Il Giunto, Istituto Tecnico Industriale Statale "G. Cardano" - Pavia

Data articolo

26-05-2021

Autori

Riccardo Serci 4 BI

Chi è e cosa fa l'Ethical Hacker?

Nella mattinata del 18 marzo 2021 la nostra classe ha avuto un video-incontro con il dott. Lorenzo Grespan, che ci ha spiegato in che cosa consiste il suo lavoro di Ethical Hacker (Hacker Etico) presso un'azienda situata nel Regno Unito.

L'Ethical Hacker è sempre più ricercato dalle aziende di tutto il mondo, in quanto è un professionista informatico nell'ambito della sicurezza.

Al termine hacker si associa, in genere, un'immagine negativa: è visto come un pirata della rete, una figura ambigua che manomette i sistemi o si appropria di file per scopi malevoli.

Gli hacker "buoni", "etici" o "White Hat" si distinguono, invece, dai pirati informatici o "cracker" perché, al contrario di questi, operano a beneficio di aziende, enti e organizzazioni.

Essi vengono, infatti, autorizzati da quest'ultimi per effettuare i propri attacchi a reti, infrastrutture informatiche e siti web: questa autorizzazione garantisce la legalità delle loro attività di hacking.

Lo scopo è quello di identificare e risolvere eventuali vulnerabilità e migliorare, così, la sicurezza e la buona funzionalità del sistema analizzato.

Il fine,quindi, è "buono", ovvero vuole prevenire le attività criminali di hacker maligni, chiamati in gergo " Black Hat Hackers".

L'importanza di questo professionista diventa ancora più chiara se pensiamo, ad esempio, che anche i governi sono spesso vittime di attacchi sempre più complessi da parte di hacker malintenzionati.

Ogni impresa deve assicurare un trattamento riservato ai dati propri e dei clienti: ad esempio nomi, username e password, dati di contatto, informazioni personali e dei conti bancari…

Solitamente sono le aziende di grandi dimensioni che investono di più in sicurezza informatica, per ridurre al minimo il rischio di perdita o manomissione dei dati, oppure strutture che devono gestire dati

sensibili come banche, assicurazioni, strutture sanitarie, agenzie ed enti governativi (ad esempio nel settore della Difesa), società che raccolgono e analizzano enormi quantità di dati riguardanti i propri utenti.

Gli Ethical Hacker lavorano al computer, in ufficio oppure da remoto, con orari di lavoro che variano a seconda dei progetti e degli attacchi informatici in corso.

Gli attacchi possono essere di tipo virtuale: ad esempio attraverso l'uso di spyware, software spia che catturano informazioni all'interno della rete, e worm, software che si introducono nel sistema e consentono di controllare il computer da remoto.

Gli attacchi di tipo fisico, invece, consistono nel furto di unità di memoria, interruzione di corrente, danneggiamento delle apparecchiature…

Le possibilità di attacco sono potenzialmente infinite, limitate solo dalla creatività e dalle capacità tecniche dell'hacker.

Concluso l'attacco, l'Ethical Hacker prepara un documento in cui descrive la falla di sicurezza e propone le soluzioni per ripararla: pensa e opera come se fosse un attaccante malintenzionato, per poi poter intervenire come difensore del sistema informatico che ha tentato di sabotare.

Durante l'incontro il dott. Grespan, esperto di sicurezza informatica, ci ha presentato il suo lavoro in modo coinvolgente, arricchendo la presentazione con esempi tratti dalla sua esperienza e con suggerimenti utili.

Abbiamo compreso che per diventare un Ethical Hacker è necessaria una specializzazione dopo la scuola superiore e che questa offre interessanti opportunità di lavoro.

Ci ha illustrato , inoltre, alcuni pericoli che possiamo incontrare su Internet e come possiamo aggirarli: ad es. dobbiamo evitare di usare la stessa password su diversi siti e di navigare su pagine web non affidabili.

Riccardo Serci 4 BI