LA CYBERSECURITY (FINALMENTE) PARTE DALLA PREVENZIONE

OGGI I PRINCIPALI INVESTIMENTI IN CYBERSECURITY SONO INDIRIZZATI PIÙ VERSO STRUMENTI DI CONTROLLO E MONITORAGGIO DELLE MINACCE, CHE DI RISPOSTA E REAZIONE. A CONFERMA DI UNA MAGGIORE CULTURA DELLE IMPRESE SUL TEMA, COME CI RACCONTA CYBER 4.0

MASSIMILIANO LUCE

Cyber 4.0 è il Centro di Competenza Nazionale ad Alta Specializzazione sulla cybersecurity promosso e cofinanziato dal Ministero delle Imprese e del Made in Italy. Il Centro è un partenariato pubblico-privato che include 47 organizzazioni, rappresentanti del mondo accademico, industriale, delle istituzioni pubbliche del contesto associativo e delle fondazioni. Cyber 4.0 nasce con l'obiettivo di supportare lo sviluppo e il rafforzamento di competenze in materia di cybersecurity nelle imprese e nella Pubblica Amministrazione, attraverso attività di formazione, awareness, advisory e consulenza, orientamento, promozione dell'innovazione e della ricerca industriale. Nello spirito di cooperazione che il Centro promuove fin dalla sua costituzione, questa intervista sulle attuali sfide della cybersecurity, a partire dal settore automotive, è frutto della composizione di contributi provenienti da soci pubblici e privati, raccolti e armonizzati attraverso la voce di Matteo Lucchetti, direttore operativo di Cyber 4.0: in particolare, Stefano Panzieri, professore associato dell'Università di Roma Tre, Alessandro Calabrese, Senior Consultant di Hermes Bay, e Massimo Centofanti, Director Cybersecurity Technology Unit di AizoOn.

Partiamo dall'ambito automotive: quali sono oggi le principali sfide e criticità in termini di cybersicurezza?

L'industria automotive ha preso coscienza solo recentemente delle tematiche di cybersecurity e dell'importanza che esse rivestono nel proprio settore. È infatti questo un settore che, negli ultimi anni, è stato interessato da numerose innovazioni: guida autonoma, veicoli elettrici, connettività. Ciò ha portato a un crescente utilizzo di tecnologie per la connettività dei veicoli, in particolare delle Electronic Control Unit (Ecu) e software embedded per il controllo dei sistemi. Attualmente si stima che i veicoli dispongano in media di più di 150 Ecu con più di 100 milioni di linee di codice. Queste tecnologie ampliano notevolmente la superficie di attacco, soprattutto per quanto riguarda i veicoli che fanno uso di tecnologie Vehicle-to-everything (V2X), ossia di condivisione di informazioni con l'ambiente circostante (infrastruttura, Cloud, altri veicoli e pedoni). I rischi che l'adozione di tali tecnologie comporta sono molteplici e coinvolgono l'intera value chain del prodotto automotive, dal fornitore esterno di servizi front-end ai sistemi del singolo veicolo. Solo per citarne alcuni: spionaggio attraverso moduli di riconoscimento vocale; controllo diretto dei sistemi di sicurezza

del veicolo (freni, motore ecc.); furto dei dati del conducente; compromissione dei sistemi di diagnostica del veicolo; accesso a funzioni di guida autonoma, motore e freni, attraverso vulnerabilità nei sensori del veicolo; Denial of Service di veicoli che dipendono dai dati provenienti da server di back-end. Uno dei primi casi di cyberattacco a veicoli risale al 2015 e ha portato al ritiro dal mercato di 1,4 milioni di Jeep Cherokee da parte di Fiat Chrysler. In questo scenario, molti passi avanti sono stati fatti sotto il profilo normativo e degli standard.
La ISO 21434 (Road Vehicle, Cybersecurity Engineering), che copre gli aspetti di cybersecurity per tutto il ciclo di vita della vettura, dalla fase di progettazione a quella di rottamazione, per tramite di uno degli enti normativi che si occupa di definire i requisiti di omologazione, è diventato normativa Unece R155, che prevede che i costruttori automobilistici rispettino e debbano farsi certificare determinati requisiti legati alla cybersecurity. Tali misure sono estese anche ai provider che forniscono, ad esempio, la centralina elettronica o i sensori radar, i quali dovranno adeguarsi affinché il veicolo venga omologato.

È possibile individuare delle nuove tendenze nelle tipologie dei cyberattacchi rivolti contro sistemi e processi industriali?
Secondo i dati di varie agenzie, anche nel 2022 il numero di attacchi verso i processi industriali sono aumentati sensibilmente (manufacturing +21%, utility +39%). Sottolineo comunque che sono stime derivanti solo dagli attacchi denunciati dalle aziende e che quindi forniscono ancora una rappresentazione molto parziale del fenomeno. Gli attacchi per larga parte sono portati ai fini di estorsione e utilizzano in numero sempre maggiore una molteplicità di canali contemporaneamente, sfruttando spesso vulnerabilità legate al fattore umano. Nella maggior parte dei casi l'attacco consiste in un ransomware che blocca le macchine chiave del processo produttivo. La situazione geopolitica attuale sta provocando un effetto più consistente, in termini di aumento del numero degli attacchi, su settori economici quali agricoltura, energia, manifattura, logistica e high-tech.

Quali strategie dovrebbe adottare un'azienda manifatturiera per proteggere efficacemente i propri sistemi e processi industriali?
Un tema di fondamentale importanza è quello della diffusione e del rafforzamento di un nucleo di competenze di base che permetta di minimizzare il rischio legato al fattore umano. Spesso il primo veicolo di ingresso ai sistemi aziendali sono proprio i dipendenti o i loro dispositivi personali collegati alla rete aziendale, come testimoniato anche da un recente studio Enisa (l'Agenzia Europea di Cybersecurity), che evidenzia come oltre l'80% degli attacchi verso

Matteo Lucchetti, direttore operativo del Competence Center Cyber 4.0

le pmi sia innescato da fenomeni di social engineering. La formazione è importante anche per le aziende che esternalizzano i propri servizi verso fornitori terzi, perché si devono comunque tenere in azienda le competenze necessarie a esprimere corretti requisiti di sicurezza e a monitorare la loro adeguata adozione ed esecuzione. Da un punto di vista tecnico e procedurale, poi, è necessario sempre e in ogni caso - indipendentemente dalla dimensione aziendale - effettuare un'accurata analisi del rischio cyber: mappare i propri asset informativi e i processi, identificare aree di potenziale vulnerabilità, valutare l'impatto delle principali minacce cyber, anche in relazione alla probabilità di accadimento, e riferirsi alle best practice di cybersecurity industriale più diffuse, come lo standard IEC 62443. Non dimentichiamo, infine, che la cybersecurity non è solo una buona architettura di rete, ma anche dispositivi di monitoraggio efficaci che possono evidenziare comportamenti malevoli e innescare per tempo delle contromisure efficaci; in tal senso, si rileva che gli investimenti maggioritari in cybersecurity siano ormai indirizzati verso strumenti di prevenzione, controllo e monitoraggio, più che di risposta e reazione.

Come cambiano tendenzialmente strategie e priorità di difesa tra una pmi manifatturiera e una grande impresa industriale?
Le pmi rappresentano il 99% delle attività economiche nel territorio dell'UE, dato che si riflette anche nel panorama nazionale. Le principali criticità sono legate ad attacchi generalmente più semplici e meno mirati di quelli che sono indirizzati alle grandi aziende, ma che trovano una maggior percentuale di successo. Questo è dovuto a diversi fattori, peculiari di un contesto di piccola impresa: scarsa consapevolezza delle misure di cybersecurity da parte dei dipendenti, carenza di budget da investire nella cybersecurity e mancanza di personale adeguatamente formato sulla protezione dei sistemi IT e OT. Sono questi i fattori sui quali si dovrebbe intervenire in priorità. Dal punto di vista tecnico, poi, le misure sono

quelle che anche le grandi aziende dovrebbero applicare. Solo per citarne alcune: segregazione delle reti e principi di minimo privilegio; security-by-design e hardening dei sistemi IoT; selezione e controllo di componenti, dispositivi, software e hardware, possibilmente in linea con standard internazionali; controllo degli accessi, fisici e logici; adozione di strumenti di monitoraggio continuo; dotazione di un piano di gestione e risposta agli incidenti e sua manutenzione, monitoraggio della supply chain e attenzione alle tecnologie non di origine nazionale.

Quali sono le caratteristiche salienti dell'offerta oggi sul mercato di prodotti e servizi per la cybersecurity dei sistemi industriali?
L'offerta di apparecchiature dedicate alla protezione dei dispositivi industriali è ancora molto potenziabile. Ad oggi sono disponibili firewall che applicano regole di numerosità e complessità crescente con il costo, ma sono ancora pochi quelli che tengono conto dei modelli matematici dei processi a cui i dispositivi industriali sono collegati, vera frontiera in questo settore. La causa di un mercato non ancora maturo è anche in una debolezza della domanda: le aziende appaiono restie a investire in oggetti che, nell'auspicio che tutto vada bene, potrebbero non entrare mai in funzione. I numeri in continuo incremento ci dicono però tutt'altro ed è importante sottolineare l'utilità di tali investimenti. Anche in questo caso, awareness, formazione ed education sono attività chiave per stimolare un mercato che necessariamente crescerà in futuro.

In che modo la cybersecurity può favorire la transizione digitale in fabbrica?
In qualsiasi ambiente, compresa la fabbrica, la transizione digitale può avvenire solo integrando tutti i presidi di cybersecurity necessari a proteggere dati e infrastrutture IT.
Manutenzione predittiva o monitoraggio energetico, capisaldi dei modelli di sviluppo industriale sostenibile, sono direttamente vulnerabili ad attacchi cyber che ne minano l'efficacia e possono produrre danni notevoli. Inoltre, i processi di monitoraggio degli impianti e dei processi producono dati che possono essere usati per molte attività contemporaneamente, non necessariamente solo cyber, e pertanto in futuro l'integrazione di questi dati nei processi informativi e di controllo della fabbrica potranno portare ulteriori - notevoli - benefici.

Come devono evolvere le competenze del personale di fabbrica per impiegare al meglio i prodotti e i servizi oggi a disposizione per la cybersecurity dei sistemi industriali?
La formazione riveste un ruolo importante a tutti i livelli: dagli utilizzatori degli impianti a chi li progetta o guida la progettazione interfacciandosi con le società di consulenza esterne. Si tratta di imparare nuovi strumenti mai utilizzati prima: anche chi fa formazione deve prepararsi a fornire le competenze giuste nella modalità più adatta. È una sfida per tutti. Le attività di upskilling e reskilling del personale, però, possono beneficiare degli incentivi previsti dal piano Formazione 4.0 promosso dal Ministero delle Imprese e del Made in Italy.

In questa direzione quali saranno gli obiettivi e il contributo del Centro di Competenza Cyber 4.0 per il 2023?
Cyber 4.0 sta sviluppando un programma molto intenso di attività per supportare il sistema delle industrie italiane, specificamente con riferimento all'ambito delle pmi.
Tale azione va sia nella direzione di sviluppare una consapevolezza diffusa dei temi di cybersecurity, anche tramite incontri sul territorio che stiamo realizzando attraverso un roadshow che toccherà tutte le Regioni italiane nel 2023, sia nell'aggregazione di community locali per la condivisione di esperienze, strumenti e procedure di risposta a eventuali criticità cyber.
È poi a disposizione un catalogo di servizi di supporto e corsi di formazione, realizzati attraverso il coinvolgimento dei nostri 47 soci, sia nel mondo accademico sia nelle grandi imprese e nelle aziende specializzate in cybersecurity.
Insieme ai Digital Innovation Hub di Confindustria e ai PID delle Camere di Commercio stiamo lavorando alla realizzazione di un approccio unificato all'assessment dei rischi cyber per le pmi, attraverso il quale costruire la lista di priorità d'azione, strumenti necessari, interventi consigliati, impatti di costo e pianificazione connessa alla realizzazione delle misure di protezione che saranno così identificate.
Stiamo poi predisponendo un laboratorio presso il nostro Centro, al quale sarà possibile accedere anche da remoto, per effettuare test di tecnologie di cybersecurity particolarmente innovative, alcune delle quali sviluppate anche attraverso i nostri progetti di ricerca. Certamente saranno incluse tecnologie OT e sistemi di controllo industriali.
Sempre in tema di progetti di ricerca, siamo in attesa della delibera del Ministero che sbloccherà risorse del PNRR per lanciare nuovi bandi proprio nel 2023, che prevediamo possano includere anche tematiche di cybersecurity industriale. Un approfondimento specifico, poi, sarà dedicato a questo tema dal nostro gruppo di lavoro di Strategic Advisory, costituito con l'obiettivo di analizzare tematiche che hanno impatto diretto sulle policy in corso di realizzazione, a livello nazionale e comunitario. Altri progetti sono infine in corso di approvazione, avremo ulteriori aggiornamenti a breve. ■