CYBERSECURITY: LA NUOVA FRONTIERA DELLA PROTEZIONE DI DATI E PERSONE

Nel momento in cui i sistemi diventano sempre più intelligenti e interconnessi, cresce la loro superficie di attacco mettendo a rischio i segreti industriali, mentre i robot aziendali interagiscono sempre più a stretto contatto con gli esseri umani aumentando la possibilità di causare danni fisici agli operatori che lavorano con queste macchine

Gabriele Pagani
Consulente in Tecnologie dell'Informazione e della Comunicazione, Ingegnere dell'Informazione Junior

Internet of Things (IoT)
In italiano "Internet delle Cose", è un neologismo utilizzato per descrivere la rete di dispositivi dotati di tecnologie di identificazione, in grado di comunicare dati su sé stessi e accedere ad informazioni aggregate da parte di altri oggetti connessi. Fanno parte di questa tipologia i dispositivi collegati ad Internet quali: telecamere, macchine di stabilimenti produttivi, motori a turbina, pozzi petroliferi, dispositivi indossabili, elettrodomestici, smart TV, termostati, frigoriferi, ecc.

In questi anni l'evoluzione dei servizi IT e, non da ultima, la quarta rivoluzione industriale (Industria 4.0) hanno generato una forte interconnessione dei sistemi e alla rete Internet, originando un'enorme quantità di dati che rappresentano uno dei beni più preziosi per l'azienda. La tutela delle informazioni sensibili deve essere un obiettivo prioritario pena l'elevata probabilità di perdita o diffusione di quei dati che sono la base dell'attività produttiva e organizzativa dell'impresa: il "segreto aziendale".
L'Industry 4.0, l'Internet of Things, gli Smart Devices e il Cloud portano a migliorie e a sviluppi impensabili fino a qualche anno fa, sia in termini di costi che di velocità di realizzazione dei progetti. Una ricerca della IDC (una delle principali società in ricerche di mercato nel settore ICT e innovazione digitale) stima che solo in Italia entro il 2020 la spesa per il comparto IoT raggiungerà i 35 miliardi di dollari.
L'euforia verso queste nuove tecnologie spesso fa trascurare l'implementazione delle più elementari tecniche di sicurezza tanto da far parlare di "Insecurity by Design", ad indicare che l'insicurezza sembra quasi un principio costitutivo del progetto. Le vulnerabilità non si riferiscono solo ai singoli componenti tecnici, ma anche ai sistemi informatici di cui fanno parte, alle procedure e alle risorse umane coinvolte.
Tutto ciò che è interconnesso con il Sistema Informativo Aziendale deve essere valutato anche dal lato della sicurezza per il suo intero ciclo di vita, dalla progettazione alla dismissione. Che si tratti di computer, tablet, telecamere, smart TV, sistemi di controllo e acquisizione (SCADA), macchine a controllo numerico (CNC), mezzi di trasporto o altro. Ognuno di questi soggetti può essere veicolo di attacchi verso altri sistemi aziendali.
Dal 2016 diversi malware come Mirai, Persirai e il nuovo IoTroop (nato a fine 2017) scansionano ininterrottamente Internet alla ricerca di dispositivi da

infettare, come router e telecamere, utilizzando una lista di credenziali impostate di fabbrica, password deboli, oppure le diverse vulnerabilità presenti nei firmware (il software integrato nei chip dei dispositivi) spesso non aggiornati. Attraverso device infettati si attaccano altri obiettivi, si inviano email truffa o di spam e potenzialmente si può accedere alla rete aziendale.

Anche un vecchio sistema che alla data di progettazione sarebbe stato impensabile collegare ad Internet, oggi, grazie anche agli incentivi allo sviluppo dell'Industry 4.0, può essere accessibile dall'esterno del perimetro aziendale. Già nel 2011 Mc Afee sosteneva che sarebbero bastati 3 minuti e 3 righe di codice per alterare il funzionamento di apparati elettromeccanici. Nel 2014 Kaspersky ha dichiarato che un sistema di controllo industriale connesso a Internet ha il 100% di probabilità che già dal primo giorno venga attaccato.

Un sistema di gestione dell'aria condizionata, pubblicato su Internet, può essere utilizzato per rubare informazioni sensibili oppure per interrompere la produzione poi chiedere un riscatto per sbloccare gli apparati. Esattamente quello che è stato dimostrato nel 2016 al DEF CON di Las Vegas, quando 2 ricercatori hanno bloccato i climatizzatori della sala dove si teneva la conferenza impedendone la riaccensione.

Nel momento in cui i sistemi diventano sempre più intelligenti e interconnessi, cresce la loro superficie di attacco.

I robot aziendali comunicano con software o dispositivi esterni il cui controllo è consentito agli esseri umani tramite app per smartphone; alcuni possono addirittura essere raggiunti direttamente da Internet per il monitoraggio e la manutenzione a distanza. L'interazione sempre più a stretto contatto con gli esseri umani aumenta la possibilità di causare danni fisici agli operatori che lavorano con queste macchine, come dimostrato in uno studio in collaborazione tra il Politecnico di Milano e Trend Micro pubblicato a maggio 2017 in cui si è effettivamente alterato il funzionamento di sistemi robotici tipici del settore industriale. Si è riuscito a dimostrare nella pratica che è possibile provocare danni fisici agli operatori e il sabotaggio dei prodotti generati, poi richiedere un riscatto per rivelare in quali fasi produttive sono stati silenziosamente introdotti micro-difetti difficilmente percettibili anche dal controllo qualità.

Se questi eventi in passato sembravano accadimenti eccezionali e remoti, una ricerca della Banca d'Italia pubblicata a febbraio 2017 ha portato alla luce che il 45% delle PMI italiane dell'industria e dei servizi non finanziari con più di 20 dipendenti nel 2016 ha subito "almeno" un attacco informatico. Un'altra ricerca, questa volta di Kaspersky, pubblicata nel 2015 ha stimato il danno medio finanziario per le PMI derivato da incidenti informatici intorno ai 35.000 € all'anno. Valore che comprende principalmente i costi di data recovery, perdita di volume d'affari, tempi di inattività e danno d'immagine. Oltre a questi, oggi bisogna considerare anche le sanzioni in caso di mancato adeguamento al Regolamento Europeo sulla protezione dei dati personali, che possono raggiungere i 20 milioni di euro o il 4% del fatturato.

Mentre le macchine e i dispositivi possono essere protetti attraverso sistemi automatici di difesa, come antivirus, firewall e sistemi di prevenzione alle intrusioni (IPS), l'elemento più difficile da controllare è l'insieme di persone che utilizzano questi strumenti aziendali.

Lo smarrimento o il furto di un pc portatile o anche solo di una chiavetta USB contenente informazioni sensibili per l'azienda potrebbe seriamente danneggiare la reputazione dell'organizzazione, portare a perdite economiche o addirittura a pesanti sanzioni.

Il fattore umano resta l'anello debole nella catena della sicurezza IT. La scarsa consapevolezza induce l'utente ad avere comportamenti che agevolano le violazioni di sicurezza. Sempre più spesso la prima breccia in un sistema si ottiene semplicemente sfruttando aspetti del comportamento umano codificati e standardizzati. Tramite la tecnica del "Social Engineering" un malintenzionato può ottenere direttamente dalla vittima le informazioni necessarie a proseguire l'attacco, effettuato poi attraverso strumenti tecnologici, mediante telefono, e-mail o grazie a notizie rilasciate sui social network.

Gli attacchi con obiettivo la frode, l'estorsione, il furto d'identità o di dati sensibili si fondano sulla probabilità che l'operatore possa essere indotto a cliccare su link suggeriti in una mail, a collegare dispositivi infetti, o ad eseguire operazioni comunicate al telefono per semplice curiosità, perché convinto di poter risolvere problemi.

In questo scenario è fondamentale promuovere un programma di formazione continua del personale, a tutti i livelli aziendali, che permetta di apprendere strumenti e procedure certe a tutela delle operazioni svolte durante le attività lavorative.

Da ciò ne deriva la fondamentale importanza per l'azienda della costruzione di una buona strategia di data protection, che preveda regolari valutazioni dei rischi, al fine di conoscere e governare dettagliatamente i processi e i servizi IT erogati, non solo per adempiere ad obblighi legislativi, ma per migliorare la propria efficienza e resilienza. ■