La Cybersecurity tra innovazione, mercato e normazione

A cura di UNINFO - Ente Federato all'UNI

La *Cybersecurity* è indubbiamente, ad oggi, uno degli argomenti di maggiore attualità sul mercato. Perché? I motivi sono molteplici, e si differenziano e aumentano al mutare delle tecnologie e delle pratiche informatiche utilizzate nel mondo del *business*. Cresce in maniera esponenziale dunque, la necessità di tutelare un vero e proprio *"cyber-patrimonio"* che ogni azienda possiede.

Le sfaccettature con cui si può approcciare l'argomento sono quindi varie, avendo da proteggere dati (interni e di terzi), informazioni, processi, finanze, siti, *know-how*, sistemi, strategie aziendali, e si potrebbe continuare oltre.

La *Cybersecurity*, infatti, anche come inteso da una norma-panoramica, lo *standard* ISO/IEC 27032:2012 *"Information technology - Security techniques - Guidelines for cybersecurity"*, è da intendersi come l'interazione di persone, software e servizi su internet mediante l'utilizzo di dispositivi tecnologici e connessioni di rete. E da qui è semplice intuire la multidisciplinarità del tema trattato, che potrebbe far subito pensare, a un primo approccio (che poi è l'esigenza, spesso, contingente, se non l'urgenza) all'aspetto della protezione dai rischi, ma che ha invece un più ampio risvolto una volta che si amplia il perimetro, andando a coinvolgere altri fabbisogni - come la tutela dei dati o la *privacy* - o semplicemente l'attività aziendale nel suo *day-by-day* - funzionamento della posta elettronica, accesso remoto ai sistemi, gestione del sito (o *e-commerce*), difesa dai virus informatici ecc.

Ed è proprio per cercare di mettere in evidenza le applicazioni nei diversi campi e alcuni orientamenti pratici in materia di *Cybersecurity* che UNINFO, ente di normazione tecnica operante con delega UNI a livello nazionale e internazionale in ambito ICT (dove rappresenta l'Italia presso l'ISO, l'ISO/IEC JTC 1 e il CEN, oltre a partecipare direttamente alle attività ETSI come socio effettivo) ha voluto raccogliere in un dossier esperienze diverse e fornire così un quadro il più possibile inclusivo su questo argomento. Le stesse sono poi un esempio di pluralità di interessi che sono o potrebbero essere coinvolti per accrescere la platea di competenze e professionalità che in UNINFO - e nello specifico del caso nella Commissione UNINFO UNI/CT 510 Sicurezza/*Security - Mirror Committee* di ISO/IEC JTC 1/SC 27 - partecipano per definire, sinergicamente e consensualmente, lo sviluppo degli *standard*, che includono metodi, tecniche e linee guida per affrontare i diversi aspetti della materia trattata, nel caso della *Cybersecurity*, inclusa in un ancor più vasto e aperto tema, che è, appunto, la Sicurezza Informatica.

La volontà è inoltre quella di divulgare l'utilità e la necessità della normazione tecnica che su questo *hot-topic* (come su molti altri) supporta le aziende attive sul mercato cercando, come da prassi per questo tipo di attività, di informare, formare e condividere informazioni al fine di sviluppare insieme agli *stakeholder* e agli esperti di settore - attraverso un processo *trasparente, democratico e consensuale* - le norme tecniche, e uno *stato dell'arte*, quindi, in questo caso, su *Cybersecurity*.

Obiettivo del dossier non è certamente completare o esaurire i numerosi punti di vista, le esperienze e le applicazioni della materia, naturalmente troppo ampia e in continua evoluzione, ma tracciare un percorso che inizi dal binomio *innovazione-normazione*, per estendere poi il concetto ad alcuni dei temi che, non solo in ambito normativo ma anche sul mercato e sui media, hanno catturato maggiore attenzione ed *effort* negli ultimi tempi. Abbiamo deciso quindi, con questo approccio, di stabilire un *fil-rouge*, che si concentra in principio sul Regolamento europeo n. 679/2016 (GDPR), di recente applicazione, per poi procedere passo a passo estendendo la circonferenza del discorso agli aspetti inizialmente sottolineati, quali la protezione dei dati, la sicurezza informatica *stricto sensu*, *l'internet of things*, l'intelligenza artificiale, fino a giungere al macrotema per eccellenza in termini di azienda, Industria 4.0.

Questo è dunque lo spettro su cui si sono delineati gli approfondimenti che seguiranno, con l'intenzione di fornire al lettore degli spunti informativi e dei *business case studies* che permettano da un lato di avere una visione ampia e il più possibile puntuale dello stato dell'arte regolamentare e normativo, e dall'altro capire come il mercato e alcune *industries* (molto diverse tra loro, per citarne alcune, Enel, IBM, Inail) stanno recependo e reagendo a queste novità, esigenze e necessità.

Fabrizio Spaolonzi
Responsabile Area Comunicazione UNINFO

Innovazione e normazione: un binomio che funziona anche grazie alle prassi di riferimento

Uno dei benefici della normazione volontaria è quello di "codificare" le buone pratiche, diffondere rapidamente la conoscenza e trasferire i risultati della ricerca al mercato, promuovendo in questo modo il trasferimento tecnologico.

Il processo di normazione in quanto tale inoltre, è un processo di condivisione della conoscenza e di produzione della conoscenza, perché la normazione è una piattaforma di scambio di informazioni per i diversi attori che provengono da contesti differenti e hanno capacità e conoscenze anche molto diverse tra loro, spesso complementari. Il mondo della ricerca, l'industria, la pubblica amministrazione, gli utenti e i consumatori di prodotti finali possono trovare sui tavoli della normazione tecnica un terreno su cui confrontarsi e mettere a fattor comune le migliori soluzioni. Le norme tecniche - i così detti *standard* -riflettono lo stato dell'arte "aggiornato" di una tecnologia, di un prodotto o di un servizio e questo è particolarmente importante nel campo delle tecnologie emergenti, dove conoscenze e prodotti progrediscono rapidamente e si trasformano velocemente. In questo contesto le norme sono uno strumento di grande valore per promuovere la commercializzazione di nuovi prodotti, perché contribuiscono a stabilire le "regole del gioco" per quei mercati che sviluppano prodotti e servizi che introducono nuove tecnologie, soprattutto quando si affronta il tema dell'interoperabilità.

I benefici della normazione sono stati riconosciuti dall'Unione europea già nel lontano 2008, dove nelle Conclusioni del Consiglio UE in tema di normazione e innovazione, si sottolineava come il mondo della ricerca potesse riversare i risultati delle proprie attività nelle norme o nei prodotti della normazione e nella Comunicazione COM(2015) sul mercato unico dove si citava: *"le norme sono fondamentali per l'innovazione e il progresso nel mercato unico perché aumentano la sicurezza, l'interoperabilità e la concorrenza e contribuiscono a eliminare gli ostacoli al commercio"*. Anche nel programma europeo di finanziamento della ricerca e innovazione (*Horizon 2020* e il futuro *Horizon Europe*) viene evidenziato il contributo delle norme allo stimolo della competitività dell'industria europea.

Oltre alle norme sviluppate dai tavoli tecnici di normazione nazionale, europea o internazionale, un altro prodotto della normazione nazionale particolarmente adatto a promuovere l'innovazione sono le prassi di riferimento (UNI/PdR). Istituite nel 2012 dal Consiglio Direttivo dell'UNI, le UNI/PdR sono documenti tecnici para-normativi (ovvero prodotti della normazione come indicato nel Regolamento europeo 1025/2012 relativo alle attività di normazione tecnica) che supportano il trasferimento della conoscenza e dell'innovazione. Sono elaborate rapidamente, grazie a un processo di condivisione dei contenuti ristretta a un numero limitato di esperti e sono strumenti pensati per contribuire alla preparazione di contesti di sviluppo per le future attività di normazione tecnica nazionale e internazionale. Quali documenti di applicazione volontaria e di applicazione sperimentale, sono di fatto propedeutiche a future attività di normazione e aiutano a "sondare il terreno" in nuovi settori

innovativi, promuovendone la diffusione anche grazie alla loro messa a disposizione gratuita sul sito UNI.

Ed è in questo contesto che nel settembre 2018 è stata pubblicata la Prassi di Riferimento UNI/PdR 43 "Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)". Il documento, frutto della collaborazione tra UNI, UNINFO e AIP - Associazione Informatici Professionisti, è stato elaborato dal Tavolo "Processi di gestione *privacy* in ambito digitale" ha l'obiettivo di fornire una serie di linee guida a supporto della gestione e del monitoraggio dei processi e delle attività definite dal Regolamento europeo n. 2016/679 (GPDR) in riferimento al trattamento dei dati personali in ambito ICT. Strutturata in due sezioni "Gestione e monitoraggio dei dati personali in ambito ICT" e "Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT", la prassi affronta il tema del trattamento di dati personali mediante strumenti informatici (ICT), definendo in modo oggettivo e ripetibile le azioni necessarie a un corretto trattamento dei dati personali, offrendo a titolari e responsabili del trattamento dei dati una linea guida e alle autorità di controllo un metro di giudizio, e ponendo le basi per meccanismi di certificazione come auspicati dall'art. 42 del Regolamento europeo n. 2016/679 (GPDR).

Dopo aver chiarito i concetti di diritto alla *"privacy"* e protezione dei dati personali, il documento illustra le principali novità introdotte dal GDPR, soffermandosi su quelle di maggior rilievo del "diritto all'oblio", dell'istituzione del *Data Protection Officer*, dell'introduzione della DPIA *(Data Protection Impact Assessement)* e dei nuovi concetti di *"data protection by design"* e *"data protection by default"*.

In un mondo soggetto a una rapida informatizzazione, destinatarie della UNI/PdR 43:2018 sono tutte le organizzazioni che trattano i dati con strumenti informatici, con particolare riferimento alle piccole e medie imprese, che senza dubbio necessitano di strumenti di riferimento standardizzati, in coerenza al disposto del citato art. 42 GDPR.

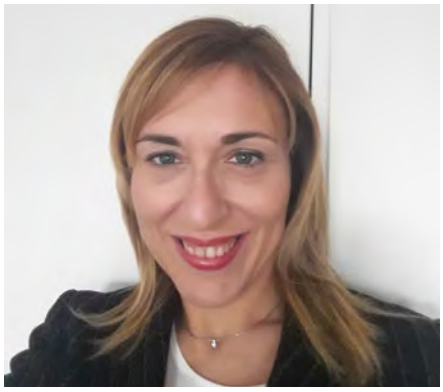
I benefici attesi dall'applicazione di questa prassi di riferimento sono:

- per i titolari dei dati: una guida che possa indirizzare le organizzazioni a gestire i dati nel rispetto del Regolamento, fornendo l'opportunità di trasmettere tale comportamento come un vantaggio competitivo;
- per i responsabili dei dati: oltre ai benefici sopra indicati per i titolari, un sistema di misurazione delle proprie *performance* e di individuazione obiettiva delle proprie responsabilità nel rapporto con i titolari;
- per le autorità di controllo: uno strumento di valutazione della diligenza di titolari e responsabili;
- per gli interessati (utenti, cittadini): una garanzia di rispetto dei propri diritti.

La parte 2 della UNI/PdR fornisce un adeguato insieme di requisiti che permette alle organizzazioni, in particolare alle PMI, di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace, potendo dimostrare tale conformità ed efficacia anche attraverso un percorso di valutazione di conformità da parte di soggetti terzi, vale a dire la certificazione.

La UNI/PdR 43 è disponibile anche in lingua inglese al fine di favorirne la massima diffusione oltre i confini nazionali.

Elena Mocchio
Responsabile Divisione Innovazione UNI



Monica Ibido
Funzionario Divisione Innovazione UNI

GDPR Data Driven Approach

L'introduzione del recente regolamento generale sulla protezione dei dati dell'UE 2016/679 (GDPR), progettato per armonizzare le leggi sulla *privacy* dei dati in tutta Europa e per rimodellare il modo in cui le organizzazioni gestiscono i dati dei cittadini europei, ripropone fortemente l'attenzione sull'importanza dei dati personali e del trattamento che subiscono. Infatti, ogni trattamento di dati personali deve avvenire in osservanza dei principi di qualità fissati all'articolo 5 (adeguatezza, esattezza, aggiornamento, sicurezza, protezione, integrità,...) seguendo il criterio di responsabilizzazione del titolare al quale è richiesto non solo il rispetto di detti principi ma anche la dimostrazione che abbia messo in campo tutte le misure a tutela degli stessi (art. 5, par. 2 e art. 24, par. 1). Il Regolamento assegna obblighi specifici in capo ai responsabili del trattamento, distinti da quelli individuati per i titolari, e in particolare l'adozione di misure tecniche e organizzative idonee a garantire la sicurezza del trattamento (art. 32) attraverso i concetti di riservatezza, integrità, disponibilità, resilienza e capacità di ripristino. Non è la prima volta che vengono introdotti dei concetti che nell'immaginario comune sono ben chiari ma che, in una visione scientifica, possono risultare ambigui a causa dell'assenza di una definizione formale e del relativo algoritmo di calcolo.

Il presente articolo propone l'utilizzo dello standard UNI CEI ISO/IEC 25012:2014 per le caratteristiche che devono assumere i dati, a partire dalla fase di progettazione *(privacy by design)* come modello di qualità dei dati, e dello *standard* UNI CEI ISO/IEC 25024:2016 per la misurazione della qualità dei dati da garantire come impostazione predefinita *(privacy by default)*.

L'adozione di un sistema di *governance* della qualità dei dati permette di rispondere alle esigenze delle organizzazioni e di far fronte alla crescente esigenza di diffusione e trasparenza delle informazioni trattate. In questa prospettiva, la valorizzazione del patrimonio informativo è un obiettivo strategico per migliorare la qualità dei servizi resi e aumentare l'efficienza della macchina organizzativa. Proteggere un'informazione vuol dire preservarne le caratteristiche di riservatezza, integrità e disponibilità. Il primo passo per garantire che un'informazione sia adeguatamente protetta è la classificazione, ovvero l'attribuzione all'informazione di un livello stabilito secondo opportuni criteri, che indirizzi l'applicazione di controlli di sicurezza commisurati a tale livello.

Oltre all'adozione di un sistema di qualità dei dati, occorre monitorare e incrementare nel tempo il livello raggiunto e verificare la robustezza del modello adottato (meta-qualità). Secondo quest'ottica è basilare confrontare le aspettative rispetto al reale grado di qualità anche attraverso la *data quality analytics visualization* (esempio: diagramma di coerenza).

L'impianto che si propone si basa su quattro fasi principali: la progettazione iniziale, l'esercizio del processo di misurazione, la valutazione dei risultati ottenuti, e una fase di individuazione di azioni di miglioramento.

Nella fase progettuale iniziale occorre scegliere il contesto di riferimento (livello concettuale, logico e fisico), definire i requisiti di qualità e il modello di qualità dei dati, valutare l'opportunità di riduzione/estensione del modello (*override/overload* delle caratteristiche e/o delle misure) e identificare le entità target nella fase opportuna del ciclo di vita del dato.

Si ritiene opportuno sottolineare che:

1. il numero di misure *(Quality Measurement Element)* non è omogeneo tra caratteristiche diverse;
2. non sono definite nella norma né criteri di aggregazione delle misure, perché dipendono essenzialmente dal contesto in cui sono applicate, né soglie preassegnate per i valori attesi.

Quindi, nella progettazione dell'impianto ciascuna organizzazione può individuare, in base alla propria realtà di interesse, una differente importanza, e quindi un differente peso, ai vari indicatori e, allo stesso modo, selezionarne un sottoinsieme oppure decidere di aggiungerne di nuove (preservando il quadro metodologico della serie SQuaRE - ISO/IEC 25000:2014).

Il processo di misurazione può avvenire attraverso *software* commerciali o, più semplicemente, costruendo un insieme di interrogazioni modulari, riutilizzabili e plasmabili su diverse realtà a seconda del modello individuato. La soluzione presenta grande portabilità grazie all'utilizzo di un *database* relazionale che contiene gli algoritmi realizzati, le misure effettuate e quelle attese. Per poter individuare eventuali *outlier* all'interno del campo dei valori o *cluster* di dati è molto importante preservare le misurazioni elementari disaggregate all'interno della banca dati.

La valutazione dei risultati deve essere svolta da un esperto che valuta il livello di qualità raggiunto alla fine di ogni iterazione e l'andamento della stessa, ai vari livelli di granularità, nel tempo, sino a considerare l'eventuale intervento di *assessment* da parte di un ente terzo.

La possibilità di avere informazioni di qualità controllata e certificata, favorisce la collaborazione fra strutture aziendali interne ed esterne, elimina le operazioni manuali (*cleaning* e *query ad hoc*), migliora i processi decisionali e abilita la cooperazione basata sui dati, migliora la qualità del servizio erogato, attenua i rischi di commettere errori, valorizza i dati e permette di conseguire l'efficienza IT, secondo un modello a ciclo continuo.

Maria Cristina Paoletti
Membro esperto UNI/CT 504 "Ingegneria del Software"
Professionista Attuario INAIL

Alessandro Simonetta
Vice Presidente UNI/CT 504 "Ingegneria del Software"
Professionista Informatico INAIL

L'intelligenza Artificiale alla prova del GDPR

Intelligenza Artificiale?

L'intelligenza Artificiale, anche se ha una storia lunga di quasi settant'anni alle spalle, solo in tempi recenti ha lasciato il territorio della ricerca accademica per trasferirsi nel mondo reale. Sistemi per la raccomandazione dei prodotti in vendita, assistenti automatici che comprendono la lingua naturale, traduttori automatici, *software* per il riconoscimento facciale sono ormai incorporati nei prodotti di largo consumo e quasi dati per scontati. Le automobili a guida autonoma sembrano ormai dietro l'angolo. Sistemi che hanno la capacità di imparare sono ormai maturi in settori come quello finanziario (per la valutazione relativa alla concessione di prestiti e mutui, ad esempio), del *marketing* (per la profilazione individuale delle abitudini di consumo), della sicurezza (studio delle anomalie comportamentali, modelli predittivi della probabilità di reati in specifiche localizzazioni).

Anche se tutte le applicazioni descritte sono efficaci, esse sono ben lontane dall'IA che la fantascienza ci ha raccontato in moltissime opere: quello che hanno in comune è la limitatezza del loro perimetro. La singolarità (la comparsa delle IA sovrumane) e anche la rivolta delle macchine senzienti può certamente attendere. La realtà per il momento è molto più prosaica e più che di Intelligenza Artificiale si dovrebbe parlare di algoritmi per l'apprendimento automatico *(machine learning)*. Questi algoritmi sono sì in grado di "imparare", ma per farlo hanno bisogno di dati, in grandi quantità.

I dati sono stati definiti, a ragione, la moneta dell'economia digitale e spesso sono appunto usati come mezzo di scambio per ottenere servizi *online* che non richiedono pagamenti in denaro, come Google Maps, Facebook e innumerevoli altri esempi.

La norma europea

Dato che in molti casi i dati in questione sono dati personali, l'uso di queste tecniche ricade in pieno nel perimetro della protezione dei dati, ora regolata in Europa dal (famigerato?) Regolamento Generale per la Protezione dei Dati (RGPD in italiano GDPR in inglese).

L'Unione affronta la regolamentazione sulla protezione dei dati personali definendola come un diritto fondamentale degli individui (assieme alla *"privacy"* o riservatezza, che costituisce un diritto fondamentale a sé stante e distinto). Il Regolamento poggia sul principio che i dati personali che ci riguardano sono sempre e comunque sotto il nostro controllo, anche se ceduti a vari soggetti per svariati motivi (in contrasto va detto con l'approccio degli Stati Uniti, dove i dati, anche personali, una volta ceduti, appartengono in toto al titolare del trattamento).

Il GDPR impone limiti in particolare alle attività di profilazione degli individui, che viene definita come una *"forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona"*.

I paletti (e le sanzioni) previsti però prevedono una ben mirata eccezione, per gli stati e le pubbliche autorità. I soggetti privati, nello sviluppo e nello sfruttamento degli algoritmi di apprendimento automatico hanno l'obbligo di conformarsi a principi e limitazioni ben precise, tenendo conto nel caso del *marketing* diretto che gli interessati possono in qualsiasi momento opporsi.

La sfida della privacy

Dato che gli algoritmi di apprendimento automatico hanno la possibilità se ben usati di generare valore non solo per le aziende, ma anche per i clienti, costruirne di conformi alla regolamentazione diventa fondamentale per intercettarne il potenziale innovativo. Fare questo richiede un cambiamento di prospettiva, anche culturale. Occorre comprendere che operare ignorando i principi della protezione dati diventa ora estremamente rischioso e che i dati personali hanno valore economico solo se acquisiti e trattati in conformità. In particolare con il consenso esplicito dell'interessato, quando necessario (principio della liceità dei trattamenti) e per finalità esplicite e chiaramente comunicate agli interessati (limitazione della finalità). Culturalmente, è necessario combattere la "astinenza da *big data*", malattia che affligge chi era abituato a conservare grandi insiemi di dati personali per finalità non ben specificate e a tempo indeterminato.

Forse la sfida più grande per gli utilizzatori degli algoritmi, soprattutto quelli predittivi che realizzano la profilazione e le decisioni automatizzate, è costituita dal "problema della scatola nera". Data la loro particolare natura, questi algoritmi imparano dai dati e operano le loro decisioni senza la possibilità per gli utenti (e per gli stessi sviluppatori) di ricostruire i singoli passaggi che hanno portato al risultato finale. Il principio di trasparenza e responsabilità *(accountability)* della disciplina sulla protezione sono difficilmente soddisfatti da modelli simili. Ripensarli in modo da essere in grado di giustificare e ricostruire le decisioni prese è al momento un ambito attivo di ricerca, e in ogni caso modificare i modelli esistenti è quasi impossibile. La sfida è quella di creare algoritmi trasparenti sin dalla progettazione, per rispettare un altro limite fondamentale posto dal GDPR, il principio della *"privacy by design"* che obbliga a rendere conformi prodotti e processi sin dalla fase di progettazione.

L'altra faccia della medaglia è ovviamente il rischio di soffocare un settore innovativo e di rendere l'Europa meno competitiva. L'approccio UE alla regolamentazione potrebbe soffocare l'innovazione, spostando gli incentivi verso la non-adozione di tecnologie innovative o l'adozione di versioni "auto-limitate" delle stesse, con effetti pesanti anche sulla competitività dell'Europa rispetto alle altre aree del mondo. L'asticella posta dal GDPR all'uso dell'IA "pratica" è veramente molto alta, a volte più alta di quella degli stessi decisori umani, che non sono tenuti a giustificare sempre il loro processo cognitivo. Se riusciremo a conciliare i due aspetti però gli Europei potrebbero sviluppare un enorme vantaggio tecnologico.

Alessandro Guarino
CEO, StAG S.r.l. e convenor del CEN/CENELEC JTC13/WG5 "Privacy and data protection"

Cybersecurity e IA, modelli e soluzioni

L'ecosistema digitale fornisce enormi opportunità e vantaggi sia per la domanda che per l'offerta. D'altra parte, l'ecosistema stesso si basa sulla fiducia tra chi fornisce il servizio e chi usa il servizio. Infatti, il consumatore potrebbe decidere di abbandonare il servizio con la stessa velocità con la quale lo ha adottato, se la fiducia dovesse venire a mancare.
Quello che leggiamo sui giornali oramai quotidianamente non aiuta certo a migliorare questa fiducia. Ragione per cui le organizzazioni sono costrette a fare continui investimenti sulla *cybersecurity*, spinti da diversi elementi.
Eccone alcuni:

- la necessità di garantire la crescita. La digitalizzazione ha generato una fortissima accelerazione in tutte le transazioni. L'adozione delle nuove tecnologie è funzionale alla esistenza della azienda o istituzione stessa. Pultroppo molte di queste tecnologie non sono state create per essere sicure. La sicurezza è qualcosa che spesso viene considerata un valore intrinseco, come l'ossigeno: cosi fondamentale che non si può prescindere dalla sua esistenza. Spesso per tutti i beni di valore intrinseco, si ha la tendenza a pensare che sarà qualcun'altro a preoccuparsi di fornire questo valore.
  Quando si pensa a un servizio, nessuno ad esempio si preoccupa dell'ossigeno consumato da coloro che forniscono il servizio. Senza ossigeno però non c'è servizio. Il paradasso è che la tendenza a pensare che qualcun'altro si preoccuperà del bene intrinseco, fa si che spesso nessuno si preoccupi del bene. Se questo però non accade, potrebbero verificarsi disastri prevedibili con conseguenze imprevedibili;
- le metoodologie di attacco sono sempre piu' complesse e sofisticate;
- la conformità all'implementazione di controlli di sicurezza *(compliance)* è sicuramente un elemento positivo perché forza l'adozione di politiche e di misure di sicurezza (è questo il concetto, giusto?). Se alla mancanza di *compliance* si associa una multa, questo diventa un problema ulteriore. I CxO devono quindi preoccuparsi di difendersi dagli *hacker*, ma anche di evitare di pagare delle multe.

In ogni caso, o per *compliance* o per genuino desiderio di evitare di essere attaccati compromettendo se stessi e i dati dei propri clienti, nel corso degli anni le organizzazioni hanno fatto importanti investimenti in *cybersecurity*, volti ad acquisire le migliori tecnologie e a intervenire sui processi.
Nella nostra esperienza abbiamo osservato fino a 85 prodotti di 45 *vendor* diversi in uso presso lo stesso cliente. Tutti prodotti che richiedono installazioni, configurazioni, personale specializzato per la gestione e manutenzione. Inoltre, tutti questi prodotti sono spesso non integrati e la mancanza di integrazione è dovuta non solo ai diversi prodotti, ma anche ai processi. Infatti è raro vedere la gestione delle configurazioni integrata con controlli di sicurezza focalizzati sulla identificazione di un cyberattacco *(detection)*.
IBM ha deciso di rispondere a questo tipo di esigenze con un *framework* che si ispira al sistema immunitario: non ci sono solo controlli raggruppati in macro-aree, ma i controlli sono integrati l'uno con l'altro intorno alla funzione focalizzata sulla *detection*. Integrazione non vuol dire solo che i controlli di sicurezza devono informare il centro del sistema immunitario e, quindi la piattaforma di *security intelligence* (che include il SIEM), ma anche che la stessa piattaforma centrale deve avere la possibilità di attivare i controlli di sicurezza, per fare ad esempio una investigazione ulteriore o per iniziare una attività.
C'è un altro elemento chiave nella strategia IBM sulla *cybersecurity*. Se da una parte la difesa si deve preoccupare di prendere in considerazione milioni di elementi, dati non strutturati, prodotti, normative, regolamentazioni, attacchi sofisticati, dall'altra i *cyber*-criminali lasciano sempre una traccia nell'ecosistema digitale. Nel mondo digitale il crimine perfetto non esiste. Ovviamente sono necessarie tecnologie particolari per riuscire a trovare le tracce lasciate dal criminale o semplicemente è necessario essere pù efficienti e veloci del *cyber*-criminale.
Questo è il motivo per cui IBM ha deciso di utilizzare *l'Artificial Intelligence* (AI) sin dal 2015 per aiutare chi lavora nella *cybersecurity* nella ricerca, analisi, comprensione di importanti moli di dati.
Seguono alcuni esempi:

Analisi dell'incidente

La correlazione di eventi con un SIEM efficiente rende spesso possibile l'identificazione di un attacco in corso. Gli *hacker* però studiano diverse vie per attaccare una vittima in funzione dei controlli di sicurezza implementati. Idealmente quanto prima le varie sequenze di attacco vengono messe in relazione, tanto prima l'attacco nella sua interezza potrebbe essere bloccato ed evitare quindi che i sistemi vengano compromessi. Il problema è che per fare questo tipo di analisi è necessario avere sotto controllo milioni di eventi, osservare una enorme quantità di informazioni strutturate e non, mentre l'attacco potrebbe cambiare forma. IBM ha investito in una soluzione *(Watson for Cybesecurity)* in grado di ingerire miliardi di record provenienti da migliaia di sorgenti diverse, strutturate e non e spesso scritte in linguaggio naturale, aggiungendo la conoscenza di *cybesecurity* necessaria per rimuovere rumore inutile e prioritarizzare le sorgenti di informazione. Infine, *Watson for Cybesecurity* migliora la sua conoscenza continuamente, senza tralasciare dettagli che potrebbero risultare fondamentali durante l'analisi.

Anomaly Detection

Spesso in *cybersecurity* la difesa deve fronteggiare attacchi non conosciuti. Modellizzare un comportamento con l'AI per identificare anomalie, risulta pertanto un approccio efficiente. Questo è possibile a vari livelli, dal traffico di rete fino all'utilizzo delle *userid*. IBM *Qradar User Behavior Analysis* è in grado ad esempio di modellizzare l'utilizzo delle *userid* e informare prontamente il SIEM.

Identificare le vulnerabilità da correggere

Risolvere le vulnerabilità è critico sia in termini di costi di sviluppo che di installazione delle *patches*, sopratutto se la vulnerabilità è molto pervasiva. Minimizzare le vulnerabilità da risolvere e focalizzarsi solo su quelle che potenzialmente possono essere utilizzate dall'*hacker* è pertanto cruciale. IBM APPSCAN usa AI per fornire informazioni su quali sono le vulnerabilità che hanno la maggiore probabilità di essere sfruttate.

Calcolare il rischio di un accesso con la biometria

In genere il rischio di un accesso si calcola in funzione di cosa l'utente sa (utenza e *password*) e su cosa l'utente ha *(token)*. La biometria è sempre più utilizzata per fornire informazioni su quello che l'utente è. Anche in questo caso, l'AI diventa imprescindibile. IBM Trusteer ha fatto grossi investimenti in quest'area ad esempio modellizzando il movimento del mouse.

Adversial AI

Non è solo la *cybersecurity* ad avere vantaggio nell'uso di AI. Negli ultimi anni abbiamo assistito a importanti progressi nello sviluppo di AI. I sistemi di AI oggi raggiungono *performance* compatibili con quelle umane su attività, cognitive come riconoscere oggetti o immagini, classificare video, convertire discorsi in testi, o tradurre in lingue differenti. Molti di questi risultati si basano su *Deep Neural Networks* (DNNs). I DNNs sono complesse machine di *machine learning* che hanno similarità con i neuroni interconnessi del cervello umano. I DNNs sono capaci di trattare *input* multidimensionali (ad esempio milioni di pixel in immagini ad alta risoluzione) rappresentando *pattern* con vari livelli di astrazione, creando relazioni tra queste rappresentazioni e concetti semantici ad alti livelli. Una proprietà intrigante del DNNs è che mentre sono altamente accurati, sono vulnerabili a cosi chiamati *"adversial examples"*. *Adversial examples* sono *input* (ad esempio immagini) che sono stati deliberatamente modificati per produrre la risposta desiderata da un *hacker* in un DNNs.

Attacchi *adversarial* rappresentano una seria minaccia allo sviluppo di sistemi di AI. Alterazioni di immagini, video, *speech* e altri dati virtualmente non identificabili come malevoli vengono utilizzati per confondere i sistemi di AI.

Tali alterazioni possono essere efficaci anche se l'attaccante non conosce l'esatta architettura del DNN o ha accesso ai suoi parametri.

Ancora più preoccupante, attacchi *adversarial* possono essere utilizzati nel mondo fisico: invece che manipolare i pixel di immagini digitali, è possibile suggestionare il riconoscimento facciale indossando occhiali specificatamente disegnati per confondere i sistemi di riconoscimento o compromettere i sistemi di guida autonoma confondendo il riconoscimento della segnaletica. Ecco perché IBM ha annunciato un *toolkit* con API che garantiscono che il processo di apprendimento dei sistemi di AI stia avvenendo in maniera consistente alle aspettative.

Gli *hackers* inoltre usano l'AI per generare *distribution list* da utilizzare in campagne di *phishing*. *Tool* di AI che imparano a fare attacchi (ie SQLi) sono già sul mercato. Ovviamente sono stati sviluppati per fini benevoli *(penetration test)* ma possono anche essere usati per fini malevoli.

Conclusione

Ci sono diverse ragioni per usare l'AI nella *cybersecurity*. Sicuramente sono tanti gli *use* che ne beneficiano ma anche gli attaccanti la usano e non si può lasciare questo vantaggio a chi attacca.

Domenico Raguseo
CTO, IBM Security, Italy, SPGI and CEE

Un approccio olistico e sostenibile alla Cyber Security nel mondo delle utilities

Una breve presentazione di Enel

Enel, società energetica multinazionale italiana, è uno dei principali operatori mondiali integrati di elettricità e gas. A fine novembre 2018, Enel opera in 35 Paesi in 5 Continenti, con una capacità di generazione installata di circa 89 GW, vendendo gas e distribuendo energia elettrica con una rete che a livello globale assomma a circa 2.2 milioni di km.

Con 73 milioni di clienti a livello mondiale, Enel ne possiede, fra gli operatori europei, la più estesa popolazione. Lavorano in Enel circa 69.000 persone che quotidianamente ispirano le proprie attività a due principi fondamentali: innovazione e sostenibilità.

La Cyber Security in Enel

La strategia dell'Enel, fortemente supportata da sempre più evoluti processi di digitalizzazione, si è sviluppata negli ultimi anni in uno scenario energetico caratterizzato sempre di più da migliaia di piccoli impianti rinnovabili interconnessi sparsi per il mondo, sale per controllarli a distanza e dati immagazzinati nel *cloud*.

Tutti questi fattori tecnologici rappresentano certamente opportunità per creare un sistema energetico sempre più resiliente, ma allo stesso tempo comportano nuovi rischi fra i quali quelli creati da possibili attacchi cibernetici.

Fra l'altro va considerato che, negli ultimi anni, tali attacchi sono cambiati radicalmente in termini di frequenza, modalità di effettuazione e tipologia di attaccanti.

Il loro numero è cresciuto in maniera esponenziale, il loro grado di sofisticazione è diventato sempre più evoluto e il livello degli attaccanti, la cui individuazione è sempre più difficile, è cresciuto fino a identificarsi, in alcuni casi, con stati nazionali.

La molteplicità e la complessità degli ambienti sui quali Enel opera (in termini di dati, persone, settori di *business*) e la crescente integrazione delle componenti tecnologiche (p.e. i sistemi *"business critical"* come gli SCADA - *Supervisory Control And Data Acquisition*, le *smart grid*, i contatori elettronici) nella vita digitale del Gruppo hanno reso necessario definire un approccio olistico alla *Cyber security*.

Tale approccio si è concretizzato in un nuovo modello di difesa cibernetica basato su una visione sistemica che copre il settore IT (*Information Technology* - dal *cloud* fino ai dispositivi mobili), l'OT (*Operational Technology* ovvero tutto ciò che riguarda il settore industriale, come, ad esempio, il telecontrollo delle centrali di produzione e distribuzione) e l'IoT (*Internet of Things*, ovvero l'estensione della comunicazione e dell'intelligenza al mondo degli oggetti).

Tale modello di difesa cibernetica è stato implementato con un percorso sviluppato negli ultimi anni e che proveremo a riassumere.

Roadmap di implementazione del modello di difesa cibernetica

Nel settembre 2016 è stata costituita una specifica unità di *Cyber Security* a livello globale il cui responsabile ricopre il ruolo di *Chief Information Security Officer* (CISO) del Gruppo, a diretto riporto del *Chief Information Officer* (CIO).

Nel corso del 2017 la struttura organizzativa si è ulteriormente rafforzata con la definizione di due nuovi ruoli aziendali: il *Cyber Security Risk Manager* e il *Cyber Security Response Manager*.

Tali nuovi ruoli aziendali garantiscono il pieno coinvolgimento delle linee di *business* nelle attività collegate alla sicurezza informatica. Si viene così a realizzare un elemento fondamentale del modello della *Cyber Security* Enel che permette di coinvolgere quotidianamente ogni singola divisione di *business* nei processi chiave di valutazione e riduzione del rischio *cyber* e nella definizione delle risposte da mettere in campo in caso di attacco e della priorità delle azioni da intraprendere.

Nello stesso anno 2017 è stato anche pubblicato il *Cyber Security Framework* di Enel, che permette di indirizzare e gestire le attività in materia di sicurezza informatica con un approccio *"Risk-based"* secondo il principio di *"Cyber Security by design"* (vedi figura 1 a pagina 25).

Tale *framework* prevede il coinvolgimento delle aree di *business* per il tramite del *Cyber Security Risk Manager*, il recepimento delle indicazioni normative, dei regolamenti e di nuove disposizioni legislative, l'utilizzo delle migliori tecnologie disponibili e l'accrescimento della consapevolezza delle persone.

I principali processi che costituiscono tale *framework* sono:

- *Cyber Security Risk Assessment* il cui obiettivo è la identificazione, la analisi e la valutazione dei rischi cyber nel Gruppo Enel.
- *Cyber Security Strategy* i cui obiettivi sono quelli di guidare la strategia di Cyber Security, di definirne obiettivi e priorità, indirizzarne le iniziative e coordinare gli investimenti dell'intero Gruppo. Assicura inoltre la definizione delle *policy* e il monitoraggio delle iniziative in corso.
- *Cyber Security Design and Implementation* che assicura la adozione dei principi e delle linee guida di *Cyber Security* all'avvio di una nuova soluzione (applicativa o infrastrutturale) e nello svolgimento dell'intero suo ciclo di vita. Fondamentale per la implementazione di una Security *"by design"*.
- *Cyber Security Risk Treatment* che punta a definire e implementare i piani di intervento per ridurre i rischi *cyber*.
- *Cyber Security Assurance* le cui finalità sono la analisi, la verifica e il test della efficacia delle misure di risposta al rischio. Individua

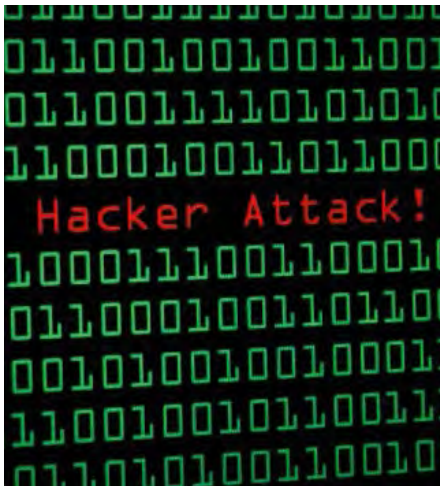


Figura 1

le vulnerabilità e valuta i controlli di sicurezza, monitorando i piani di riduzione delle vulnerabilità.

- *Cyber Emergency Readiness* che assicura il monitoraggio, la tracciatura e la reportistica della esposizione al rischio e la gestione degli incidenti di sicurezza.
- *Identity Access Management and Control* per la gestione dell'intero ciclo di vita delle identità digitali nel Gruppo Enel e per la effettuazione dei controlli di sicurezza sui privilegi di accesso.
- *Cyber Security Awareness and Training* per il coordinamento di tutte le iniziative di *awareness* e addestramento nel Gruppo Enel al fine di aumentare il livello di attenzione di tutti, lavorando sul decisivo fattore umano.

Definizione della strategia di Cyber Security e gestione del rischio.

La strategia di *Cyber Security*, in linea con quanto previsto dal *framework* appena sinteticamente descritto, viene definita sulla base di:

- un'attività di identificazione dei possibili rischi;
- un processo iterativo, condiviso e sinergico con le aree di *business*, che consolida progressivamente aspetti quali lo scenario atteso per la sicurezza informatica del Gruppo, gli obiettivi e le conseguenti iniziative.

La strategia viene approvata dal vertice di Gruppo e successivamente declinata in specifici piani di attuazione. Al fine di concretizzare tutto ciò, nel 2017 è stata anche predisposta e consolidata la nuova metodologia di *Cyber Risk Management*, applicabile sia in ambito IT sia in ambiente industriale (OT), compreso anche l'IoT.
Tale metodologia sviluppa il *Risk assessment* con un percorso che si snoda attraverso i tre seguenti passi:

- analisi degli impatti sul *business* a fronte di violazioni di confidenzialità, integrità e disponibilità delle informazioni;
- analisi delle minacce e delle loro probabilità di accadimento;
- analisi delle vulnerabilità sui diversi *layer* (tecnici, organizzativi) e dei relativi controlli esistenti.

A valle di questo percorso, il *Cyber Security Risk Manager* ottiene una valutazione del livello del rischio *cyber* della soluzione applicativa o infrastrutturale. Qualora tale livello di rischio venga considerato non accettabile, chiede al *Cyber Security Response Manager* un piano di trattamento per la sua riduzione.

Protezione dei sistemi e delle reti e Computer Emergency Readiness Team (CERT)

Le attività di analisi della sicurezza si sviluppano quotidianamente in accordo a piani definiti per massimizzare il livello di copertura dei sistemi del Gruppo.
Vengono, fra le altre, svolte attività di verifica sistematica (*"Ethical Hacking"*) del livello di protezione raggiunto da sistemi e applicazioni IT e industriali.
È stato, inoltre, avviato un progetto pilota per l'installazione di sonde per il monitoraggio, a livello mondiale, della sicurezza in ambito industriale. Le prime sonde sono state installate in Italia e le altre saranno progressivamente installate in Sud America e in Spagna nel corso del 2018.
È infine particolarmente curata l'attività di protezione dei siti web del Gruppo Enel per renderli sicuri rispetto ai tentativi di attacco.
Un fondamentale passo della strategia Enel per aumentare la capacità di prevenzione del crescente numero di attacchi *cyber* e per affrontare in modo coordinato gli incidenti di sicurezza informatica mediante una tempestiva comunicazione di informazioni e dati su minacce e vulnerabilità, è stata la costituzione, nel 2017, di un *Cyber Emergency Readiness Team* (CERT) che permette di:

- prevenire, rilevare e rispondere agli incidenti di *Cyber Security*;
- raccogliere e gestire informazioni privilegiate relative a minacce, attori e vettori di attacco;
- garantire scambi informativi e collaborazioni in un contesto "sicuro" e tra attori identificati.

Il CERT è già attivo nella comunità internazionale della *Cyber Security*, nella quale gli attori si riconoscono reciprocamente in base ad accordi ufficiali. Già nel 2017 sono stati siglati i memorandum di intesa con 6 CERT nazionali (Italia, Romania, Cile, Argentina, Perù, Colombia). Nel 2018 sono stati siglati 2 ulteriori memorandum di intesa con CERT nazionali (Spagna, Brasile) ed è stata avviata la *Global Control Room* del CERT.

Formazione e sensibilizzazione delle risorse umane

I programmi di formazione e informazione in materia di sicurezza informatica sono diventati un'iniziativa permanente all'interno del Gruppo essendo ormai da tutti riconosciuta la importanza del fattore umano sul tema della sicurezza informatica. È infatti fondamentale creare cultura, consapevolezza e competenze al fine di minimizzare il rischio di attacchi che sfruttino le vulnerabilità delle risorse umane (*"social engineering"*).

Aniello Gentile
Manager - Cyber Security - Global Digital Solutions
Enel S.p.a

La gestione della sicurezza delle informazioni. Lo standard UNI CEI EN ISO/IEC 27001:2017

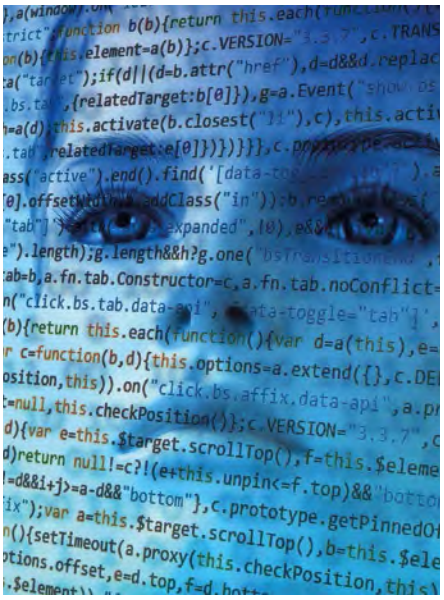
Grazie all'evoluzione tecnologica e all'introduzione del neologismo *cybersecurity*, negli ultimi anni si sente parlare maggiormente dei temi legati alla sicurezza informatica e più in generale delle informazioni. La parola *cybersecurity* tuttavia, che secondo l'Accademia della Crusca si traduce in italiano con cibersicurezza[1], è l'unione del termine cibernetico e sicurezza. La cibernetica[2] è *la disciplina che si occupa dello studio unitario dei processi riguardanti «la comunicazione e il controllo nell'animale e nella macchina»* e non si accosta proprio perfettamente agli argomenti di sicurezza cui, invece, vuole fare riferimento.

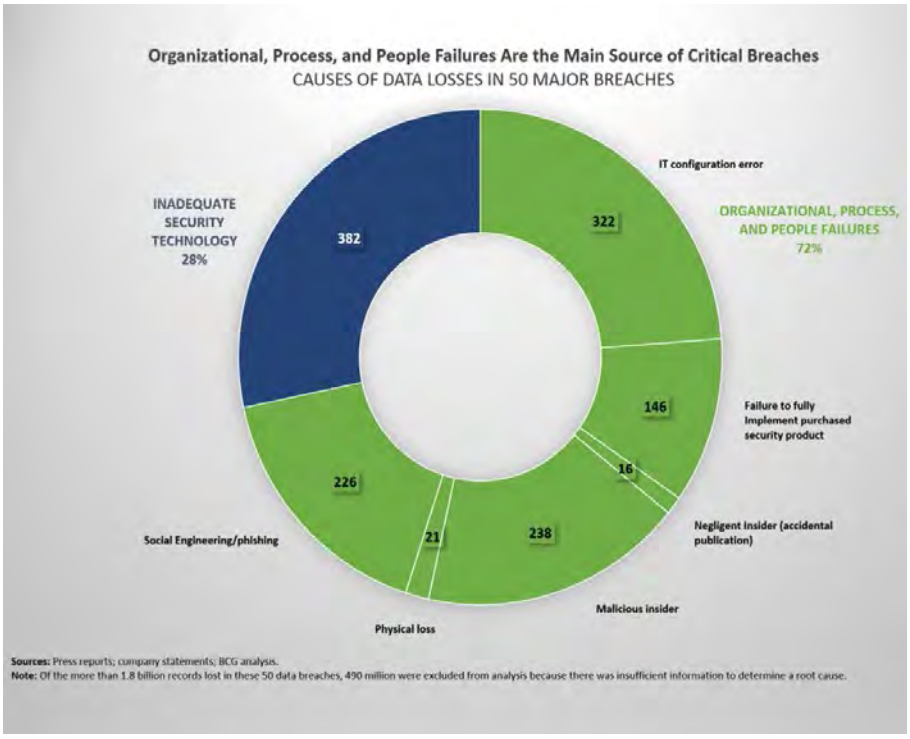
La sicurezza delle informazioni, infatti, è la pratica di impedire l'accesso, l'uso, la divulgazione, l'interruzione, la modifica, il controllo, la registrazione o la distruzione non autorizzati di informazioni. Da qui ha senso parlare di violazioni dei dati, i cosiddetti *data breach* e così via. La sicurezza informatica è solo un aspetto di un argomento, più ampio e vasto, che riguarda la protezione delle informazioni.

Lo *standard* UNI CEI EN ISO/IEC 27001:2017 definisce le linee guida per realizzare un sistema di gestione della sicurezza delle informazioni, ovvero una strategia e un insieme di processi per trattare le informazioni garantendone la riservatezza, l'integrità e la disponibilità.

Occorre, infatti, definire una politica di gestione della sicurezza che tenga conto del contesto in cui si trova a operare l'organizzazione, degli obiettivi e delle aspettative di tutti gli *stakeholder*, le cosiddette parti interessate. È intuitivo che il concetto di sicurezza delle informazioni in un'azienda che realizza automobili da corsa sia differente da quello percepito in una compagnia che fornisce energia elettrica. Nel primo caso ci sarà più interesse nel preservare la riservatezza di brevetti relativi a soluzioni tecniche innovative. Nel secondo caso, probabilmente, si darà la priorità alla disponibilità e all'integrità delle informazioni per la prevenzione e gestione di eventuali interruzioni del servizio.

È evidente che solo il *Top Management* può avere una visione complessiva sugli obiettivi legati al *business* dell'organizzazione. Per questo motivo la norma richiede il coinvolgimento dell'alta direzione





attraverso una forte *leadership* che indirizzi il livello di esposizione ai rischi e definisca i ruoli, le responsabilità e le autorità pertinenti la gestione della sicurezza delle informazioni.

La gestione dei rischi, la valutazione periodica delle minacce che potrebbero interessare l'organizzazione, mettendo a repentaglio il raggiungimento degli obiettivi di *business*, sono un altro punto cardine della norma. Ciascuna realtà aziendale è sottoposta a minacce differenti che devono orientare gli investimenti per realizzare le contromisure necessarie a contrastarle.

Gestire i rischi legati alla sicurezza delle informazioni, oltre alla scelta della soluzione tecnologica più all'avanguardia, significa anche dotarsi di personale competente che sia consapevole delle dinamiche legate alla protezione dei dati. Un dipendente che da vent'anni svolge correttamente il proprio lavoro, ma che inconsapevolmente apre un messaggio e-mail ingannevole, espone le informazioni aziendali a un potenziale rischio di furto e di danneggiamento.

Lo *standard*, quindi, indirizza la gestione delle risorse umane in termini di formazione continua e aumento della sensibilità rispetto ai temi legati alla sicurezza delle informazioni.

Tutto il sistema, i processi e le procedure, devono poi essere sottoposti ad *audit* interni, ovvero controlli periodici per verificarne un efficace funzionamento, così come devono essere periodici la gestione dei rischi e il confronto con la direzione per individuare i punti da indirizzare nell'ottica del miglioramento continuo.

L'approccio suggerito dalla UNI CEI EN ISO/IEC 27001 deve essere applicato a tutti gli aspetti della sicurezza che concorrono alla tutela delle informazioni. Devono essere quindi implementanti presidi per la sicurezza fisica, per esempio l'accesso controllato agli edifici e i sistemi antiincendio, insieme ai controlli della sicurezza logica tenendo sempre presente i rischi a cui è sottoposta l'intera organizzazione.

È importante ricordare che non è possibile garantire la sicurezza al 100%. L'approccio proposto dalla UNI CEI EN ISO/IEC 27001 è mantenere il rischio a un livello considerato accettabile per l'organizzazione, conservando la capacità di reagire a eventuali imprevisti.

La UNI CEI EN ISO/IEC 27001 promuove il concetto di resilienza dell'organizzazione nella sua completezza, non solo nei sistemi IT. Le misure di sicurezza riguardano anche l'adeguamento dei processi e la gestione delle risorse umane.

Non a caso il fattore umano continua a essere l'anello più debole della catena di gestione della sicurezza delle informazioni[3], infatti, nel 72% dei casi le cause delle violazioni più gravi sono riconducibili a problemi organizzativi, di processo ed errori umani[4]. Nessuna soluzione tecnologica potrà rappresentare un presidio sufficiente per contenere eventuali comportamenti sbagliati, indotti o volontari.

Antonio De Martino
IT Security Manager

Note

[1] https://www.lanazione.it/firenze/cultura/accademia-della crusca-1.4308000
[2] http://www.treccani.it/enciclopedia/cibernetica/
[3] https://www.schneier.com/
[4] https://www.bcg.com/publications/2017/technology-digital-building-a-cyberresilient-organization.aspx

La convergenza di IT e OT: un problema di tecnologia, cultura e competenze

La cosiddetta Trasformazione Digitale o Quarta Rivoluzione Industriale è basata sul concetto di interconnessione. Se consideriamo la definizione che ne dà l'Osservatorio Industria 4.0 del Politecnico di Milano:

"Una visione del futuro secondo cui, grazie alle tecnologie digitali, le imprese industriali e manifatturiere aumenteranno la propria produttività ed efficienza tramite l'interconnessione e la cooperazione delle proprie risorse (impianti, persone, informazioni) sia interne alla Fabbrica sia distribuite lungo la catena del valore", vediamo che l'interconnessione è l'elemento chiave per permettere la cooperazione tra risorse sia interne all'azienda che al suo esterno.

Addirittura il Piano Nazionale Industria 4.0 pone l'interconnessione come caratteristica obbligatoria per l'accesso alle agevolazioni fiscali di investimenti in *"Beni funzionali alla trasformazione tecnologica e digitale delle imprese secondo il modello «Industria 4.0»", definendo interconnessione come la "Capacità di scambiare informazioni con sistemi interni o esterni per mezzo di un collegamento basato su specifiche documentate, disponibili pubblicamente e internazionalmente riconosciute (esempi TCP-IP, HTTP, MQTT)"*.

È inoltre prevista la possibilità di accedere alle agevolazioni fiscali nel caso in cui l'ammodernamento o il *revamping* di un sistema di produzione esistente lo renda interconnesso.

Questo porta a una sempre più stretta integrazione tra sistemi IT *(Information Technology)* e sistemi OT *(Operational Technology)*.

Dal punto di vista dei sistemi di produzione questo apre una serie di scenari che devono essere analizzati e gestiti con attenzione, tenendo conto della situazione reale dei sistemi di produzione.

Innanzitutto si deve considerare che, storicamente, l'interconnessione tra macchine all'interno della fabbrica era realizzata utilizzando sistemi proprietari (tipicamente specificati e implementati dai fornitori dei dispositivi quali PLC e CNC), disaccoppiati fisicamente dalla rete tipica dei sistemi informativi *(Ethernet)* utilizzata per il collegamento dei terminali comunque presenti sullo *shop floor*. Questo, se da un lato garantiva l'inaccessibilità del macchinario da parte di soggetti esterni, dall'altro lato ha fatto sì che la *cybersecurity* non fosse uno dei requisiti prioritari di chi sviluppava i *device* di fabbrica.

Questa distinzione fra reti di fabbrica e reti aziendali ha anche portato, in molti casi, a una separazione di responsabilità e di competenze: la rete aziendale gestita dai Sistemi Informativi aziendali, la rete di fabbrica (che comprende tipicamente uno o più protocolli proprietari) tipicamente gestita dalla produzione, spesso con regole e competenze distinte, senza una figura professionale che garantisca la compatibilità delle due. Inoltre, in particolare le PMI, la sensibilità al tema *cibersecurity* è in generale bassa per i sistemi informativi ("sono un'azienda piccola, chi può avere interesse ai miei dati?"), ancora inferiore per i sistemi di fabbrica.

Sono stati condotti esperimenti che hanno dimostrato la vulnerabilità dei dispositivi di fabbrica: uno degli esempi noti è stato realizzato presso il Politecnico di Milano dove, con la collaborazione di Trend Micro, si sono potuti modificare i parametri interni di un controllo robot, in modo non immediatamente riconoscibile a un esame superficiale.

Un video che mostra tale esperimento è disponibile sul canale:
https://www.youtube.com/watch?v=BxHYtFlKruY
mentre un documento al riguardo è reperibile al link:
https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf

Un esame di altri controllori robot ha permesso di verificare la presenza di vulnerabilità simili.

Si deve poi tenere conto che la vita utile di un impianto di produzione si misura in anni e che, grazie alla flessibilità che i clienti hanno sempre più richiesto ai *system integrators*, la vita utile è andata crescendo nel tempo: è normale vedere impianti costruiti 15-20 anni fa e ancora pienamente utilizzati, grazie appunto alla flessibilità e a buoni piani di manutenzione. Questo implica che è assolutamente normale trovare sullo *shop floor* controllori basati su sistemi operativi e architetture non più supportati dal produttore e per i quali non sono disponibili i cosiddetti aggiornamenti di sicurezza.

Infine, esistono alcune differenze chiave tra i sistemi IT e i sistemi OT:

- mentre nei sistemi IT è entrato nel sentire comune l'univocità dell'utenza, con meccanismi di autenticazione, e con la proprietà da parte dell'utente di *username* e *password*, l'accesso ai sistemi OT è quasi sempre condiviso tra più persone (ad esempio personale di manutenzione su diversi turni o personale di manutenzione di diversi mestieri);
- nei sistemi IT normalmente l'utente lavora su un numero limitato di dispositivi (spesso uno, il *Personal Computer*), nel caso dei sistemi OT l'utente lavora su un parco macchine (tutte le macchine dell'azienda o di un reparto dell'azienda);
- mentre l'autenticazione sui dispositivi IT è gestita in modo centralizzato e remoto (il Dominio), nel caso dei dispositivi OT l'autenticazione è quasi sempre locale.

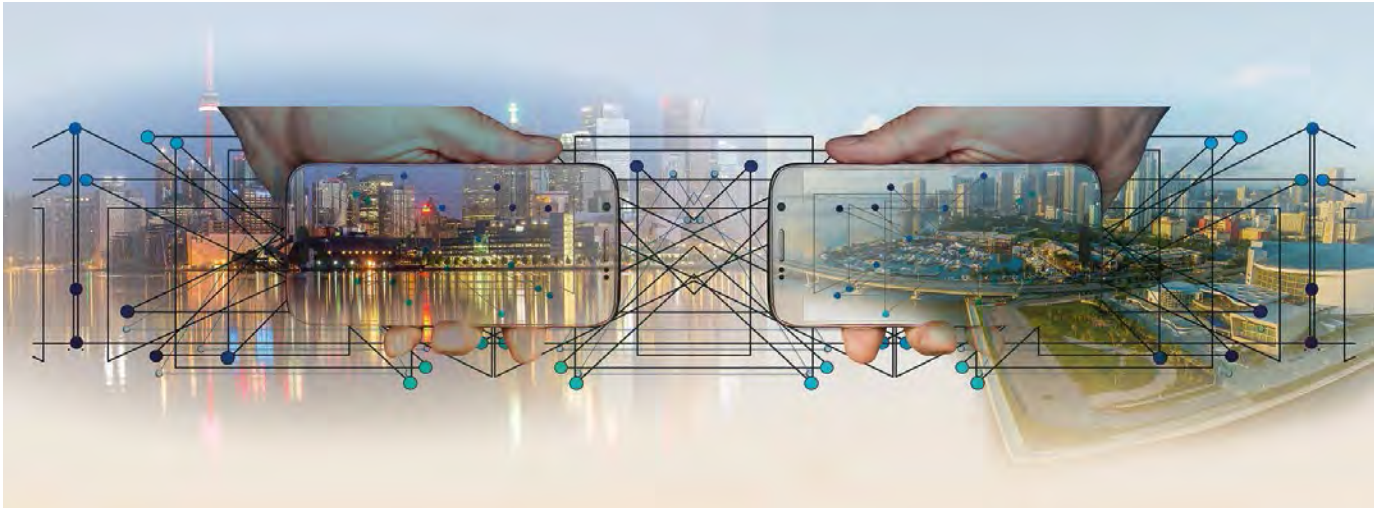
Per questi motivi il problema della gestione e dell'allineamento delle credenziali di accesso diventa problematico (non è pensabile che l'utente aggiorni individualmente le credenziali su un intero parco macchine).

Quindi oggi, per adeguarci al modello della Trasformazione Digitale, stiamo integrando tra di loro:

- sistemi potenzialmente vulnerabili;
- sistemi in cui non siamo in grado di garantire l'aggiornamento dei vari *software* (non c'è modo di verificare a priori la compatibilità delle applicazioni a una nuova versione di *software*);
- sistemi in cui non possiamo in modo strutturato garantire l'aggiornamento delle credenziali di accesso.

Per rispondere a questa sfida è necessario prima di tutto fare una grande opera di sensibilizzazione, in particolare nei confronti delle PMI. È poi necessario definire strumenti che permettano di aggirare alcuni dei problemi esposti, quali ad esempio l'autenticazione biometrica (superando i problemi di *privacy* ecc.) e creare delle figure di specialisti di rete "a tutto tondo" che siano in grado di gestire la rete, sia essa per collegare esclusivamente PC e server o integrando i dispositivi di campo.

Franco Deregibus
Responsabile Digital Innovation Hub Piemonte



Robotica collaborativa, tra safety e security

La connettività dei controllori dei robot industriali è uno dei cardini dell'adeguamento e miglioramento del macchinario nella strategia I4.0, in termini di accesso sia alla grande quantità di dati attesa dalla integrazione orizzontale e verticale con i sistemi informativi di fabbrica, che a funzionalità di interazione con l'utente.
Un fattore abilitante è l'accesso ai servizi di connessione, principalmente destinati a:

- diagnostica del controllo e dei sistemi asserviti (assi esterni, controllo di processo al *tool*, ecc.);
- configurazione dei parametri delle applicazioni (accesso ai programmi utente);
- aggiornamento del *sw* di sistema;
- servizi di comunicazione con altri nodi distribuiti, funzionali alla esecuzione delle applicazioni;
- accesso a interfacce utente o *app* in mobilità.

Per fare un esempio di servizi funzionali al controllo in linea, alcune funzioni di visione, mappatura 3D e identificazione oggetti sono spesso caratterizzate dalla necessità di elaborazione di moli di dati elevate e accesso a librerie esterne per l'estrazione di *feature*. Inoltre, l'uso di segnali da sensori per la navigazione o la prevenzione di collisioni, sia a scopi operativi che di protezione operatore/macchinario *(safety)*, prevede una connessione a bassa latenza sia cablata che *wireless* verso nodi distribuiti.
La connettività, e il conseguente aumento della superficie di attacco, implica pertanto una problematica di *security*, la cui importanza relativa è resa evidente dalla pervasività e rilevanza delle funzioni sopra elencate. L'obiettivo delle tecnologie di *security* è quello di proteggere l'integrità funzionale del sistema robotizzato rispetto ad alterazioni malevole a tutti i livelli: *software* utente, sistema operativo o strato di controllo, *firmware* degli azionamenti.

Vulnerabilità e punti di accesso

Data la finora scarsa attenzione riscontrata sul tema della *security* in robotica industriale, si registrano in generale vulnerabilità estese dal punto di vista della struttura e/o implementazione del *software* di controllo.
A ulteriore conferma, nella attuale fase di revisione delle norme tecniche sulla *safety* dei robot industriali, comprese quindi le applicazioni collaborative (famiglia ISO 10218) e di servizio (ISO 13482), sono poste a bassissima priorità le iniziative di integrazione o riferimento ai requisiti indicati nella famiglia IEC 62443. Requisiti puntuali per le suddette norme di prodotto dei robot non sono al momento prevedibili oltre a un generico richiamo alle norme valide per l'intero dominio dei sistemi di automazione.
L'origine risiede nella assente o insufficiente considerazione in sede di analisi e stima del rischio dei pericoli di natura esogena - quindi vettori di attacco sostanzialmente ignorati o derubricati - con modalità di accesso sia diretta che di rete ai sistemi di controllo. Infatti, sovente si assume che i sistemi robotizzati siano connessi soltanto a una rete isolata, il che porta a considerare le vulnerabilità nel *software* e nel *firmware* di controllo come non sufficientemente critiche.
Tuttavia, i moderni robot godono di un'ampia superficie di attacco. In primo luogo, sono connessi alla rete di fabbrica *(porta Ethernet)* e, quindi, ad altri dispositivi industriali, computer, *software* di terze parti tramite apposite API di integrazione. In secondo luogo, possono essere connessi all'esterno tramite appositi dispositivi di accesso remoto. Al di là di potenziali problemi di configurazione, questi dispositivi talvolta sono affetti da vulnerabilità di progettazione o implementazione, anche gravi, alla stregua di ben più comuni dispositivi *"internet of things"*, permettendo a un attaccante di accedere alla rete di fabbrica, che non è quindi possibile considerare isolata. Sono poi possibili anche punti di accesso legati alla semplice interazione tra dispositivi all'interno della rete di fabbrica (esempio: connessione di un dispositivo compromesso alla rete, o di un dispositivo USB infetto, con conseguente propagazione del *software* malevolo o dell'attacco) che problematiche, spesso sottovalutate o trascurate, legate all'utilizzo improprio del dispositivo robotico (esempio: modifica di parametri critici tramite la semplice interazione con il *teach pendant*).

Il ruolo della security nella robotica

L'importanza delle tecnologie di *security* è funzionale ai seguenti obiettivi di protezione:

- protezione delle persone, ovvero l'aspetto di *safety* associato alla riduzione del rischio derivante da guasto o utilizzo improprio, anche causato da un attacco informatico. Un degrado del livello di sicurezza funzionale (espresso in termini di IEC 60612 SIL o ISO 13849 PL) o una mascheratura delle funzioni di sicurezza avrebbe conseguenze gravi sui danni potenzialmente arrecabili agli operatori;
- protezione degli impianti, intesa come integrità strutturale e funzionale delle macchine e delle risorse di impianto (integrità fisica), almeno nella modalità prevista per la esecuzione delle operazioni. Tra gli effetti di una perdita di integrità fisica sono compresi anche perdite, diminuzioni o alterazioni (con difetti) di produzione, ciascuna con gravi ripercussioni economiche;
- protezione della proprietà intellettuale e dei dati in generale. Anche nel caso dell'integrità e confidenzialità dei dati, una perdita di funzione determina effetti gravi sia diretti che indiretti.

Rispetto alle funzioni di integrità o di protezione sopra elencate, la dinamica e gli effetti degli attacchi dipendono dalla architettura del controllo di un sistema robotizzato e dal componente oggetto di violazione.

Effetti degli attacchi

Dal punto di vista dell'integrità fisica, uno degli effetti di un attacco a un robot (collaborativo o non) è l'alterazione dei parametri di controllo (esempio: taratura dei regolatori, parametri di carico e inerzie, tarature o compensazioni cinematiche), con conseguente riduzione dell'accuratezza dei movimenti. Concretamente, tali parametri sono talvolta memorizzati all'interno di uno o più file di configurazione, spesso blandamente offuscati per impedirne la lettura e la modifica da parte dell'utente, ma non da parte di un avversario determinato, in caso di compromissione o accesso non autorizzato al controllore. Un altro esempio è dato dall'alterazione malevola del programma utente, con modifica del comportamento in linea.

Dal punto di vista della *safety*, le applicazioni collaborative si basano molto spesso su funzioni di sicurezza da controllo (*safety related parts of control system*, ISO 13489-1), per la implementazione dei requisiti di riduzione del rischio in varie condizioni d'uso con operatori a stretto contatto con le macchine, quali la riduzione dell'energia e della velocità nel caso di impatti accidentali, la regolazione della velocità per il mantenimento delle distanze minime nello stesso spazio condiviso, la limitazione della velocità nella guida e movimentazione manuale, ecc. (ISO/TS 15066).

Le funzioni di sicurezza si compongono di funzioni di sicurezza ai *driver*[1] per gli *output*, logica e canali di *ingresso*[2]. I livelli di alterazione delle funzioni sono due:

- modifica della configurazione della funzione e della logica, che comportano in ogni caso un accesso con credenziali, una conferma e un *cold restart*. In questo caso, un attacco ha limitate possibilità di rimanere non rilevato. In realtà, l'evoluzione verso la cosiddetta *smart safety*, di cui le preponderanti funzionalità sono realizzate dalla logica e dal *software* di sicurezza separato dallo spazio utente, e prevedono ampio uso di attivazioni condizionali, parametrizzazioni e cambi di stato. In questo scenario, si può immaginare un aumento della superficie di attacco anche per questo livello *software*.
- Configurazione di parametri *hardware*, non residenti nel *software* di sicurezza, che, influenzando il comportamento del sistema robotizzato, possono alterare o compromettere l'effetto delle funzioni di sicurezza (in funzionamento inalterato). La modifica, ad esempio, dei parametri inerziali o di carico del sistema robotizzato, determina una variazione nel calcolo della quantità di moto o della potenza o della stima della forza esercitata che sono determinanti per la reazione protettiva del robot in caso di contatto. Basterebbe rendere il robot malevolmente più leggero per assecondarne una assai maggiore velocità a parità di energia scambiata in un impatto con una persona, con effetto reale assai più pericoloso.

Inoltre, la trasmissione del dato da risorse (punti di calcolo, generazione di informazione esempio da sensori) ai fini della *safety* ha stringenti vincoli in termini di latenza, disponibilità (protezione contro le perdite di pacchetti, ecc.) e integrità del dato: qualsiasi effetto di *tampering* del dato implica l'erronea esecuzione di un calcolo critico ai fini della *safety*. Per esempio, le misure di distanza ricavate da sensore sono determinanti in funzioni di mantenimento delle distanze minime o di arresto prima di potenziali collisioni.

A livello *software*, è possibile, quand'anche deprecabile, che siano presenti delle porzioni di programma utente in grado di modificare in modo dinamico le singole funzioni di sicurezza, regolarmente configurate ma attivate in modo dinamico. Inoltre, molte funzioni legate alla *safety* dipendono dalla corretta esecuzione dei cicli di lavoro, soggetti soltanto a procedure di verifica e validazione del *software* utente. La maggiore vulnerabilità di questa porzione ha, come analizzato in precedenza, effetti potenzialmente molto gravi sulla alterazione delle condizioni di protezione *(safety)*.

Indicazioni e raccomandazioni

È auspicabile, pertanto, che l'elaborazione dei futuri *standard* considerino non solo le tematiche di segmentazione di rete, ma si occupino a tutto tondo di problemi di *security* del *software* a uso industriale, sia dal punto di vista di chi li progetta che dal punto di vista di chi li installa o esegue. La componente umana, a livello utente, può essere anch'essa un vettore di attacco - per quanto inconsapevole - da cui discende una necessità di potenziamento della sensibilità e formazione specifica sulle problematiche di *security*, nell'ottica della consapevolezza degli effetti sia di *safety* che di integrità economica dei sistemi utilizzati.

Marcello Pogliani
Dipartimento Elettronica, Informazione e Bioingegneria - Politecnico di Milano

Federico Vicentini
Coordinatore UNI/CT 24/GL09 "Robot e sistemi robotizzati"
Consiglio Nazionale delle Ricerche

Note

[1]Tipicamente, secondo EN IEC 61800-5-2, Safe Limited Speed Safe Stop 2 (SS2), Safe Brake Control (SBC), Safely-Limited Speed (SLS), Safely-Limited Position (SLP).
[2]Con varie architetture, ad esempio ISO 13849-1 cat. 2 o 3, a prescindere dal tipo di sorgente collegato, variabile da ingresso di tipo safeIO o connessioni di rete, come introdotto in precedenza.

È necessario normare le misure di sicurezza per i device IoT?

Il 20 settembre del 2016 il sito web del giornalista Brian Krebs[1], giornalista specializzato in inchieste sul *cybercrime*, è stato colpito dal più grosso attacco di *Denial of Service* visto fino ad allora, con un traffico aggregato che è arrivato fino a 640GBps, rendendolo di fatto inaccessibile il *blog*. L'attacco sembra fosse una ritorsione da parte di alcuni cybercriminali ai quali Krebs aveva dato fastidio in una delle sue inchieste.

Questo episodio, che è stato addirittura analizzato da ENISA in una nota informativa[2], ha fatto scalpore per diversi motivi: oltre a essere così massiccio, ha mostrato la "potenza di fuoco" che un'organizzazione criminale poteva mettere in gioco in un proprio attacco.

Ma quell'episodio è rimasto nella storia della *cybersecurity* soprattutto per un'altra ragione: l'attacco è stato effettuato grazie a più di 100.000 dispositivi, principalmente videocamere connesse a Internet, che i criminali avevano compromesso e che hanno iniziato a mandare traffico via Internet al sito web che ospita il blog del giornalista. Dispositivi in buona parte destinati alla videosorveglianza, quindi alla sicurezza, di marche e modelli diversi, erano tutti stati compromessi attraverso lo stesso *malware* specializzato, perché tutti presentavano le stesse vulnerabilità, e questo perché tutti questi dispositivi erano basati, alla fine, sugli stessi componenti, realizzati da un unico produttore cinese.

Questo episodio mette in evidenza una delle più importanti vulnerabilità di Internet e dei sistemi e servizi che la utilizzano: l'insicurezza diffusa dell'Internet delle cose (*Internet of things*, IoT). Il problema si riassume abbastanza facilmente: i tanti dispositivi "connessi" che ormai cominciano ad affollare le nostre case, aziende e infrastrutture, sono tutti basati sugli stessi componenti, realizzati in milioni di esemplari da pochi produttori. Questi componenti sono realizzati secondo logiche principalmente di economicità, perché questa è la loro forza: è proprio grazie a questa infatti che per pochi euro possiamo avere la videocamera connessa, la tv connessa, la presa connessa e così via. L'intera Internet delle cose si basa sulla disponibilità a bassissimo prezzo di funzionalità di base per la connettività e la programmazione. Ma naturalmente, dove guida l'economicità ne risentono altri fattori, e fra questi sicuramente la sicurezza. Nessuno di noi infatti, quando compra un *set-top-box* per connettere la tv a Internet, o un frigorifero

"intelligente", si chiede se è sicuro; casomai si assicura che non si guasti subito, o che abbia tante funzionalità, o che sia veloce e comodo nell'utilizzo. I produttori non si sentono quindi minimamente sotto pressione per produrre componenti sicuri, cosa che richiederebbe ulteriore progettazione, test e soprattutto sottrarrebbe alle altre funzionalità un po' delle poche risorse di memoria e calcolo disponibili in questi strumenti.

A questo problema si aggiunge quello dell'aggiornamento: quando viene scoperta una vulnerabilità nel *software* o nel *firmware* di questi componenti, generalmente non è chiaro chi e come li potrebbe aggiornare. Del resto, se magari ci poniamo il problema di aggiornare il nostro pc o *smartphone*, o anche eventualmente il nostro *router* ADSL o il *set-top-box* per la televisione, certamente non ci passa per la testa di aggiornare un termostato intelligente. Anche decidessimo di farlo, non sapremmo come, e anche se il menu di configurazione del dispositivo prevedesse una funzionalità "aggiornamento", scopriremmo che di solito è del tutto inutile, perché non c'è un aggiornamento disponibile, né un sito da cui scaricarlo. Dispositivi con vulnerabilità note e sfruttabili, rimangono quindi nelle nostre case e aziende per anni, alla mercé di chi ne voglia assumere il controllo.

Quello che è peggio, quegli stessi componenti, così comodi ed economici, vengono utilizzati in tanti altri sistemi: apparati elettromedicali, apparati di rete e sistemi di controllo industriali, automobili. Anche qui, la disponibilità di componenti tutto sommato testati, ben conosciuti ed economici, spesso prevale sull'esigenza di una sicurezza di cui spesso non è percepita la necessità.

Per le aziende, e in particolare per quelle che gestiscono infrastrutture critiche, tutto questo si inquadra nel tema più ampio della sicurezza della *supply chain*, dove oltre all'insicurezza dovuta alla poca cura nella produzione di questi componenti, si può aggiungere l'insicurezza dovuta ad azioni ostili di aziende vicine al proprio governo, in un'ottica di conflitto fra potenze che sta coinvolgendo sempre di più il cyberspazio[3]. È di questi giorni la notizia che il Governo degli Stati Uniti, dopo aver vietato l'utilizzo del *software* Kasperski sui sistemi governativi[4] perché troppo vicino al governo russo, sta chiedendo ai propri alleati di non utilizzare apparati di rete Huawei[5] perché l'azienda sarebbe troppo vicina al governo cinese (il che corrisponde in pratica a suggerire di utilizzare apparati di produzione americana).

Limitandoci al tema dell'insicurezza dell'IoT, cosa si può fare per mitigare i rischi di questi componenti? Sicuramente è necessario che fin dalla progettazione degli apparati si ragioni in termini di *privacy* e sicurezza *by design* e quindi anche tenendo conto delle caratteristiche delle singole componenti.

Tuttavia, a livello di singolo cittadino, azienda o anche Paese, probabilmente i limiti saranno comunque notevoli.

La radice del problema sta infatti nella qualità e nella gestione di componenti prodotti in centinaia di milioni di esemplari, e che tutti utilizzano e per i quali ci sono poche alternative, realizzati da aziende che, oltre ad essere un anello molto lontano nella *supply chain*, non sono sicuramente facili da mettere sotto pressione.

Al momento, l'unica strada sembra essere quella di intervenire a livello europeo: normative che abbiano efficacia sull'intero mercato europeo possono avere un impatto tale da essere considerate anche da queste aziende. La Commissione europea si sta muovendo proprio in questa direzione: nel contesto di una serie di iniziative volte a migliorare la sicurezza del cyberspazio dell'Unione, sta predisponendo un regolamento che prevederebbe una certificazione di sicurezza per i prodotti da utilizzare in Europa[6]. Il tema della certificazione di sicurezza per i prodotti non è né nuova né semplice, e i tentativi precedenti di svilupparne, in Europa ma anche negli USA, hanno avuto poco successo. Nel caso dei dispositivi IoT però, sembra al momento l'unica percorribile.

Gabriele Faggioli
Presidente Clusit

Alessio Pennasilico
Presidente Associazione Informatici Professionisti

Claudio Telmon
Comitato Tecnico Scientifico Clusit

Note

[1] https://krebsonsecurity.com/
[2] https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices
[3] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks-back-on-the-agenda
[4] https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4
[5] https://www.corrierecomunicazioni.it/telco/pressing-usa-sugli-alleati-boicottate-huawei-la-replica-richiesta-sorprendente/
[6] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework