

## TEMA SULLA SICUREZZA INFORMATICA



Come sempre, è utile partire dalle definizioni. La prima è quella relativa alla sicurezza delle informatiche è caratterizzata “dalla salvaguardia della riservatezza, integrità e disponibilità delle informazioni gestite da un’organizzazione”. Una salvaguardia non solo da attacchi diretti, ma anche ad esempio da fenomeni come calamità naturali oppure da problemi accidentali e che non riguarda certo soltanto la difesa degli apparati informatici, dal momento che l’attenzione alla sicurezza delle informazioni esiste ben da prima dell’ICT. Più specificatamente rivolta alla protezione degli apparati informatici da azioni di attacco volontarie è la sicurezza informatica, che è un sottoinsieme della sicurezza delle informazioni, e che può essere definita come l’insieme di prodotti, servizi, regole organizzative e comportamenti individuali che proteggono i sistemi informatici di un’azienda.

L’Italia è stata la vittima preferita dagli hacker di tutto il mondo. Già ad ottobre, i dati diffusi dal Clusit, l’Associazione italiana per la Sicurezza Informatica, che facevano riferimento ai primi sei mesi dell’anno, attestavano la crescita degli attacchi informatici in Italia al 31% rispetto all’anno precedente, con 730 episodi definiti “gravi”. Non stupisce quindi che, a seguito degli attacchi degli ultimi mesi, il Governo italiano abbia sancito l’avvio di un piano che vede la definizione di una serie di misure per rafforzare la sicurezza cibernetica nazionale. Il testo dell’ultima manovra finanziaria, in particolare, prevede un fondo con una dotazione iniziale di 1 milione di euro per ciascuno degli anni 2019, 2020 e 2021 per potenziare gli investimenti e le dotazioni strumentali in materia di cyber security. Solo cambiando prospettiva sarà possibile salvaguardare i dati in movimento e dimostrarsi a prova di futuro.

Per le aziende servono nuove tecnologie per combattere il cybercrime, in un’era in cui dati e informazioni personali sono sempre più al centro dell’attenzione, sia per chi vuole impadronirsene e sfruttarli sia per chi deve tutelarli, la reputazione di un’azienda dipenderà sempre più da un’architettura di sicurezza completa.

Le aziende non potranno continuare a fare affidamento solo su infrastrutture IT tradizionali e le tecnologie per la protezione dalle bot, la crittografia a livello di applicazione, la sicurezza delle API e l’adozione dell’analisi comportamentale e dell’intelligenza artificiale avranno un ruolo sempre più di primo piano nella protezione dagli attacchi. Grazie a strumenti automatizzati e all’apprendimento automatico sarà possibile rilevare e mitigare gli attacchi con un livello di precisione e accuratezza mai visto prima.

Visure Italia, servizio specializzato in indagini patrimoniali, recupero crediti e informazioni commerciali, è stato hackerato. Con un tweet notturno gli attivisti informatici di LulzSec Italia hanno avvisato di “aver scoperto essere online, i dati di 46.604 utenti di @visureitaliacom”. E proprio nel giorno in cui “ha messo

online una nuova versione del proprio sito.” A dimostrazione della veridicità delle loro affermazioni gli hacker hanno anche pubblicato un’immagine con nome, cognome, professione, email e password dei clienti che avrebbero fruito del servizio.

A mio avviso l'Italia dovrà migliorare la propria sicurezza informatica il più presto possibile, bisogna combattere l'ignoranza dei cittadini in questo particolare ambito, sensibilizzare i giovani e con importanti investimenti cercare di limitare ai minimi termini gli attacchi informatici.

