PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6100 di Lunedì 15 giugno 2026

Come difendersi dagli attacchi informatici potenziati dall'IA

Gli strumenti di intelligenza artificiale rafforzano le capacità dei cybercriminali. Un memorandum dell'Information Commissioner's Office indica cinque azioni chiave per migliorare la sicurezza informatica e proteggere dati e sistemi.

Negli ultimi tempi gli applicativi di intelligenza artificiale sono stati usati dai criminali informatici in maniera sempre più incisiva, aumentando il loro potere di penetrazione nei sistemi informativi e danneggiamento o cattura di dati. Ringrazio l'information Commissioner's Office che ha messo a disposizione degli esperti di informatica un memorandum in cinque punti, su come potenziare le difese contro queste speciali tipologie di attacco.

I dati confermano come ormai i criminali informatici utilizzano sempre più spesso gli applicativi di intelligenza artificiale per sviluppare attacchi, che sono più veloci, più penetranti e più difficili da individuare. Ad esempio, questi applicativi permettono di impersonare in maniera assolutamente credibile i contatti del soggetto attaccato, e aiutano a individuare debolezze presenti nel software.

Di seguito vengono offerti cinque pratici esempi di misure difensive, che possono essere attuate in tempi e modalità relativamente rapide.

1-Cercate di costruire il profilo dell'attaccante

Uno strumento fondamentale per mettere a punto misure di difesa è la individuazione del profilo dell'attaccante, in termini di competenze e di strumenti a disposizione.

Sulla base dell'esperienze già oggi disponibili, gli attaccanti più probabili sono coloro che sfruttano applicativi di phishing, fortemente potenziati da applicativi di intelligenza artificiale. La credibilità delle immagini e della voce sono tali da ingannare anche una persona debitamente sensibilizzata.

Gli applicativi sono anche in grado di rendere più rapidi ed incisivi i tentativi di individuazione delle password, ed ecco il motivo per cui occorre sostituirle periodicamente, adottando tecniche che non permettano di ricostruire le nuove password, facendo riferimento alle precedenti.

Un altro attacco assai pericoloso riguarda il cosiddetto "avvelenamento" dei dati. In questo caso gli applicativi di intelligenza artificiale inseriscono in applicativi esistenti dei metadati, che sono difficilmente individuabili e consentono all'attaccante l'accesso al sistema informatico. Non per niente il National cybersecurity Center ha recentemente aggiornato il suo quadro di riferimento per la valutazione degli attacchi informatici, dando ampio spazio agli attacchi sviluppati con tecniche di intelligenza artificiale.

2-Verificare il livello di sicurezza di base e la stratificazione delle vostre difese

Molto spesso gli attacchi informatici vanno a buon fine, almeno dal punto di vista dell'attaccante, perché sfruttano delle debolezze della sicurezza di base del sistema attaccato. Ecco perché non è sufficiente avere dei validi sistemi di sicurezza di base, ma occorre anche introdurre dei sistemi stratificati, come ad esempio controlli multipli su un determinato messaggio, in modo da dare l'opportunità al sistema di individuare l'attacco in corso.

3-Cercate di limitare al massimo i punti di accesso al sistema

L'esperienza mostra che pochi punti di accesso ben protetti rappresentano una validissima misura di sicurezza. D'altro canto, tutti rammentiamo come l'accesso ai castelli era proprio impostato secondo questo principio: un solo accesso ben protetto rendeva assai più difficile il superamento delle difese. Si faccia particolare attenzione al fatto che l'accesso al sistema non possa avvenire tramite applicativi di intelligenza artificiale, se non sono state introdotte adeguate misure di analisi e contrasto delle procedure di accesso.

Se nelle procedure di accesso sono coinvolti soggetti terzi, occorre accertarsi che questi ultimi adottino procedure di analogo livello di sicurezza.

4-Migliorate le vostre procedure di individuazione e contrasto a possibili incidenti informatici

Occorre individuare tutta una serie di comportamenti potenzialmente anomali, come ad esempio una frequenza eccessiva di accesso ai dati, un trasferimento o spostamento di dati apparentemente non giustificato, un tempo di collegamento da parte di un soggetto terzo non coerente con le funzioni ad esso affidate.

Questo è il momento in cui gli applicativi di intelligenza artificiale possono essere un utile strumento per migliorare il livello di sicurezza informatica, segnalando per tempo situazioni anomale. Resta comunque indispensabile un costante controllo umano, per prevenire situazioni critiche.

Con l'occasione, occorre aggiornare il piano di contrasto a situazioni di emergenza, accertandosi che le simulazioni siano coerenti con l'effettiva realtà operativa.

5-Infine, proteggete in modo particolare i dati personali

I dati personali, come è evidente, meritano un'attenzione affatto particolare, in quanto sempre più spesso diventano bersaglio specifico degli attacchi informatici.

Non per nulla il GDPR richiede l'adozione di misure di sicurezza, che devono essere costantemente aggiornate, in funzione dell'evoluzione degli scenari di attacco.

Con l'occasione, appare anche evidente come sia opportuno ridurre al minimo i dati personali trattati ed archiviati, per ridurre al minimo anche i dati che potrebbero esser attaccati.

Un'appropriata educazione, regolarmente aggiornata, impartita ai soggetti coinvolti, rappresenta un prezioso strumento di sicurezza, che oltretutto ha il vantaggio di essere facilmente aggiornabile, con moduli integrativi.

Infine, non dimentichiamo che la cifratura o la pseudoanonimizzazione dei dati può ridurre in maniera significativa i danni conseguenti ad un attacco.

Nel complesso, si tratta di misure certamente già note agli esperti di sicurezza informatica, ma gli applicativi di intelligenza artificiale rappresentano una situazione, che richiede un costante aggiornamento delle difese, sia in termini di qualità, sia in termini di tempestività di intervento.

Adalberto Biasiotti

www.puntosicuro.it