Il valore di un framework integrato per un ambiente collaborativo sicuro

Author : Redazione

Date : 7 Giugno 2019

Estratto dalla relazione di Martina Casiraghi tenutasi al 10° Cyber Crime Conference 2019

Berlino, gennaio 2019, attacco hacker in Germania. I dati personali di centinaia di politici, inclusi quelli della cancelliera tedesca Angela Merkel, sono stati pubblicati su un account Twitter a seguito di un attacco hacker. Il ministro della giustizia tedesco è intervenuto sulla questione definendo l'hackeraggio un grave attacco alla democrazia.

Amsterdam, febbraio 2019, studenti e tirocinanti presso una delle principali cliniche sanitarie della città, per anni hanno avuto libero accesso ai dati personali e record medici di centinaia di pazienti. Scandalo non solo per la capitale olandese, ma anche per l'intero mondo della sanità.

Oslo, marzo 2019, attacco hacker contro Norsk Hydro, gigante mondiale nella filiera del metallo. A seguito dell'attacco, Norsk Hydro ha dovuto interrompere la produzione in molteplici impianti in tutto il mondo. In generale, l'industria del metallo e mineraria risultano essere le più vulnerabili: il 97% delle società del settore ammette di avere tutt'ora difese inadeguate.

Roma, aprile 2019, chi sarà il prossimo?

Di fronte ad uno scenario così allarmante, l'unica arma è la prevenzione Buongiorno a tutti, io sono Martina Casiraghi, International Marketing Executive per Boole Server. Quest'oggi intraprenderemo insieme un viaggio nel mondo della Cyber Security e cercheremo soprattutto di comprendere il valore di un framework integrato per un ambiente collaborativo sicuro.

Dunque, iniziamo il nostro viaggio con una domanda: perché tutta questa necessità di intervento e di prevenzione?

Perché i dati che abbiamo sotto gli occhi sono allarmanti: il 41% delle aziende detiene più di 1000 file con contenuto altamente confidenziale, tra cui i dati delle carte di credito o

informazioni personali sui propri dipendenti, lasciati completamente in chiaro. Un file su 5 risulta non protetto, quindi potenzialmente accessibile a qualsiasi utente non autorizzato, e meno di un terzo delle aziende può contare su un piano strategico di Cyber Security. Uno scenario di estrema fragilità.

Chi si approfitta di questa vulnerabilità?

In primis, il cybercrime che sta raggiungendo livelli di sofisticatezza senza precedenti. Pensate che, a livello globale, si verifica in media un attacco informatico ogni 39 secondi.
Questo vuol dire che, per esempio, da quando io ho iniziato a parlarvi questa mattina, nel mondo si sono verificati almeno 4 casi di attacchi.
Nel quadriennio 2014-2018 c'è stato un incremento del 77,8% del numero di attacchi gravi.
Passando all'Italia, lo scenario non è di certo più confortante: il 55% delle aziende ammette di aver subito almeno un attacco informatico.

Quali sono i settori più colpiti?
In primis la sanità, seguono la pubblica amministrazione, l'istruzione e il settore finanziario.
Seconda criticità è l'errore umano.
Analisti ed esperti di sicurezza, infatti, concordano nell'affermare che la maggior parte degli incidenti di sicurezza sia legato all'errore umano: tra l'80% e il 90% dei casi.

Cosa si intende quando si parla di errore umano?
Intendiamo anche la semplice negligenza. Pensate che il 97% degli utenti abitudinari di internet non è in grado di riconoscere una e-mail di phishing.
La leggerezza nel pubblicare informazioni strettamente personali sul web, la scarsa consapevolezza delle policy e delle procedure aziendali in tema di security, l'uso di password banali e spesso ripetute su più account, o ancora, anche la semplice distrazione, per esempio quando ci si dimentica di effettuare il logout prima di lasciare il proprio dispositivo, quindi lasciandolo potenzialmente in preda di qualsiasi sguardo indiscreto.

Terza criticità, lo scenario contemporaneo.
Ricco, certo, di nuovi trend e nuove potenzialità, ma al tempo stesso incubatore di nuovi e potenziali rischi.

Pensiamo anche solo ai nuovi trend dell'Industria 4.0, a partire da algoritmi e tecniche dell'intelligenza artificiale, passando per il machine learning, la realtà aumentata, blockchain, così come la progressiva decentralizzazione delle architetture logiche e tecnologiche e l'avvento di soluzioni in Cloud. O ancora il boom dei dispositivi, quindi l'accesso dei dati via mobile.

Chi di noi, infatti, questa mattina non ha guardato, per esempio, le proprie e-mail personali o di lavoro almeno una volta dallo smartphone?
Quindi, la vera domanda sembra essere: "chi e cosa rimane effettivamente all'interno dei confini aziendali? Ha ancora senso parlare di utenti interni e utenti esterni, dati all'interno del perimetro aziendale e dati all'esterno del perimetro aziendale?".
Quello che è certo è che i confini si sono fatti sempre più labili. E proprio per questo motivo, al

crescere della complessità degli ambienti IT, anche le esigenze di gestione e quindi di sicurezza aumentano.

Perché bisogna intervenire fin da subito?
Perché l'impatto sul business in caso di Data Loss sarebbe catastrofico.
L'azienda andrebbe incontro innanzitutto a una perdita finanziaria diretta, subirebbe un forte rallentamento delle attività, perderebbe in termini di competitività, subirebbe pesantissimi danni all'immagine, così come una perdita di credibilità.
Dovrebbe affrontare tutta una serie di pesantissime sanzioni di carattere normativo e, infine, sobbarcarsi tutta una serie di costi di ripristino.
Quindi diventa prerogativa dotarsi di un piano strategico di Cyber Security.
Perché? Perché, ricordiamocelo, servono 20 anni per costruirsi una reputazione, bastano 20 secondi per rovinarsela.
Cosa possiamo dedurre da quello che abbiamo visto velocemente finora?
Che è necessario un cambio di paradigma.
In particolar modo, passare da un approccio classico basato sul Risk Management a una gestione preventiva della minaccia.
Come?
Tramite un approccio olistico che tenga in considerazione diversi aspetti.
Certo la sicurezza delle piattaforme dei sistemi usati, ma anche il fatto di avere a disposizione un corpus di policy sempre aggiornato, così come puntare alla formazione del personale, oppure si rende necessario un commitment trasversale tra tutte quelle che sono le principali funzioni aziendali.
Solo in questo modo è possibile creare un vero e proprio ecosistema di protezione dati, che non può che avere effetti positivi sulla mia azienda.
In primo luogo, l'aumento della capacità di prevenzione da qualsiasi potenziale minaccia; in secondo luogo, l'aumento della sicurezza di sistemi, piattaforme, impianti utilizzati; in terzo luogo, un aumento della stabilità aziendale nel suo complesso.

E arriviamo così al concetto di resilienza, cosa vuol dire?
Significa che, in caso anche di evento avverso, la mia azienda è in grado di reagire in maniera attiva e proattiva. Ho quindi raggiunto il mio goal ultimo, quello di diventare Cyber-resilient.

Continua a leggere…