

Modalità

I destinatari di questo corso sono tutte le persone che, a vario titolo, utilizzano tecnologie informatiche quali personal computer, smart phones e tablets per scopi personali e/o professionali.

Non è richiesta alcuna competenza tecnico-informatica specifica.

Il corso viene tenuto da un formatore che spiega i rischi informatici e le modalità per evitarli attraverso moltissimi esempi pratici presi dalla realtà.

Verranno mostrati esempi di fatti avvenuti e delle relative conseguenze, mostrando dal vivo alcune tecniche di attacco messe in opera dai criminali informatici ai danni di persone o aziende e spiegandone le motivazioni.

Gli esempi sono presi quindi dalla vita reale e non richiedono competenze specifiche per essere compresi.

Per maggiori informazioni è possibile rivolgersi ai seguenti contatti:

Alberto Redi

alberto.redi@sec-lab.com

+41 78 911 12 60

Saul Greci

saul.greci@sec-lab.com

+41 76 816 08 17



Security Awareness

La sicurezza in azienda

La Security Awareness, ovvero la sensibilizzazione alla sicurezza, è una componente critica per ogni individuo. Le persone, così come i computer, immagazzinano e trasferiscono informazioni. Molti attacchi oggi sfruttano la componente umana, scavalcando i controlli tecnici di sicurezza e utilizzando tecniche, come il social engineering, per carpire le informazioni.

La formazione sulla Security Awareness è stata sviluppata per educare gli utenti all'utilizzo appropriato delle informazioni, alla loro protezione e sicurezza e alle responsabilità individuali nel mantenerne la confidenzialità e l'integrità.

La cultura della sicurezza è il fattore chiave per un'azienda che abbia l'obiettivo di ridurre i rischi e proteggere la propria reputazione. I benefici a lungo termine di un programma riuscito di Security Awareness comprendono una maggior sensibilità ai temi della sicurezza, una protezione migliore e una maggior produttività dei dipendenti e dell'intera azienda.

Il corso, creato dagli stessi autori dei leggendari corsi di ethical hacking Zone-H, è rivolto a tutti, dall'utente privato alle aziende e organizzazioni. I suoi contenuti sono strutturati a moduli che possono essere combinati a dipendenza delle esigenze e delle competenze dell'audience.

Contenuti del corso

Introduzione

- Fattori di rischio
- Chi sono gli hacker e per chi lavorano
- Il valore di un sistema compromesso

Navigazione web

- Navigare in sicurezza
- Riconoscere i contenuti malevoli
- Identificare i siti truffa

E-mail

- Riconoscere le e-mail truffa (phishing e scam)
- Evitare le infezioni

Ingegneria sociale

- Evitare il tranelamento di informazioni
- Cosa non ti dovrebbe mai essere richiesto
- Le richieste truffa al telefono

Sicurezza dei dati

- Cosa succede quando perdo un dispositivo?
- Proteggere le informazioni sensibili
- L'importanza dei backup

Proteggere la propria privacy

- Ripulire i dispositivi
- Evitare il furto di identità
- Condividere con attenzione

La reputazione

- Verificare la reputazione di persone e servizi web

Gestione delle password

- Linee guida di utilizzo delle password
- Memorizzare le password in modo sicuro

Pratiche comuni di protezione

- Il decalogo per proteggersi

Security Lab

Security Lab si propone al mercato come azienda di consulenza nell'ambito dell'ICT Security o, come più recentemente e meglio definito, Cyber Security, annoverando tra i suoi clienti aziende che operano nel settore della finanza, dell'industria e delle telecomunicazioni in diverse nazioni.

Security Lab si avvale di personale altamente specializzato nei settori della sicurezza organizzativa, legale e tecnologica, con significative esperienze internazionali.

La costante attività di Security Lab di monitoraggio del mondo del crimine digitale e della scena underground consente di abbinare ad un approccio metodologico la conoscenza derivante dalla continua ricerca sulle vulnerabilità ed i crimini nella rete.

Zone-H

Zone-H, osservatorio digitale indipendente e open-source, è oggi la voce più autorevole in Internet in materia di crimine informatico. La home page di www.zone-h.org registra 35.000 singoli accessi al giorno per un totale di circa 800.000 click. I siti Zone-H sono attualmente disponibili in inglese e portoghese.

Informazione ed analisi in tema di cyber terrorismo e cyber crime, servizi per l'implementazione della security e programmi educational vengono elaborati e messi a disposizione della comunità IT che ogni giorno può contare su advisory, statistiche, aggiornamenti e informazioni, frutto di un costante monitoraggio della rete da parte dello staff Zone-H.

Il programma educational è frutto del know-how e dell'esperienza di Zone-H, che organizza corsi e seminari in tutto il mondo trattando gli aspetti fondamentali della Internet security con lo scopo di promuovere la diffusione della filosofia dell'osservatorio di prevenzione e il costante aggiornamento dei sistemi di difesa informatici tra i professionisti IT.