IL FOGLIO

27-OTT-2017
pagina 2
foglio 1

1234567890

La cybersicurezza non è solo un problema di password rubate, ma una priorità per ogni azienda

Milano. Basta contare fino a 60 ed ecco che in rete sono state eseguite oltre duecento milioni di operazioni. Oppure, per restare in Italia, nelle 24 ore della giornata di ieri Terna Spa (il gestore unico di tutta la rete elettrica italiana, ossia il soggetto che consente di svolgere qualsiasi attività tecnologica) ha subito 5.700 (sì, cinquemilasettecento) attacchi informatici e ricevuto 80.000 email tra spam e fishing, fortunatamente con zero violazioni.

La cybersecurity è la seconda emergenza in Europa, dopo i temi ambientali e prima dell'immigrazione, come emerge anche dall'ultimo meeting sullo stato dell'Unione europea dello scorso 13 settembre; tutte le grandi aziende e le infrastrutture critiche nazionali subiscono ogni giorno attacchi informatici e nel solo 2016 il 47 per cento delle aziende piccole e medie in Italia ha subito almeno un attacco, con costi medi di 3,5 milioni di euro per ogni attacco andato a buon fine, mentre per le piccole e medie imprese gli attacchi informatici possono mettere a repentaglio l'esistenza della azienda stessa.

Partendo da queste premesse, ieri a Milano si è svolta la terza edizione di WOW (Wide Opportunities World), la conferenza annuale con cui Samsung chiama a raccolta il mondo delle aziende e della ricerca per discutere e approfondire un argomento specifico e attuale per il mondo della tecnologia. Il tema scelto è stato, per l'appunto, la cybersicurezza. Il presidente di Samsung Italia, Carlo Barlocco, ha iniziato la sua relazione centrando subito il punto: l'evoluzione digitale è un grande traguardo, ma la digital transformation senza controllo è nulla. Parafrasando un celebre slogan pubblicitario, la connessione è nulla senza controllo. Questo è già vero oggi, ma lo sarà ancora di più nei prossimi anni quando intelligenza artificiale (AI) e internet delle cose (IoT) saranno le basi attraverso cui fruiremo dei servizi tecnologici. Oggi tutti i grandi produttori mondiali stanno elaborando hardware e software che operino sull'intelligenza artificiale (si pensi agli assistenti virtuali Bixby di Samsung e Assistant di Google o al nuovo chip a reti neurali presentato da Huawei sul suo smartphone top di gamma, Mate 10 Pro) e, allo stesso modo, dispositivi fissi e mobili connessi alla rete abbracciano ormai praticamente tutti i settori della vita personale e lavorativa. L'internet delle cose è sempre di più una realtà quotidiana e non soltanto un'idea concept delle fiere di informatica (auto, sistemi di sorveglianza, mobili per la casa, frigoriferi, aspirapolvere, penne, orologi, bracciali: tutto connesso alla rete, integrato e comandabile anche a distanza dai propri smartphone). Proprio nello IoT Samsung può giocare il ruolo di leader, perché nessun altro produttore può vantare una presenza così diretta e di lungo corso in tutti i principali settori della tecnologia e del mondo consumer (dai processori ultra avanzati ai sensori per le fotocamere, dai prodotti per la casa ai servizi per le aziende).

I dati che riverseremo nel mondo digitale aumenteranno ancora (e già adesso sono moltissimi), di conseguenza aumenterà l'esigenza della sicurezza, sia nel mondo consumer che in quello business.

Una consapevolezza culturale

Per questi motivi, la lotta ai crimini informatici deve partire anzitutto da una consapevolezza culturale: tutti gli utenti devono essere bene informati su cosa stanno riversato in rete e su quali strumenti hanno a disposizione per controllare i loro spazi virtuali. In secondo luogo, le aziende devono pensare alla cybersecurity come un obiettivo strategico, perché i costi economici e reputazionali provocati dagli attacchi hacker sono enormemente superiori agli oneri da sostenere per una adeguata protezione. Insomma, la cybersecurity può apparire come un tema poco attuale o di nicchia e proprio per questo c'è il rischio concreto di sottovalutarlo. In gioco non ci sono solo le nostre password di Facebook e le nostre foto delle vacanze sul cloud, c'è in ballo la sicurezza di tutte le aziende connesse del pianeta e, non ultimo, il modello di sviluppo in grado di determinare quali saranno i player economici protagonisti delle prossime evoluzioni tecnologiche, a prescindere che operino nel mondo digitale o in quello tradizionale. Perché, si sa, in una guerra (anche informatica) chi ha saputo leggere prima le mosse degli avversari, vince.

Marco Giorgio