Innovare per difendersi: la cybersecurity si evolve con l'AI

Nell'era dell'intelligenza artificiale, come difendersi dai possibili attacchi e trasformare questo strumento in opportunità? Ne parliamo con Jelena Zelenovic Matone, CISO presso Banca Europea per gli Investimenti.

di Giusy Scoppetta

«La tecnologia fa un salto in avanti e ridefinisce il nostro modo di vivere, tutto ciò porta con sé un entusiasmo e un senso di potere enorme; allo stesso tempo ci pone di fronte alla scelta su come utilizzare questo nuovo grande mezzo, l'AI: utilizzarla per creare, dunque costruire, o per distruggere? La scelta è nelle nostre mani». Sono parole sicure quelle di Jelena, pronunciate con quella incisività che vuole essere anche provocazione in noi che stiamo ascoltando. Il punto è chiaro: in un mondo in cui la cybersecurity sta cambiando, dobbiamo esser pronti a ridefinire il nostro modo di difenderci. È indispensabile far fronte ai possibili attacchi e per farlo dobbiamo iniziare a comprendere le potenzialità che l'AI possiede anche come strumento di protezione. Dal suo intervento, nascono spontanee alcune domande, che le poniamo a margine. Insieme parliamo di diversità, resilienza digitale e futuro; perché alla fine dobbiamo guardare tutti nella stessa direzione.

Lei è presidente di Women Cyber Force, un'organizzazione che promuove la diversità nel settore cyber security. Quanto è importante la diversità per contrastare la criminalità informatica?

È estremamente importante per proteggere l'organizzazione in altri modi, anche se al momento vi è ancora un'errata convinzione sulla cybersecurity. Si pensa sia una black box, con un unico interesse per la progettazione, e questo potrebbe essere un motivo per il quale molte persone, soprattutto donne, sono intimorite da questo ambito. In realtà la cybersecurity è molto di più: si occupa di monitoraggio, creazione di policy, compliance e sensibilizzazione. Dunque, abbiamo bisogno di diversità, non solo da un punto di vista di genere, ma anche culturale, educativa e di mentalità. Di sicuro, dobbiamo sapere come lavorare con persone diverse e mantenerle motivate a lavorare. Nel caso delle donne: vivono la cybersecurity in modo diverso e forse, senza altri modelli femminili a cui guardare, possono scoraggiarsi. In questi casi è necessario il mentoring.

Come convivono innovazione e rispetto delle normative?

Sicuramente hanno tempi diversi, l'innovazione va molto più veloce delle normative, che invece hanno un percorso più lento, dovendo esser approvate. L' AI corre: ogni giorno puoi avere una nuova app, idee innovative, pensare a nuove attività. Possono coesistere? Direi di si. Come già detto, è qualcosa per cui lottiamo tutti: consentire l'innovazione, ma essere sicuri. Dobbiamo tenerla d'occhio: l'innovazione senza governance e regolamentazione è sconsiderata, la regolamentazione senza innovazione è semplicemente sterile. Quindi, come professionisti, dobbiamo lavorare affinché si mantenga una via di mezzo. Per esempio, nel caso dell'AI, ChatGPT può benissimo esistere, ma va monitorata, assicurandosi di proteggere i dati correttamente. Devono esserci trasparenza e spiegabilità, ma allo stesso tempo si deve consentire che l'innovazione accada, anche se naturalmente non è semplice.

La resilienza informatica è la nuova moneta della fiducia digitale. Non basta saper evitare gli attacchi, ma bisogna ripartire più forti di prima?

Sì, bisogna ripartire, imparando da ogni attacco quali sono le lacune. Devi ricominciare agendo meglio, perché devi recuperare affinché la tua attività continui. La cosa più importante nel nostro campo è la condivisione di informazioni e il networking con circoli fidati, non solo all'interno dell'organizzazione o all'interno del Paese, ma tra Paesi, specialmente in ambito UE. Per esempio, abbiamo alcune buone reti, come CERT, che comunicano tra

loro e pubblicano informazioni per tutte le organizzazioni circa i nuovi attacchi. Ovviamente, ripuliscono i dati, non dicendo chi è stato attaccato. Qual è l'alternativa? Chiudi l'attività. Ma quando vieni attaccato, è lì che impari ed è lì che crei nuovi possibili scenari per proteggere la tua organizzazione. Ogni giorno, in modo costante, utilizziamo l'intelligenza artificiale – attraverso strumenti come i SOAR – per creare nuovi scenari. Analizziamo ciò che accade nella nostra rete, individuiamo anomalie e pattern e da questo l'AI genera automaticamente nuovi scenari per aiutarci a identificare i potenziali attacchi in arrivo. In questo senso, l'AI è ormai parte integrante del nostro lavoro quotidiano. La lezione più importante è una: bisogna sempre rialzarsi. Un'organizzazione o ade o trova la forza di andare avanti. Quando ci riesce, ne esce più forte di prima.

Quali saranno tra cinque anni le nuove frontiere della cybersecurity?

Considerando la velocità con la quale avanza l'intelligenza artificiale, è impossibile sapere con certezza cosa ci aspetta lungo la strada. Nascono innovazioni ogni giorno sia dal lato positivo – quello della protezione e della sicurezza – che da quello negativo, ovvero degli attaccanti. Mi auguro che ci sia nei prossimi anni una maggiore prontezza, soprattutto riguardo al Post-Quantum Computing (PQC), l'insieme di algoritmi di crittografia progettati per resistere agli attacchi dei computer quantistici. Spero che l'Unione Europea, come sistema unitario, sia pronta ad affrontare le sfide legate all'informatica quantistica. Mi auguro vengano sviluppati nuovi strumenti per difenderci da minacce legate all'AI che non sappiamo ancora gestire, come i deepfake e i phishing estremamente sofisticati e convincenti più di quelli creati da un essere umano. Di sicuro ci saranno nuove innovazioni anche da parte degli attaccanti. Per quanto spaventoso possa sembrare, ogni nuova minaccia ci costringerà a evolverci per creare nuove forme di difese. Cinque anni, oggi, sono un periodo lunghissimo ed è difficile immaginare cosà accadrà, soprattutto ora che abbiamo liberato il potenziale dell'intelligenza artificiale.

Avere risposte sul futuro non è semplice, ciò che sappiamo è che il futuro della cybersecurity non sarà solo nelle nuove tecnologie, ma nelle competenze, nelle nostre capacità di sfruttare i nuovi strumenti. Forse – per dirlo con Jelena – l'unica risposta certa è la resilienza: cadere, ma sapersi rialzare più forti di prima.