



OPEN INNOVATION

Cybersecurity: rischi potenziali e possibili contromisure

Molto spesso è "l'utente" l'anello debole di tutta la catena.

La sensibilizzazione verso gli strumenti utilizzati è sicuramente determinante



DI VINCENZO GERMANO*

Sempre più spesso sentiamo parlare di criminalità informatica e sempre più spesso sentiamo che è in costante aumento, evidenziando la problematica principale della tecnologia e costringendoci a chiedere cosa sia la sicurezza informatica – identificata come *Cybersecurity* –, perché è essenziale e perché è importante essere sempre informati per evitare spiacevoli situazioni.

Come analizzato nell'approfondimento del numero precedente (*si veda Il Giornale dell'Ingegnere n.4/2022, ndr*) abbiamo identificato il termine *Cybersecurity* come onnicomprensivo per descrivere il "processo di protezione" contro ogni forma di criminalità informatica, dal furto di identità alle armi digitali internazionali, questo perché è una disciplina dedicata alla protezione dei dati ma anche dei sistemi, dei dispositivi, dei servizi utilizzati per elaborarli/archiviarli, mettendoli al sicuro da criminali informatici, garantendone l'integrità, la riservatezza e la disponibilità delle informazioni. Mantenere la sicurezza informatica in un panorama di minacce in continua evoluzione è una sfida per tutte le organizzazioni e sempre più spesso gli approcci reattivi tradizionali, nei quali le risorse vengono destinate alla protezione dei sistemi contro le minacce maggiormente conosciute, mentre le minacce meno conosciute non vengono quasi del tutto prese in esame, non sono più una tattica sufficiente. Per stare al passo con i mutevoli rischi per la sicurezza, è necessario un approccio più proattivo e adattivo,

infatti diverse organizzazioni in quest'ambito raccomandano di adottare il monitoraggio continuo e le valutazioni in tempo reale come parte integrante di un quadro di valutazione del rischio per difendersi da minacce sia note che sconosciute; tuttavia, in questo processo molto spesso è "l'utente" l'anello debole di tutta la catena, perciò indipendentemente dai dispositivi utilizzati, dai dati trattati, dai sistemi in essere, il fattore e la componente umana sono fondamentali: ciò vuol dire che la sensibilizzazione verso gli strumenti utilizzati con un occhio attento alla *Cybersecurity* è sicuramente determinante. Proprio con quest'ottica, la conoscenza e la condivisione delle informazioni sull'argomento possono aiutare l'utente finale a comprendere i rischi potenziali e gli ambiti in cui la *Cybersecurity* si applica, come imparare a difendersi e a cosa fare attenzione.

GLI AMBITI DELLA CYBERSECURITY

A tal proposito scindiamo i principali ambiti di applicazione della *Cybersecurity* e approfondiamo a grandi linee quelli che possono essere i rischi potenziali e le possibili contromisure che possono essere adottate. Primo ambito tra tutti è la **sicurezza dell'applicazione** (a cui per semplicità di trattazione possiamo accorpate anche l'ambito della sicurezza dei dispositivi mobili o *Mobile security*), ovvero un termine che si riferisce a diversi tipi di pratiche di sicurezza, progettate per garantire l'assenza di "vulnerabilità" delle applicazioni che potrebbero consentire l'accesso illecito a dati sensibili,

la modifica non autorizzata del codice o il dirottamento di risorse. Il termine "applicazione" è nella sua accezione più generale, comprendendo *software* per computer, siti web, o applicazioni per *smartphone*, che richiede agli esperti di sicurezza informatica di scrivere codice sicuro, progettare architetture di applicazioni sicure, implementare una robusta convalida dei dati per ridurre al minimo la possibilità di accesso non autorizzato o modifica delle risorse dell'applicazione. Infatti, la sicurezza implica l'affrontare le vulnerabilità risultanti da processi di sviluppo non sicuri nella progettazione, codifica e pubblicazione del *software*; questo perché un'applicazione compromessa potrebbe fornire l'accesso a dati che al contrario è progettata per proteggere. Sebbene questa missione sia abbastanza facile da capire, le applicazioni non sono così semplici come una volta e garantire che siano sicure è diventato più difficile, spesso perché i moderni ambienti di sviluppo *software* permettono di creare e distribuire *software* in modo rapido, stratificando e astruendo il progettista dalla complessità delle applicazioni moderne; sebbene questo approccio aiuti a fornire le applicazioni in modo più rapido ed efficiente, ha reso la sicurezza più complessa che mai, creando punti ciechi e incertezza sulle vulnerabilità al loro interno. Perciò il successo della sicurezza inizia nella fase di progettazione, ben prima della sua distribuzione. Un altro ambito è relativo alla **sicurezza sul Cloud e la sicurezza delle reti** (rispettivamente *Cloud Security* e *Network Security*): per quanto differenti e con finalità

diverse, trattiamoli come due ambiti affini per semplicità. Il primo è una disciplina che si occupa di proteggere i sistemi *cloud computing*, cercando di mantenere privati/sicuri tutti i dati all'interno dell'intera infrastruttura online, incluse applicazioni e piattaforme, con uno sforzo combinato dei *provider cloud* e dei clienti che li utilizzano (individui, piccole e medie imprese o grandi aziende). Se si pensa ai *provider cloud* che ospitano i servizi sui loro server attraverso connessioni Internet sempre attive (affinché i dati siano raggiungibili in ogni momento), si ha la necessità che vengano implementati strumenti e tecnologie per avere protezioni per l'accesso e la visibilità di dati sensibili, un esempio è la crittografia. Questa permette di "mischiare" i dati in modo che sia possibile leggerli solo con una chiave di decodifica in modo tale che se i dati vanno persi o rubati, saranno illeggibili e inutili. Altre protezioni riguardano il transito di dati, ovvero le reti private virtuali (VPN) e la gestione di identità e accessi (in inglese IAM, *Identity and Access Management*) che si occupa invece dei privilegi d'accesso concessi agli account degli utenti, oltre alla gestione di autenticazioni e autorizzazioni di tali account; gestione *password*, autenticazione multi fattore e altri metodi rientrano nelle competenze dell'IAM. Passando oltre e analizzando l'ambito della *Network Security*, in generale può essere considerato come il processo che consente di intraprendere misure preventive, sia fisiche che mediante *software*, per proteggere la rete infrastrutturale aziendale o privata da accessi non autorizzati, mal utilizzo,

modifica/distruzione oppure diffusione impropria di dati, creando quindi un ambiente in cui i dati e i sistemi possano essere utilizzati in modo sicuro.

Un ambito poco considerato e sviluppato fino a svariati anni fa, ma fondamentale per le imprese è il **Disaster recovery/business continuity planning**, ovvero il ripristino di emergenza e la pianificazione della continuità operativa. Nel caso in cui avvenga una violazione della sicurezza informatica, ci siano dei disastri naturali o eventi di altra natura, i dati devono essere protetti e l'attività deve poter continuare. Grazie a questo ambito le organizzazioni si preparano a mantenere in funzione i propri sistemi "critici" durante e dopo qualsiasi tipo di incidente (interruzioni di corrente, incendi, disastri naturali e altro) e a riprendere e recuperare le operazioni nel minor tempo possibile. Le politiche di ripristino di emergenza determinano il modo in cui l'organizzazione ripristina le operazioni e le informazioni per tornare alla stessa capacità operativa di prima dell'evento; al contrario la continuità operativa è il piano su cui l'organizzazione fa affidamento mentre cerca di operare senza determinate risorse. Infine, per quanto di ambiti se ne possono identificare ancora diversi, concludiamo con la **formazione dell'utente finale** (*End-user education*), che riguarda l'educazione alle buone abitudini (modifica della *password* e inserimento di una *password* complessa, autenticazione a 2 fattori e via dicendo). Considerando che "la conoscenza è potere", la consapevolezza dell'utente sulle minacce informatiche è preziosa in tutti gli ambiti della sicurezza, perciò fornire la giusta formazione sui suoi fondamenti è determinante per aumentare la consapevolezza delle migliori pratiche del settore, delle procedure e delle politiche organizzative, del monitoraggio e della segnalazione di attività sospette e dannose.

CONCLUSIONI

Abbiamo appena visto come la *Cybersecurity* può essere declinata in vari ambiti differenti e, grazie alla conoscenza dei rischi associati alla tecnologia, si possono limitare problematiche e ottenere vantaggi come la protezione da attacchi informatici e violazioni, la protezione di dati e reti, la prevenzione dell'accesso non autorizzato ma anche riduzione di tempi di recupero dopo una violazione. Nel prossimo articolo affronteremo alcune tipologie di minacce per aumentare la sensibilità verso tali aspetti e cercare di prevenire minacce e violazioni.

*INGEGNERE ELETTRONICO E COMPONENTE COMMISSIONI INNOVAZIONE E INGEGNERIA FORENSE ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO