Analizzando le violazioni disicurezza famose nella storiaaa

Da qualche anno, anzi ormai da decenni, lasicurezza informatica è diventata un nervo scoperto.Non colpisce tutti allo stesso modo, ma gli incidentiseri si accumulano. In alcuni casi si registranomiliardi di record sottratti in una notte, con ricaduteeconomiche, sociali e persino politiche che, a primavista, sembrano sproporzionate. Dai grandi dellatecnologia alle infrastrutture critiche, quasi nessunsettore appare davvero al riparo. Studiare questiepisodi non offre ricette magiche, ma aiuta: sicapisce come mutano le minacce, doveinciampiamo più spesso e, forse, come evitare glistessi errori. Le cifre parlano chiaro: miliardi diaccount compromessi e danni che possono arrivarea centinaia di milioni di dollari, a volte anche di più.

I giganti della tecnologia sottoattacco

Occorre citare subito un caso ricorrente in ognidiscussione: Yahoo. Tra il 2013 e il 2014, stando a quanto reso noto, furono coinvolti circa 3 miliardi diaccount. Nel 2016 se ne aggiunsero altri 500 milioni.Non vennero sottratte solo email e date di nascita,ma anche domande di sicurezza,concepite persalvare l’accesso. L’impatto fu significativo anche sulfronte business: il prezzo divendita aVerizon furitoccato al ribasso di 350 milioni di dollari. Da quelmomento, piattaforme onlinedi ognitipo, dai socialai casino online, iniziarono a irrigidire le difese neltimore di rinnovati attacchi.

Anche Facebook ha affrontato gravi problemi. Nel2021, i dati di circa 533 milioni di utenti di 106paesi sono comparsi in forum di hacking. Numeri ditelefono e dettagli personali sono stati pubblicati,ossia informazioni che nessuno vorrebbe incircolazione. L’impressione generale è che la scaladel problema fosse stata sottovalutata.

Quando i dati intimi diventanopubblici

Quando la fuga riguarda informazioni intime, non solo dati anagrafici, l’impatto è ancora più grave. Il caso CAM4 del 2020 è spesso citato come emblematico e molto imbarazzante. Un server mal configurato lasciò esposti più di 11 miliardi di record: un’enormità. Tra questi figuravano preferenzee dettagli personali molto sensibili. Un errore banale di configurazione è bastato a causare il danno. Sembra incredibile, ma è successo proprio così. La lezione che emerge è brutale: non si tratta solo di privacy violata; il materiale esposto può essere usato per ricatti o pressioni. Sono necessari protocolli rigorosi, controlli continui e un sano livello di paranoia nella gestione di dati così delicati.

Ransomware che paralizza le infrastrutture

Per quanto riguarda il ransomware, WannaCry nel 2017 ha segnato un cambiamento: oltre 200.000 computer in circa 150 paesi sono stati colpiti sfruttando una falla di Windows. Non si tratta di un film: ospedali britannici rallentati, ritardi nei servizi e il sistema ferroviario tedesco tra le vittime. Una sola vulnerabilità con conseguenze globali riassume bene la situazione.

Il caso Colonial Pipeline nel 2021 ha reso l’impatto ancora più concreto: la benzina alle pompe si esaurì, o quasi. L’attacco ha bloccato la distribuzione di carburante, con effetti a catena sulla East Coast americana, dove passa il 45% del flusso. L’azienda ha pagato un riscatto di 4,4 milioni di dollari; una parte fu recuperata dalle autorità. Non è stato un lieto fine, ma nemmeno il peggiore.

Il settore delle telecomunicazioni nel mirino

Un esempio significativo riguarda il cuore delle comunicazioni: Syniverse. Nel 2021 è emersa una