di Commercio Genova

PERCHE' UN CORSO DI CYBERSECURITY?

A CURA DI START 4.0 E CAMERA DI COMMERCIO DI GENOVA

Le Piccole Medie Imprese costituiscono il tessuto produttivo del Paese e, come tale, risultano l'obiettivo primario degli attacchi informatici, anche se persiste l'errata percezione che questo tipo di attacchi abbia principalmente come obiettivo le grandi imprese. Inoltre, le PMI risultano il principale veicolo attraverso il quale i criminali informatici riescono a colpire e a sottrarre i dati delle grandi aziende.

È necessario, pertanto, che le PMI si dotino di organizzazioni e sistemi che garantiscano la resilienza e la resistenza agli attacchi cyber, pena gravi ricadute sulle attività, la perdita di commesse e le sanzioni previste dalle nuove normative in materia. A questo si aggiunge un danno di immagine legato alla reputazione e alla credibilità che mina la competitività aziendale.

È pertanto opportuno che le Associazioni del territorio e le istituzioni mettano a disposizione dei loro associati e delle aziende del territorio un lungimirante progetto di Cybersecurity Awareness, riconosciuta come la prima e più significativa arma di difesa per riconoscere le minacce e non cadere in inganno, come evidenziato da ENISA (European Union Agency for Cybersecurity) nel "CYBERSECURITY FOR SMES" di giugno 2021.

OBIETTIVI DEL CORSO:

- **Fornire strumenti e strategie per la sicurezza informatica in azienda.**
- **Conoscere le tecniche di social engineering e il phishing.**
- **Imparare a riconoscere i ransomware e malware più comuni.**
- **Imparare a scegliere ed usare le password per proteggere i dati e i documenti aziendali.**
- **Saper selezionare gli strumenti di protezione migliori per la propria realtà aziendale.**

Camera di Commercio Genova

START 4.0

DESCRIZIONE

La digitalizzazione e la connettività continuano a creare nuove opportunità di business per le PMI, ma modificano i confini aziendali ed espongono a rischi importanti che possono compromettere gravemente l'operatività. La prima e più importante forma di prevenzione è la consapevolezza delle possibili minacce, per poter impostare le contromisure adeguate dotandosi dei corretti sistemi di protezione.

Esistono normative cui adeguarsi che il management aziendale deve conoscere e che possono influire non solo sulle attività, ma sulle possibilità di business perché spesso sono proprio le PMI ad essere attaccate in quanto fornitori di grandi aziende. E' necessario dare garanzie ai propri clienti in tema di cybersecurity e potersi assicurare le commesse.

Per rimanere competitivi occorre quindi considerare la Cybersecurity come un vero e proprio asset aziendale su cui i clienti baseranno la propria scelta.

La crescita del numero di attacchi dimostra che la domanda corretta da porsi non è "se" ci attaccheranno ma "quando". Questo corso sarà la vostra prima forma di protezione.

DURATA E MODALITA' DEL CORSO:

Il corso prevede lezioni da 2 ore, per un totale di 24 ore in modalità ibrida (aula + live streaming) per chi voglia partecipare sia in presenza che da remoto.

I materiali verranno resi disponibili ai partecipanti alla fine di ogni lezione.

Camera di Commercio Genova

START4.0

PROGRAMMA DEL CORSO

A) I fondamentali (4h)

1) Concetti e definizioni

- Cyberspazio
- Cybersecurity definizione
- Cybercrime
- Darkweb
- Criptovalute
- Blockchain
- Mondo IoT e rischi cyber

2) La normativa in materia cyber

B) Rischi e metodiche di attacco (4h)

- L'(in)sicurezza di internet
- Attacchi significativi
- Il Social Engineering
- Il phishing e spear phishing
- I Dos e i Ddos
- Gli APT
- I Man in the middle
- I Ransomware
- Le minacce dall'interno.

PROGRAMMA DEL CORSO

C) Cosa significa “Fare Sicurezza” e come impostare un Sistema Difensivo efficace e certificabile

1) Caratteristiche del Sistema Difensivo (1h)

- Le 3 Fasi Temporali: Prevenzione, Rilevamento, Reazione
- Le 3 Aree di Competenza: Organizzativa, Tecnologica e Legale
- La Triade GRC (Governance – Risk – Compliance)

2) Governance (1h)

- Il “Modo di Progettare e Dirigere” il Sistema Difensivo: i principi fondamentali
- Il Corpus Documentale indispensabile: Manuale (Descrizione del Processo), Policy, Procedure e Istruzioni Operative

3) Risk (1h)

- Il pensiero basato sul Rischio e l’Analisi del Rischio di Information Security
- Il fattore economico e la necessità di protezione: costi vs. rischi

4) La gestione del cyber risk attraverso le contromisure di natura tecnologica (4h)

- Difesa Perimetrale (Firewall) e Content Filtering I(Antivirus, IPS/IDS)
- Identity & Access Management (IAM)
- La crittografia come strumento di protezione delle informazioni presenti sui sistemi e scambiate mediante le comunicazioni
- La PEC, la posta crittografata e indicazioni su come usare l’email in modo sicuro

PROGRAMMA DEL CORSO

5) La gestione del cyber risk attraverso le contromisure di natura organizzativa (3h)

- Il SOC, il CERT (CSIRT), il SIEM e la Cyber Threat Intelligence
- Lavoro a distanza vs smartworking e problematiche connesse alla sicurezza del lavoro a distanza
- Cyberinsurance e prodotti assicurativi
- La security by design

6) Esempio di analisi del rischio e DPIA (2h)

7) Compliance (4h)

- Il Sistema Difensivo efficace cioè progettato e gestito conformemente con gli standard internazionali della famiglia ISO/IEC 27000 certificabile: l'ISMS (Information Security Management System)
- Il processo di Certificazione dell'ISMS secondo lo standard ISO/IEC 27001
- Cenno all'impegno europeo sulla Cybersecurity (GDPR, NIS, Cybersecurity Act) e alle ricadute sui paesi membri

CALENDARIO DEL CORSO

MODULO A E MODULO B

mercoledì 24 novembre 8:30-10:30
Prof. ssa Paola Girdinio
venerdì 26 novembre 8:30-10:30
Avv. Alessandra Mancini
mercoledì 1 dicembre 8:30-10:30
Ing. Luca Caviglione
venerdì 3 dicembre 8:30-10:30
Ing. Luca Caviglione

MODULO C

mercoledì 26 gennaio 8:30-10:30
Ing. Ermete Meda
venerdì 28 gennaio 8:30-10:30
Ing. Ermete Meda, Ing. Luca Caviglione
mercoledì 2 febbraio 8:30-10:30
Prof. Alessandro Armando
venerdì 4 febbraio 8:30-10:30
Prof. Alessandro Armando, Ing. Ermete Meda
mercoledì 9 febbraio 8:30-10:30
Ing. Ermete Meda, Avv. Alessandra Mancini
venerdì 11 febbraio 8:30-10:30
Ing. Ermete Meda
mercoledì 16 febbraio 8:30-10:30
Ing. Ermete Meda
venerdì 18 febbraio 8:30-10:30
Ing. Ermete Meda

Camera di Commercio Genova

START4.0

I DOCENTI

PAOLA GIRDINIO
Presidente del Centro di Competenza START 4.0.
Prof. ssa Università degli Studi di Genova.
https://www.linkedin.com/in/paola-girdinio-50258777/

ALESSANDRA MANCINI
Avvocato partner B-right Lawyers con specifiche competenze ed esperienze in ambito cybersecurity.
https://www.linkedin.com/in/alessandra-mancini-5209131/

ALESSANDRO ARMANDO
Professore Unige e Direttore del corso di dottorato in sicurezza, rischio e vulnerabilità.
https://www.linkedin.com/in/alessandro-armando-67505913/

ERMETE MEDA
Principal Information Security Expert e docente presso master Unige in Cybersecurity.
https://www.linkedin.com/in/ermete-meda-1b37855/

LUCA CAVIGLIONE
Primo ricercatore presso IMATI (CNR) e docente in corsi di dottorato e master Unige in Cybersecurity.
https://www.linkedin.com/in/lucacaviglione/

Camera di Commercio Genova

START 4.0

SIMULAZIONI ED ESERCITAZIONI

Il corso viene completato da:

- una campagna di phishing via email e via sms
- una gioco di simulazione con la Cyber Escape Room

Cyber Escape Room

SECURITY AWARENESS SIMULATION GAME

Pensa come un criminale informatico per accedere e rubare dati confidenziali da una società nucleare! Dovrai utilizzare le tue conoscenze per riconoscere i metodi di phishing e di ingegneria sociale e sfruttare gli errori umani più comuni.

Per partecipare è richiesta una quota minima da versare in fase di iscrizione sulla piattaforma online https://formazione.start4-0.it tramite bonifico o carta di credito.

Per richieste ed iscrizioni:

formazione@start4-0.it

PID@ge.camcom.it

Camera di Commercio Genova

START4.0

punto impresa digitale