

RAPPORTI
IMPRESE

LO STUDIO

Cybercrime, è l'Ai la nuova frontiera

Ma è usata più dagli hacker che dalle aziende per difendersi
Report Accenture: 9 ceo su 10 temono un evento catastrofico

Giulia Cimpanelli

È un consulente che affianca gli esperti di sicurezza informatica, ma è anche un hacker in grado di sferrare attacchi devastanti in tempi record: stiamo parlando dell'intelligenza artificiale generativa, che sta cambiando in profondità anche il contesto della cybersecurity. Una tecnologia che pone nuove sfide alle aziende e a chi si occupa di sicurezza informatica: «La difficoltà di questo momento storico? La presenza di tecnologie emergenti dirompenti che rendono la partita più complessa - commenta Marco Molinaro, Security Lead Italia, Centro Europa e Grecia di Accenture -. Arrivano tecnologie che cambiano i paradigmi tra cui l'Ai generativa, la computazione quantistica, la realtà aumentata. L'Ai, per esempio, consente di sferrare attacchi devastanti in poco tempo: è in grado di chiamarti con la voce del tuo capo e chiederti di fare delle cose. Consente più facilmente di trovare delle vulnerabilità e scrivere programmi in grado di attaccare queste vulnerabilità. Oggi si ha bisogno di meno competenze per fare un attacco, non serve l'hacker guru».

Le aziende sono pronte ad affrontare tutto questo? «Esiste un divario tra la consapevolezza del fenomeno da parte degli amministratori delegati delle aziende - continua l'esperto - e la strategia che, di fatto, troppo spesso ancora non ne consegue». In effetti, secondo lo studio "Il ceo Cyber-Resilient", realizzato da Accenture basandosi su un sondaggio condotto su mille ceo di grandi organizzazioni a livello globale, quasi nove su dieci si aspettano un evento cibernetico di portata catastrofica a carico della loro società nei prossimi due anni. Nonostante ciò, il 60% dei ceo ha dichiarato che le proprie organizzazioni non incorporano la sicurezza informatica nelle strategie, nei servizi o nei prodotti aziendali fin dall'inizio e più di quattro su dieci (44%) ritiene che la sicurezza informatica richieda un intervento episodico piuttosto che un'attenzione continua.

Il più delle volte la sicurezza informatica raggiunge "i piani alti" solamente se l'azienda è vittima di un attacco rilevante che mette in crisi il business, oppure nel caso in cui normative o regolamentazioni europee o nazionali arrivano al tavolo e impongono investimenti. Solo il 15% dei ceo, infatti, ha riunioni del consiglio di amministrazione dedicate per discutere di questioni di sicurezza informatica. Oggi queste tematiche devono arrivare ai board e devono essere affare di tutti, non riguardare solamente il reparto It. Inoltre, per difendersi, è fondamentale pensare ai nuovi prodotti e servizi. La strategia che le imprese devono adottare è la prevenzione e la gestione del rischio "by design": «In passato si costruiva un bene o si erogava un servizio e poi si applicava la sicu-



rezza - spiega Molinaro -. Oggi progettualmente la sicurezza di un servizio o di un prodotto deve nascere insieme a servizio o prodotto».

La ricerca identifica anche un piccolo gruppo di ceo che eccellono nella resilienza informatica. Questo gruppo - che Accenture chiama "ceo cyber-resilienti" e rappresenta il 5% degli intervistati - utilizza una lente più ampia per valutare la sicurezza informatica in tutti gli aspetti delle loro organizzazioni. «Le aziende di questi leader - prosegue il manager - rilevano, contengono e risolvono le minacce informatiche più velocemente di altre organizzazioni. Di conseguenza, i loro costi di violazione sono considerevolmente in-

feriori e le prestazioni finanziarie significativamente migliori rispetto agli altri, ottenendo in media una crescita incrementale dei ricavi superiore del 16%, un miglioramento del 21% nella riduzione dei costi e del 19% di bilancio».

Accenture cerca di portare tutte le aziende a questo livello e lo fa con una nutrita compagine di professionisti: «In Italia ne assumiamo 3-400 all'anno e li formiamo sulle nuove tecnologie costantemente», conclude Molinaro. Nell'ambito della strategia Accenture sta per aprire un nuovo Cyber Fusion Center a Milano, per la prototipazione di tecnologie e soluzioni di cyber resilience e cyber protection.

© RIPRODUZIONE RISERVATA

SICUREZZA INFORMATICA
LA POSIZIONE DEI CEO

La situazione nel mondo

60% ceo che dichiarano che le proprie aziende non incorporano la sicurezza informatica nei servizi o nei prodotti fin dall'inizio

44% ceo che ritengono che la sicurezza informatica richieda un intervento episodico piuttosto che un'attenzione continua

15% ceo che organizzano riunioni del consiglio di amministrazione alla sicurezza informatica

La situazione in Italia

80% ceo preoccupati di non riuscire a contrastare gli attacchi informatici

62% ceo che non considerano la cybersecurity come una questione strategica

83% ceo che considerano la cybersecurity come una funzione esclusivamente tecnica

FONTE: IL CEO CYBER-RESILIENT, PANEL: 1.000 CEO DI GRANDI ORGANIZZAZIONI (FATTURATO > 1 MLD \$) IN 19 SETTORI E 15 PAESI IN NORD AMERICA, SUD AMERICA, EUROPA, ASIA-PACIFICO E MEDIO ORIENTE



ASSICURAZIONI

E sul mercato aumentano le polizze per tutelarsi

La scelta di imprese e studi professionali di ricorrere a garanzie
Il caso Revo Insurance

Sabotaggi, richieste di riscatto e blocco delle infrastrutture cruciali come quelle della sanità e della difesa. La cyber war va assumendo un peso crescente nell'ambito della più generale crescita degli attacchi informatici, che riguardano anche aziende e persone. Secondo le rilevazioni di Clusit (Associazione italiana per la sicurezza informatica), nel primo semestre di quest'anno vi è stata una crescita degli attacchi nell'ordine del 40% a raggiungere quota 132, a considerare solo quelli di particolare gravità.

È in questa cornice che va inquadrata la scelta di Revo Insurance di entrare nel mercato della cybersicurezza con la nuova polizza Revo SpecialtyXCyber Risk. Una copertura per la responsabilità civile verso terzi a tutela dell'impresa o dello studio professionale da rischi legati ad attacchi informatici. Le coperture previste dal pacchetto base consentono di tutelarsi nel caso di: violazione dei dati e della sicurezza, inosservanza della legge sulla notifica della violazione e violazione della privacy policy dalla quale derivi una violazione della legge sulla privacy, compresa la raccolta illecita non intenzionale di dati personali.

L'intermediario, attraverso la piattaforma proprietaria OverX, è in grado di gestire tutto il processo di quotazione del rischio, accettazione ed emissione. La polizza può essere arricchita da una serie di garanzie accessorie che coprono i danni diretti, come ad esempio: costi dei servizi di gestione dell'incidente, perdite da interruzione delle attività, perdite da cyber-estorsione a seguito di ransomware e danni patrimoniali da e-crime. In collaborazione con una serie di partner, la polizza offre servizi di assistenza post incidente in ambito It forensic, legale e comunicazione. Le minacce informatiche riguardano ormai tutti i settori, anche se con diversa intensità. Tornando all'ultimo report di Clusit, nel primo semestre di quest'anno il settore più colpito è stato quello delle organizzazioni governative, davanti all'industria.

L'Eiopa (Autorità di vigilanza europea del settore assicurativo) di recente ha avviato un'indagine per individuare le difficoltà di accesso delle Pmi alle coperture assicurative cyber, nella considerazione che una polizza informatica può svolgere un ruolo importante per attuare i rischi derivanti dalla digitalizzazione. - l.d.o.

© RIPRODUZIONE RISERVATA



DOMENICO D'ALFIO
Head of financial lines di Revo

FORMAZIONE FINANZIATA:
200 mln dal 2008

BENEFICIARI
AVVISO 2/22:
Lavoratori dipendenti
Lavoratori Cigs
Lavoratori beneficiari
Fondi Solidarietà Bilaterale

FORMARE PERSONE PER UN LAVORO MIGLIORE

FORMAZIENDA SOSTIENE E FINANZIA LE ATTIVITÀ FORMATIVE DELLE IMPRESE
WWW.FORMAZIENDA.COM

15°
FORMAZIENDA
FONDO AZIENDALE PER LA FORMAZIONE CONTINUA
2008 - 2023

QR CODE:

SOCIAL MEDIA:
@form_azienda
Fondo Formazienda
@fondoformazienda
FONDO FORMAZIENDA

CONFSAL
CONFERENZA NAZIONALE DEI SINDACATI

SISTEMA IMPRESA
CONFERENZA NAZIONALE DELLE ASSOCIAZIONI DI IMPRESE