TECNOLOGIA/6 La spinta alla digitalizzazione e all'interconnessione dei dispositivi sono le sfide attuali a cui si dovrà necessariamente guardare anche in futuro per la cybersecurity Mentre si lavora a nuovi sistemi di difesa su quantum computing e intelligenza artificiale

Sicurezza in formato IoT

di Nicola Carosielli

L'avanzata tecnologica e la crescente digitalizzazione di industria e società, si accompagnano a un sempre maggiore bisogno di protezione dagli attacchi cyber da parte di aziende e cittadini. Una necessità forse lapalissiana e che, secondo una ricerca di Cybersecurity Ventures, dovrebbe spingere la spesa globale per i servizi di sicurezza informatica a 1.750 miliardi considerando il periodo dal 2021 al 2025. Eppure questa potrebbe forse rivelarsi anche poco sufficiente a contrastare l'offensiva degli hacker, visto che i crimini informatici potrebbero arrivare a costare al mondo qualcosa come 10.500 miliardi l'anno entro il 2025, più del triplo rispetto ai 3 mila miliardi di dieci anni fa, passando per i 6 mila miliardi di dollari del 2021.

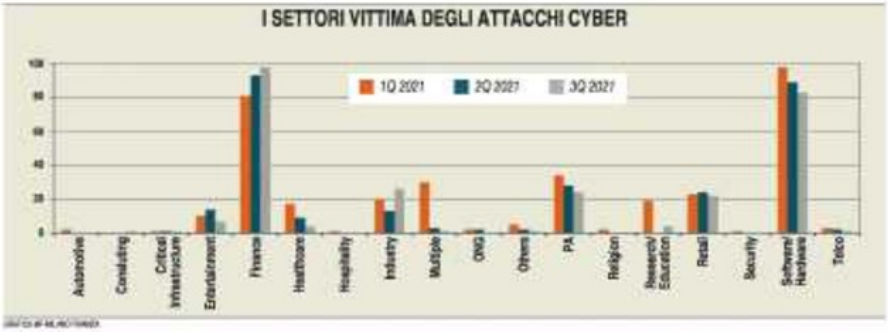
Questi dati rendono l'idea della necessità di armarsi adeguatamente. E per farlo è necessario individuare le aree d'azione su cui intervenire nel futuro tanto nel presente. «Il tema del futuro per la cybersecurity è il tema del presente ed è l'Internet of Things (IoT)» dice a *MF-Milano Finanza* Domenico Raguseo, Domenico Raguseo, direttore Cybersecurity di Exprivia, sottolineando come «mentre parliamo di cybersecurity collegandola spesso ai server, ai dati, non ci rendiamo conto che siamo circondati da migliaia di dispositivi intelligenti che regolano oramai la nostra vita. E si basano sugli stessi protocolli che possono essere compromessi nel mondo It, creando numerosi danni». Quotidianamente, secondo i dati a disposizione dell'osservatorio Exprivia, si affacciano sul territorio italiano qualcosa come 7-8 milioni di dispositivi IoT e solo considerando un particolare protocollo, il IPv4. Tali dispositivi, spiega, Raguseo, «hanno un'intelligenza, sono collegati a internet e possono essere compromessi; si tratta di dispositivi che consentono di regolare la temperatura della casa, sono collegati alle videocamere di sorveglianza e così via, per di più molti di questi dispositivi sono connessi anche senza protocollo di autenticazione, o al massimo con password di default». Un attacco in queste condizioni può portare sia a un danno incredibile per il servizio erogato ma potrebbe creare danni peggiori se si trattasse di un attacco cosiddetto Distributed Denial of Service (Ddos), che prevede la cattura di diversi computer (in questo caso quei potenziali 7-8 milioni) cui segue il lancio, nello stesso istante, di transazioni verso un punto unico che può essere un'applicazione o uno sportello bancario.

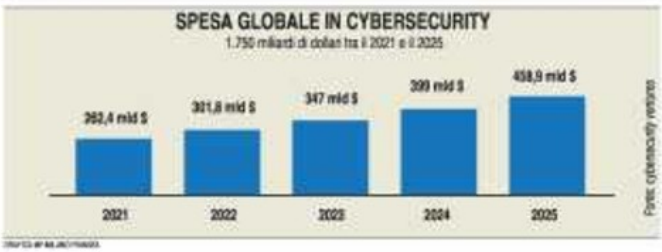
Tutto ciò, «si porta dietro un problema di carattere etico che bisogna porsi in quanto individui e che consiste, per certi versi, nella corresponsabilità che un attacco venga portato a termine, creando danni. Serve, dunque, fare la propria parte affinché il cybercrime non venga perpetrato, come succede già per alcune fattispecie previste dalla legge». La legislazione non è ancora dettagliata, ovviamente ma secondo Raguseo, si va verso un cambio nella normativa, seppur sono necessari accordi generali.

. Un'occasione che lascia intravedere anche un cambiamento nei servizi di consulenza: «Queste figure sono altamente formate, sono richieste grandissime competenze e di conseguenza rappresentano un costo elevato per l'azienda». In questo senso è chiaro, dunque, che «una gorssa azienda possa non avere problemi a strutturarsi al meglio, ma le piccole medie imprese, che rappresentano poi la vera ossatura economica del nostro Paese, avranno più difficoltà, facendo crescere di conseguenza la domanda per società di consulenza in grado di fornire questo tipo di figure professionali».

All'orizzonte, tra i temi ai quali si dovrà guardare per la sicurezza informatica non non ci sarà però solo l'IoT. «La cybersecurity è strettamente collegata al progresso tecnologico», nota infatti Raguseo, delineando nuovi trend come quello del quantum computing o dell'intelligenza artificiale (Ai). «Ogni volta che viene aggiunta una nuova tecnologia dobbiamo essere abituati a comprendere come questa innovazione possa essere usata dai cybercriminali; ora si parla molto di quantum computing, ma si dovrà dare spazio anche all'Ai, su cui ancora oggi ci sono tantissime aree di sviluppo e che dovrebbero preoccupare chi si occupa di cybersecurity». L'Artificial Intelligence, per esempio, può essere usata per attacchi come le campagne di malvertisement o addirittura per imparare tecniche di attacco senza che nessun insegnamento. Il quantum computing, che di fatto aumenta la capacità elaborativa, potrebbe invece essere usato per accorciare a livello record i tempi di decriptaggio mettendo sostanzialmente in discussione tutti i sistemi di criptografia.

Lo scenario che ci si para davanti dunque, per quanto eterogeneo, sarà soprattutto focalizzato sul quantum computing e l'Ai, senza però dimenticare che tutto il futuro della cybersecurity passa dal presente che, indiscutibilmente, riguarda la grande spinta all'interconnessione di tutto l'ecosistema digital. (riproduzione riservata)





Sicurezza in formato IoT

L'avanzata tecnologica e la crescente digitalizzazione di industria e società, si accompagnano a un sempre maggiore bisogno di protezione dagli attacchi cyber da parte di aziende e cittadini. Una necessità forse lapalissiana e che, secondo una ricerca di Cybersecurity Ventures, dovrebbe spingere la spesa globale per i servizi di sicurezza informatica a 1.750 miliardi considerando il periodo dal 2021 al 2025. Eppure questa potrebbe forse rivelarsi anche poco sufficiente a contrastare l'offensiva degli hacker, visto che i crimini informatici potrebbero arrivare a costare al mondo qualcosa come 10.500 miliardi l'anno entro il 2025, più del triplo rispetto ai 3 mila miliardi di dieci anni fa, passando per i 6 mila miliardi di dollari del 2021. Questi dati rendono l'idea della necessità di armarsi adeguatamente. E per farlo è necessario individuare le aree d'azione su cui intervenire nel futuro tanto nel presente. «Il tema del futuro per la cybersecurity è il tema del presente ed è l'Internet of Things (IoT)» dice a MF-Milano Finanza Domenico Raguseo, Domenico Raguseo, direttore Cybersecurity di Exprivia, sottolineando come «mentre parliamo di cybersecurity collegandola spesso ai server, ai dati, non ci rendiamo conto che siamo circondati da migliaia di dispositivi intelligenti che regolano oramai la nostra vita. E si basano sugli stessi protocolli che possono essere compromessi nel mondo It, creando numerosi danni». Quotidianamente, secondo i dati a disposizione dell'osservatorio Exprivia, si affacciano sul territorio italiano qualcosa come 7-8 milioni di dispositivi IoT e solo considerando un particolare protocollo, il IPv4. Tali dispositivi, spiega, Raguseo, «hanno un'intelligenza, sono collegati a internet e possono essere compromessi; si tratta di dispositivi che consentono di regolare la temperatura della casa, sono collegati alle videocamere di sorveglianza e così via, per di più molti di questi disposiditivi sono connessi anche senza protocollo di autenticazione, o al massimo con password di default». Un attacco in queste condizioni può portare sia a un danno incredibile per il servizio erogato ma potrebbe creare danni peggiori se si trattasse di un attacco cosiddetto Distributed Denial of Service (Ddos), che prevede la cattura di diversi computer (in questo caso quei potenziali 7-8 milioni) cui segue il lancio, nello stesso istanto, di transazioni verso un punto unico che può essere un'applicazione o uno sportello bancario. Tutto ciò, «si porta dietro un problema di carattere etico che bisogna porsi in quanto individui e che consiste, per certi versi, nella corresponsabilità che un attacco venga portato a termine, creando danni. Serve, dunque, fare la propria parte affinché il cybercrime non venga perpetrato, come succede già per alcuine fattispecie previste dalla legge». La legislazione non è ancora dettagliata, ovviamente ma secondo Raguseo, si va verso un cambio nella normativa, seppur sono necessari accordi generali. . Un'occasione che lascia intravedere anche un cambiamento nei servizi di consulenza: «Queste figure sono altamente formate, sono richieste grandissime competenze e di conseguenza rappresentano un costo elevato per l'azienda». In questo senso è chiaro, dunque, che «una gorssa azienda possa non avere problemi a

strutturarsi al meglio, ma le piccole medie imprese, che rappresentano poi la vera ossatura economica del nostro Paese, avranno più difficoltà, facendo crescere di conseguenza la domanda per società di consulenza in grado di fornire questo tipo di figure professionali». All'orizzonte, tra i temi ai quali si dovrà guardare per la sicurezza informatica non non ci sarà però solo l'IoT. «La cybersecurity è strettamente collegata al progresso tecnologico», nota infatti Raguseo, delineando nuovi trend come quello del quantum computing o dell'intelligenza artificiale (Ai). «Ogni volta che viene aggiunta una nuova tecnologia dobbiamo essere abituati a comprendere come questa innovazione possa essere usata dai cybercriminali; ora si parla molto di quantum computing, ma si dovrà dare spazio anche all'Ai, su cui ancora oggi ci sono tantissime aree di sviluppo e che dovrebbero preoccupare chi si occupa di cybersecurity». L'Artificial Intelligence, per esempio, può essere usata per attacchi come le campagne di malvertisement o addirittura per imparare tecniche di attacco senza che nesun insegnamento. Il quantum computing, che di fatto aumenta la capacità elaborativa, potrebbe invece essere usato per accorciare a livello record i tempi di decriptaggio,mettendo sostanzialmente in duscussione tutti i sistemi di criptografia. Lo scenario che ci si para davanti dunque, per quanto eterogeneo, sarà soprattutto focalizzato sul quantum computing e l'Ai, senza però dimenticare che tutto il futuro della cybersecurity passa dal presente che, indiscutibilmente, riguarda la grande spinta all'interconnessione di tutto l'ecosistema digital. (riproduzione riservata)