ARTICOLO DI OPINIONE

QUALI SONO LE SFIDE PER LA SICUREZZA INFORMATICA NEL 2023?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Dopo il Covid-19 come tema principale del 2021, il 2022 è stato segnato da altre forti tendenze: crisi economiche, ecologiche e sociali, conflitti geopolitici o l'emergere di un'intelligenza artificiale accessibile a tutti... Come orientarsi per il prossimo anno? Quali saranno le sfide per la sicurezza informatica nel 2023? Esercizio relativo a marketing diretto e tendenze.

LA SFIDA DEL RECLUTAMENTO

Il mercato della sicurezza informatica è soggetto da diversi anni a una grave carenza di manodopera. Secondo lo studio *Cybersecurity Workforce Study 2022,* dovrebbero essere occupati non meno di 3,7 milioni di posti di lavoro in tutto il mondo.

Colto dalle ondate delle grandi dimissioni post-lockdown, anche il settore della sicurezza informatica sta vedendo esplodere il suo tasso di turnover. Secondo questo stesso studio, il 21% degli intervistati avrebbe cambiato lavoro negli ultimi 12 mesi, con un aumento del 13% rispetto allo scorso anno. Stipendio, condizioni di lavoro, scopo dell'azienda: sono tutti elementi che oggi rientrano in parti uguali nella decisione finale dei candidati.

Una penuria che arriva a porre una domanda terribile: **un'azienda di sicurezza informatica può morire per mancanza di risorse umane?** Per alcune società di servizi legati alla sicurezza informatica, il 2022 è stato un vero banco di prova. Una situazione destinata a dilagare nel 2023: verso un SOC senza risorse e che non può reagire abbastanza rapidamente a un allarme critico? Verso aziende senza CISO?

Ma il settore si sta mobilitando e si sta attivando. Considerato come il contesto geopolitico del 2022 abbia spinto gruppi di hacker etici a sostenere i governi, è possibile che questo movimento continui nel 2023. Fino a strutturarsi? Dall'altro lato, la sensibilizzazione nelle scuole o anche il numero crescente di corsi di formazione sulla sicurezza informatica rappresentano vere promesse per il futuro. Ma la creazione di questi nuovi talenti pone poi altri interrogativi: quanto presto saranno disponibili? È una strategia affidabile a lungo termine? Su questo stesso tema del reclutamento, dobbiamo osservare con attenzione ciò che sta accadendo a Google, Microsoft o persino Meta... **E se l'ondata di licenziamenti nel settore tecnologico fosse un'opportunità per la sicurezza informatica?** Come la domanda, anche il mercato è aperto.

LA SFIDA DELLA COLLABORAZIONE TRA EDITORI

Data la sofisticatezza degli attacchi informatici, l'analista non può più fare affidamento esclusivamente sui dati segnalati dal firewall a livello di rete o dall'agente di protezione a livello di workstation. Deve avere una visione d'insieme di ciò che sta accadendo nel sistema informatico.

Per consentirgli di ottenere questa visione d'insieme, un prodotto di sicurezza informatica deve aggregare, correlare e classificare i dati che produce e riceve. Perché è la condivisione di questi flussi di dati, prodotti da fonti diverse come database con una buona reputazione o informazioni di *Cyber Threat Intelligence* (CTI), che permette di rilevare al meglio la minaccia. **Rilevamento, protezione, riparazione diventano quindi parti diverse dello stesso meccanismo**. La sicurezza informatica così come la conosciamo si sta evolvendo, con l'adozione di tecnologie come EDR, XDR e NDR. Ma questo approccio può anche andare di pari passo con un accumulo di prodotti di sicurezza informatica nelle aziende: un aspetto da pianificare per le grandi aziende e un grattacapo per quelle più piccole, senza nemmeno parlare della questione relativa al budget. Torna quindi a farsi sentire il bisogno di razionalizzazione. Ma come razionalizzare? E con quali strumenti? Una resilienza informatica da costruire, più che mai, attorno al concetto di collaborazione tra editori.

Una collaborazione che può basarsi solo su una certa dose diumiltà, una parola chiave da condividere nella comunità informatica.

LA SFIDA DELL'INTELLIGENZA ARTIFICIALE

Lanciato alla fine del 2022, il modulo di conversazione ChatGPT ha già fatto scorrere fiumi di inchiostro. E continuerà a farlo man mano che i criminali informatici si rivolgeranno a esso. Presentato da alcuni come intelligenza artificiale e da altri come agente interattivo, ChatGPT permette soprattutto di ottenere risposte elaborate a quasi tutte le richieste e questo va riconosciuto.

Parliamo di richieste come ad esempio quella di scrivere righe di codice. **Basta per trasformare chiunque in un criminale informatico?** Forse no, perché gli script possono contenere una serie di errori e quindi essere rilevati in modo relativamente facile dalle soluzioni di protezione. Ma consentono comunque ai criminali informatici alle prime armi di familiarizzare con l'argomento e ad altri di risparmiare tempo nelle fasi di compilazione del codice. Allo stesso tempo, il modulo ChatGPT può essere utilizzato per scrivere testi accattivanti e quindi portare il phishing in una nuova era... Collegando i progressi in materia di deep fake, video, audio e persino sintesi vocale, la capacità offensiva dei criminali informatici viene rafforzata. Tanto che alcuni profetizzano l'emergere di una vera e propria intelligenza artificiale malevola, come SkyNet in Terminator.

Per gli editori, questa forma di intelligenza artificiale non è nuova; è già presente da molti anni nelle soluzioni di sicurezza informatica, ad esempio nell'analisi comportamentale. La sfida si giocherà quindi piuttosto a livello della capacità di elaborazione dei dati per identificare gli attacchi informatici. In questa guerra asimmetrica tra editori e cyber-criminali, chi riuscirà meglio a padroneggiare queste nuove tecnologie? La battaglia è in pieno svolgimento...

LA SFIDA ECOLOGICA

Il controllo dell'impronta ambientale del digitale è un argomento delicato. Nel giugno 2020, il Senato ha avvertito che il settore era la fonte del 2% dei gas serra in Francia (stimato al 4% a livello mondiale, rispetto al 2,6% dell'aviazione civile, ad esempio). Più di recente, l'agenzia francese ADEME ha dichiarato che senza un profondo cambiamento nell'uso della tecnologia digitale, questa quota potrebbe raddoppiare a livello mondiale entro il 2025. E anche se vengono regolarmente additate, le piattaforme di streaming non sono le uniche ad avere un ruolo in questo problema.

Il mondo della sicurezza informatica non è responsabile di tutto questo 2%, ma ha comunque la sua parte nell'equazione totale. A causa della proliferazione di prodotti di sicurezza informatica nelle aziende, la loro impronta di carbonio aumenta meccanicamente per via della generazione di grandi quantità di dati, archiviati e replicati in ambienti cloud remoti. E oltre a generare gas serra, sia la sicurezza informatica che l'IT consumano molta acqua. Ad esempio, i data center di Microsoft nei Paesi Bassi avrebbero consumato non meno di 84 milioni di litri di acqua nel 2022, secondo il quotidiano olandese *Noordhollands Dagblad*. Si tratta del consumo annuo di 1.750 cittadini.

Una delle grandi sfide tecnologiche del futuro sarà quindi quella di mantenere lo stesso livello di efficienza razionalizzando i prodotti di sicurezza informatica, riducendo il volume dei dati raccolti e migliorando il consumo di risorse materiali. In Francia, è stato avviato un progetto di ricerca nell'ottobre 2022 per «*valutare concretamente i vantaggi dei servizi digitali ai margini della rete*». L'obiettivo: tener conto della capacità di generazione di calore delle apparecchiature e distribuirla al meglio negli ambienti produttivi dove è necessario il fabbisogno di calore. Digitale ed ecologia, finalmente compatibili?