Agenda Digitale.eu

Cyber security, Confindustria: “Quale strategia Paese per proteggere le aziende”

La materia della sicurezza digitale richiede un impegno globale e soluzioni sovranazionali e bisogna superare la logica dei sistemi “stand alone”. E’ l’intero ecosistema che dev’essere reso sicuro: tecnologie, macchine e persone. Ecco quindi come Confindustria sta affrontando la questione cyber security

7 ore fa

Alberto Tripi

Delegato Confindustria per la Cybersecurity e Presidente Almaviva

Se tutti i settori produttivi si servono di Internet per le attività in ambito Industria 4.0, la digitalizzazione costituisce il volano essenziale per la modernizzazione e l’efficientamento delle PA centrali e periferiche. Diventano allora fondamentali, da un

lato, i requisiti di affidabilità e di *continuity* che le nuove tecnologie devono garantire a livello fisico e a livello logico, e, dall'altro l'attenzione degli operatori e quella del legislatore ai temi della *privacy* e della *security*.

Confindustria sta affrontando il fenomeno della *cyber security* mettendo sullo stesso piano le azioni legate alla sicurezza dei dispositivi tecnologici e delle infrastrutture critiche, alle attività volte alla formazione e alla riqualificazione del personale, considerando la preparazione delle risorse umane il vincolo propedeutico ad una efficace strategia per la sicurezza informatica nelle aziende.

Promuovere l'industria italiana della cyber security

In Europa, la tutela dei dati personali è stata oggetto di una importante evoluzione normativa attraverso il *General Data Protection Regulation* (**GDPR**) che definisce un quadro regolatorio in linea con l'evoluzione tecnologica. Ma allo stesso tempo anche **la materia della sicurezza digitale richiede un impegno globale e soluzioni sovranazionali.** Ogni futura attività in materia di *cyberdefense*, di strategie nazionali, di certificazioni ed etichettature di processi e prodotti, di definizione di *standard* e soluzioni per l'interoperabilità, deve essere **coerente con l'attuale ecosistema internazionale e fondarsi sulla reciproca collaborazione tra Paesi e istituzioni interessate.** In tale quadro, è necessario promuovere la crescita di un'industria italiana della *cybersecurity* partendo dagli *asset* già disponibili, valorizzandoli e mettendoli a sistema, modellando il complesso delle regole per favorire uno sviluppo coordinato dell'intera filiera.

I livelli su cui lavorare sono molteplici ma tra loro fortemente interdipendenti: da una parte il quadro normativo, gli *standard* di interoperabilità, il processo di conformità e di *labeling* per le soluzioni *HW* e *SW*, dall'altra la conoscenza, lo sviluppo delle competenze e la formazione. In particolare, **la domanda di nuove professionalità in ambito digitale sta crescendo a fronte di un mercato del lavoro non ancora in grado di proporre adeguate competenze ad elevata qualifica professionale, dotate di flessibilità e capacità di adattamento a mansioni non routinarie.**

La protezione dei sistemi, delle infrastrutture "*digital based*" e dei dati trattati, scambiati e conservati è una sfida prioritaria da affrontare per assicurare al Paese sicurezza e crescita.

Il numero di attacchi mirati contro i "settori critici" si è quasi quintuplicato nel corso degli ultimi cinque anni, un *trend* che sta mettendo seriamente a rischio la sicurezza a livello nazionale e globale.

La cyberguerra delle nazioni

Autori di questi attacchi non solo singoli individui o piccole comunità di *hacker* ma anche vere e proprie organizzazioni statali: **ad oggi si stimano in più di 100 le nazioni**

con capacità di compromettere e danneggiare infrastrutture critiche e servizi essenziali attraverso attacchi cibernetici di alto impatto, come i recenti WannaCry e NotPetya, in grado di causare miliardi di dollari di danni.

Il Rapporto Clusit 2018 ha quantificato in 500 miliardi di euro il costo causato dai vari attacchi informatici avvenuti, a livello globale, nel corso del 2017. Nel computo totale, truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari.

Nello stesso studio è stimato che l'Italia nel solo 2016 abbia subito danni derivanti da attività di *cyber crimine* per quasi 10 miliardi di euro.

Sempre il 2017 ha fatto registrare, secondo il Clusit, **un forte aumento degli attacchi compiuti con finalità di *Information Warfare*, gestione e uso delle informazioni per scopi militari,** con un preoccupante +24% rispetto al 2016; ed ancora il *Cyber Espionage* (lo spionaggio con finalità geopolitiche o di tipo industriale, tra cui il furto di proprietà intellettuale) cresce del 46% rispetto al precedente anno di rilevazione (2016) e nei soli Stati Uniti ha causato danni dell'ordine di 600 miliardi di dollari.

Come possiamo facilmente constatare, l'uso delle tecnologie digitali nell'economia mondiale è sempre più intenso, pervasivo e abilitante a tutte le attività istituzionali ed economiche di governi, aziende e cittadini. Oltre il 95 per cento delle imprese dei paesi OCSE è connesso a Internet, di cui più dell'80% con un sito web; più di metà della popolazione adulta aveva acquistato online almeno un prodotto nel corso del 2017 (dati 2017 OCSE, *Digital Economy Outlook*).

Colmare il gap digitale del Paese

Anche in Italia il mercato ICT dimostra un rinnovato dinamismo e si rafforzano i segnali positivi sulla digitalizzazione del Paese. Nel 2017, secondo l'ultimo Rapporto "**Il Digitale in Italia 2018**" di Anitec-Assinform e Confindustria Digitale, in Italia si è registrata una crescita del 2,3% a 68.722 ML€ che lascia intravedere ancora un progresso per i prossimi anni: 2,6% per il 2018, 2,8% per il 2019, 3,1% per il 2020 a 74.523 ML€.

Il trend discendente degli anni più bui della crisi sembra cambiare di segno sull'onda delle componenti più legate all'innovazione. Ma non ci si può fermare. **Il *gap* digitale accumulato in passato obbliga a un passo ancora più sostenuto, centrato sull'accelerazione delle politiche per l'innovazione già avviate, per l'ammodernamento della Pubblica Amministrazione, l'inclusione digitale delle piccole imprese e dei territori, lo sviluppo diffuso delle competenze che hanno una notevole importanza sui temi della sicurezza informatica.**

Italia sotto attacco ransomware

Siamo il primo Paese in Europa e il decimo nel mondo più colpito dai *ransomware*, ossia gli attacchi che si configurano come estorsioni informatiche, che bloccano l'attività di un *computer* o di un qualsiasi oggetto connesso a fronte della richiesta di un riscatto economico per la sua "liberazione" (Fonte: Trend Micro "*Unseen threats, imminent losses*", 2018).

Nel 2017 uno degli sviluppi più importanti nel panorama degli attacchi informatici è stata proprio l'evoluzione del *ransomware*, con l'avvento di "*worm ransomware*" basati sulle reti che rendono superflua la presenza dell'elemento umano per lanciare le campagne di attacco. Inoltre, alcuni criminali informatici che utilizzano questa tipologia di attacco non ambiscono più al solo riscatto ma, purtroppo, puntano alla distruzione di dati, sistemi e strutture informatiche. Questa attività è ad oggi registrata in forte aumento (Fonte: Report annuale di Cisco sulla *cybersecurity* 2018).

Entrando nel dettaglio della situazione italiana, il nostro è il Paese più colpito in Europa, con il 12,94% dei *ransomware* di tutto il continente intercettati. Il numero totale di *malware* intercettati in Italia nella prima metà del 2018 è di 15.861.878, in diminuzione rispetto ai 19.014.693 dello stesso periodo del 2017. Le minacce arrivate via *mail* sono state 323.341.302 e il numero di "app" maligne scaricate nella prima metà del 2018 è di 10.662. Nella prima metà del 2018 sono stati 1.901 i *malware* di *online banking* che hanno colpito l'Italia, in crescita rispetto ai 1.525 del primo semestre 2017. I *malware* per Pos intercettati, sono stati invece 17. Gli *Exploit Kit*rilevati sono stati 1.351.

Particolare importanza, anche ai fini della *cybersecurity*, assumono (ed assumeranno in misura crescente) i cosiddetti *Digital Enabler* che, per la loro articolazione, si distribuiscono in vario modo nei comparti applicativi ma meritano evidenza specifica per la loro consistenza e dinamica.

La sicurezza informatica è chiamata quindi ad un deciso cambio di paradigma per affrontare una sfida che si configura a livello globale: **bisogna superare la logica dei sistemi "*stand alone*" da mettere in sicurezza, è l'intero ecosistema che dev'essere reso sicuro: tecnologie, macchine e persone.**

Il ruolo di Confindustria

Confindustria sta affrontando il fenomeno della *cybersecurity* mettendo sullo stesso piano le azioni legate alla sicurezza dei dispositivi tecnologici e delle infrastrutture critiche, alle attività volte alla formazione e alla riqualificazione del personale, considerando la preparazione delle risorse umane il vincolo propedeutico ad una efficace strategia per la sicurezza informatica nelle aziende.

Nel corso del 2017 è stato istituito a livello Confederale un Gruppo di Lavoro specifico sulla *Cybersecurity* con lo scopo di definire azioni e strategie per la sicurezza informatica delle imprese, in coordinamento con le istituzioni, sia italiane che europee.

Nel dettaglio il Gruppo di lavoro ha una duplice finalità:

- **accompagnare il percorso di digitalizzazione delle imprese**, velocizzato e sospinto dall'entrata a regime del Piano Industria 4.0, con azioni di sensibilizzazione sul tema della sicurezza informatica e sulle misure necessarie da adottare tempestivamente per tutelare il proprio business;
- **alimentare il dialogo con le istituzioni**, in Italia e in Europa, per favorire la definizione di una politica di *cybersecurity* efficace, in grado di consolidare la collaborazione tra imprese, centri di ricerca, accademia e istituzioni, private e pubbliche, per sostenere e agevolare la cooperazione tra gli Stati membri.

Attraverso la delegazione confindustriale di Bruxelles, viene sostenuta l'iniziativa dell'UE di rivedere la Strategia Comunitaria in materia di cybersicurezza (*Cybersecurity act*), rafforzare il mandato di ENISA (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione) e di favorire la creazione di un sistema di riferimento condiviso per la sicurezza delle tecnologie digitali nell'UE.

Confindustria condivide l'iniziativa della Commissione di definire un quadro europeo per la certificazione della *Cybersecurity* che possa sostituirsi ai diversi schemi di certificazione nazionali e garantire armonizzazione a livello europeo. Assicurando, nella definizione dei criteri, uno stretto dialogo con gli *stakeholder*, ed il ruolo delle collaborazioni pubblico-privato, fondamentali per coordinare le risorse per la sicurezza delle reti in Europa, assieme alla loro *governance*.

Sul piano nazionale, lavoriamo per consolidare il ruolo di Confindustria a supporto delle imprese nel percorso di digitalizzazione, affiancando il Sistema associativo nelle attività di sensibilizzazione e formazione dei propri aderenti sul tema della sicurezza cibernetica. In particolare, attraverso la rete dei *Digital Innovation Hub*, la costituzione di un *Competence Center* nazionale sulla *Cybersecurity*, la progettazione di una piattaforma nazionale aperta per rendere accessibili alle imprese, anche a micro e piccole, strumenti e soluzioni avanzate per la messa in sicurezza dei sistemi informatici a tutela del proprio business.

In questo ambito si inserisce la stipula del protocollo d'intesa tra Confindustria e l'Agenzia per l'Italia Digitale (**Agid**) con la finalità di incentivare la diffusione della cultura digitale sul territorio connessa alla promozione di una strutturata attenzione ai temi della sicurezza informatica.

Sono gli elementi di una necessaria e strategica azione-Paese, ben sapendo che norme e linee guida, soluzioni e buone pratiche rilevanti per la *Cybersecurity* vanno sviluppate, riconosciute e collocate in una dimensione globale, per contribuire alla costruzione di un futuro digitale e sostenibile.