Cybersecurity e Intelligenza Artificiale

1. Cyber Crime Oggi

La cybersecurity non deve più essere vista come un mero costo operativo o un adempimento normativo. È diventata un **elemento fondamentale all'interno della governance aziendale**, agendo come scudo per il brand e garantendo la sopravvivenza e la resilienza economica dell'azienda.

Il Contesto e i Numeri del Cyber Crime

Il cyber crime non è più un'attività amatoriale, ma un **business globale** stimato intorno ai $10,5 trilioni di dollari all'anno. È un mercato che ha superato quello del traffico di droga per essere più remunerativo e con minori rischi.

- **Vulnerabilità e Minacce:** Nel 2024 è stato registrato un aumento del 17% delle vulnerabilità scoperte. Quotidianamente vengono scoperte **oltre 560.000 nuove minacce malware**.
- **Aumento della Velocità di Attacco:** I tempi per un attacco ransomware importante si sono ridotti drasticamente, passando da un requisito di almeno 4 giorni (prima del 2019) a soli **48 minuti**.

La Catena di Attacco (Kill Chain) e l'Anello Debole

Il processo di attacco ransomware richiede solitamente diverse fasi: identificazione della vittima, studio, attacco tramite un vettore (come una mail di phishing con un file malevolo), infezione del sistema e successivi movimenti laterali per espandersi nella rete e raggiungere i server, prima di criptare ed esfiltrare i dati.

- **Il Ruolo dell'AI nella Velocità:** L'intelligenza artificiale ha annullato la parte manuale di questo processo. È il sistema stesso del malware, guidato dall'AI, che riconosce l'ambiente, esegue scansioni automatiche, si espande, raccoglie informazioni dai computer infettati e invia le deduzioni al server di comando e controllo (C2), consentendo attacchi rapidissimi.
- **L'Anello Debole:** L'**essere umano** rimane l'anello debole. Circa il **70% degli attacchi andati a buon fine** è dovuto al furto di credenziali, un'azione più semplice rispetto al bucare un firewall.

Tipologie di Attacco e Social Engineering Evoluto

Gli attacchi possono essere di tipo generalizzato (pesca a strascico, invio a mailing list generate da data leak), oppure altamente mirati (spear fishing).

- **Spear Phishing e Profiling:** L'AI può scansionare il dominio di un'azienda (scrapping) per identificare il tipo di business e creare attacchi di phishing specifici per gli interessi della vittima.

- **Social Engineering:** Questa tecnica mira a convincere una persona a compiere azioni che normalmente eviterebbe. Un esempio è l'attacco "Click and Fix", dove un pop-up finto spinge l'utente a contattare un falso servizio assistenza e scaricare software malevolo.
- **Deepfake e Vishing:** Si è registrato un aumento del **442% nel voice phishing** (vishing) nella prima metà del 2024 e un aumento del **3000% negli attacchi deepfake** dal 2023 al 2024.
- **La Qualità del Fishing:** Le e-mail di phishing moderne sono spesso **grammaticalmente e graficamente perfette**. Possono indurre al download di applicazioni malevole persino dagli store ufficiali (come l'Apple Store).

Misure di Difesa e Consapevolezza

È cruciale adottare l'approccio **Zero Trust** ("non fidarsi mai, verificare sempre"), obbligatorio per chi è soggetto alla normativa NIS 2.

- **Gestione delle Credenziali:** Si sconsiglia vivamente l'uso dei gestori di password integrati nei browser, poiché salvano le credenziali in locale e i codici per bucarli sono facilmente reperibili (ad esempio, su GitHub).
- **Conformità Normativa:** Entrerà in vigore il 17 gennaio 2025 il **regolamento DORA** (Digital Operational Resilience Act), che obbliga le aziende finanziarie e i loro fornitori critici a prendere coscienza del rischio cyber. Le sanzioni per i fornitori possono arrivare all'1% del fatturato medio giornaliero mondiale.
- **Sicurezza del Dominio:** Molti attacchi di phishing a nome di istituzioni (es. Comune di Milano) sono possibili a causa della **mancata configurazione adeguata** di record di sicurezza del dominio come SPF, DKIM, DMARC e HSTS.

2. AI come Moltiplicatore

L'Intelligenza Artificiale rappresenta una **sfida a doppio taglio**. Nelle mani degli attaccanti, essa agisce come un moltiplicatore, rendendo i vettori di attacco esistenti più veloci, più scalabili e difficili da ignorare.

Accessibilità e Strumenti Malevoli

L'IA ha reso il cyber crime "democratico", accessibile anche a chi non ha competenze di sviluppo. Gli aggressori non hanno preoccupazioni etiche; le IA fanno semplicemente ciò per cui sono state programmate.

- **LLM Senza Limiti (Malla):** Esistono sul mercato gli ULLM (Uncensored Large Language Models), che danno vita ai **Malla** (Malicious Large Language Model Application).
- **Linguaggio Perfetto per il Fishing:** L'IA generativa è in grado di produrre **messaggi perfetti in qualsiasi lingua**, superando le difficoltà di traduzione e aggirando i sistemi di sicurezza basati sul riconoscimento di parole chiave.
- **Strumenti per i Criminali:** Nel dark web sono disponibili modelli linguistici progettati appositamente per i criminali, privi di "guardrail" etici. Esempi sono **Worm GPT** e **Fraud GPT**. Worm GPT è stato in grado di generare script Python per rubare credenziali.

- **Servizi AaaS (AI as a Service):** Agenti AI malevoli, come Xantorox Ai (basato su Evil GPT), offrono servizi illimitati come la gestione di botnet, generazione di codice malevolo e crypter, al costo di circa $350 al mese, inclusivo di supporto 24/7. Piattaforme come Flow GPT permettono inoltre di accedere a chat modificate a cui sono stati rimossi i limiti.

Evoluzione delle Minacce

L'utilizzo dell'AI comporta un salto di qualità nelle minacce informatiche:

- **Malware Adattivo:** L'AI consente la creazione di malware che **riscrive se stesso dinamicamente** per sfuggire ai sistemi di difesa. Test hanno dimostrato che i malware scritti dai Malla non venivano riconosciuti dagli antivirus nel 90% dei casi.
- **Sfruttamento delle Vulnerabilità:** Gli LLM possono essere utilizzati per analizzare software e pagine web per identificare potenziali vulnerabilità o per suggerire modi per aggirare le difese, svolgendo il lavoro di un penetration tester.
- **Rischio Deepfake:** La clonazione vocale (vishing) può essere realizzata in pochi secondi. Il rischio deepfake ha portato a frodi milionarie, come il caso di Hong Kong dove un dipendente autorizzò trasferimenti per 25 milioni di dollari in una videoconferenza popolata interamente da colleghi deepfake.
- **Rischio RAG Injection:** Esistono migliaia di server che ospitano LLM (come Llama) non adeguatamente protetti. Un attore malevolo può accedervi e inserire codice o informazioni malevole all'interno della base di conoscenza RAG (Retrieval Augmented Generation), con il potenziale rischio di controllare agenti AI con accesso completo al sistema.

3. AI VS AI

L'Intelligenza Artificiale non deve essere temuta, ma sfruttata strategicamente per raggiungere la **resilienza**. Il 62% delle aziende ha già integrato l'AI nei propri sistemi di sicurezza.

AI come Potenziatore della Difesa

L'AI offre capacità difensive che superano le limitazioni umane:

- **Analisi dei Dati Immane:** Aziende come Microsoft hanno integrato l'AI (es. Copilot in Sentinel, il sistema SIEM). Sfruttando la telemetria (dati di utilizzo inviati dal 90% dei computer Windows), Microsoft ha potuto addestrare modelli di sicurezza su volumi di dati inimmaginabili, consentendo l'interpretazione di attività e azioni potenzialmente offensive.
- **Log Analysis:** L'AI è in grado di leggere **gigabyte e gigabyte di log** senza stancarsi, offrendo una visione più ampia e rapida rispetto a un analista umano, che ha un tempo e un'attenzione limitati.
- **UEBA e Analisi Comportamentale:** I sistemi basati sull'AI utilizzano l'UEBA (User and Entity Behavior Analytics) per un **rilevamento avanzato delle anomalie**. A differenza dei sistemi statici che analizzano le firme (IoC), l'analisi comportamentale analizza in tempo reale pattern e comportamenti anomali, prevedendo un attacco prima che l'antivirus se ne accorga.

- **Difesa Proattiva contro Minacce Avanzate:** L'analisi comportamentale è fondamentale per identificare:
    - **Minacce Zero Day:** Vulnerabilità non ancora note e non corrette.
    - **Malware Fileless:** Malware che risiede solo nella memoria volatile (RAM) e non viene notato dagli antivirus tradizionali che cercano file nell'hard disk.
- **Risposta Automatizzata:** L'AI può automatizzare la risposta agli incidenti in **tempi di secondi**. Può chiudere automaticamente le porte di un firewall o isolare una macchina infetta dalla rete per impedire l'espansione, agendo molto più velocemente di un team umano.

La Strategia di Sicurezza Olistica

Per massimizzare la difesa, le aziende dovrebbero adottare una strategia olistica basata su tre pilastri interconnessi: Persone, Processi e Tecnologia.

1. **Persone (Consapevolezza e Formazione):**
    - Gli utenti sono l'anello debole. La risposta è **formazione continua e aggiornata** sui nuovi temi e sul social engineering.
    - L'AI può supportare la formazione.
2. **Processi (Standard e Zero Trust):**
    - Avere standard e procedure chiare permette di rispondere più velocemente alle emergenze e di prevenire situazioni critiche.
    - Il rispetto delle normative (come NIS 2) obbliga l'uso del *modus operandi* Zero Trust. L'AI supporta l'aggiornamento dei processi analizzando costantemente i comportamenti degli utenti.
3. **Tecnologia (Rete di Sicurezza):**
    - Investire in sistemi di sicurezza. Esistono soluzioni **open source** (come Wazu, un SIEM professionale) che permettono di risparmiare sulle licenze e investire in un team di sicurezza interno.
    - Quando si scelgono sistemi esterni (es. LLM), è meglio optare per soluzioni **enterprise** fornite da grandi aziende che gestiscono la sicurezza in modo professionale.

Trasparenza e Resilienza

È essenziale che l'AI sia **chiara e comprensibile (trasparente)** nelle sue decisioni, altrimenti si introducono rischi, come la condivisione inconsapevole di informazioni private.

In conclusione, nel contesto attuale, non basta essere solamente resistenti: **"solo i paranoici sopravvivono"**.