Cybersecurity per gli asset aziendali: gli strumenti a tutela delle imprese

Andrea Sammarco Vice Segretario Generale Unioncamere
Paolo Atzeni Agenzia per la Cybersicurezza nazionale
Fabio Martinelli CNR Istituto di Informatica e Telematica
Leonardo Querzoni Presidente Competence center Cyber 4.0
Antonio Tonini Direttore Mercato Camere di Commercio InfoCamere
Moderatore Antonio Romeo Direttore Dintec

Cyber Security con un Focus sulle imprese. Il fenomeno della Cyber security è diventato un fenomeno sicuramente importante non più solo appannaggio di grandi enti pubblici o di grandi aziende, (è di ieri proprio la notizia che ha subito un attacco Instagram), ma è diventato un problema anche di piccole imprese. Soprattutto negli ultimi anni è cresciuta di molto anche la gravità del fenomeno della Cyber Security. Stime effettuate da CLUSIT, l'associazione per la sicurezza informatica, evidenziano come nel prossimo biennio saranno dai 20 ai 25 miliardi per il nostro paese i danni generati da questo problema. E sappiamo come il tema sia aumentato enormemente in termini di numerosità di attacchi di gravità degli attacchi, ma anche di tipologia. Quindi soprattutto il target delle micro e delle piccole imprese non è estraneo a questa problematica. Sono emersi in questo forum, due filoni di attività su cui anche le imprese devono necessariamente intervenire, due driver di intervento per approcciare al tema della Cyber Security: uno è sicuramente quello delle competenze. È stato più volte oggi evidenziato, sia negli interventi di questa mattina, ma direi anche nel panel precedente, focalizzandosi proprio su l'emergenza delle competenze del fattore umano per il tema della Cyber Security. Anche noi come il sistema camerale con la rete dei PID dei punti impresa digitali evidenziamo come proprio su questo fronte, le imprese siano intervenute in modo ridotto (solo un'impresa su 10 ha effettuato degli interventi formativi sul tema della Cyber Security).
L'altro filone è che cercheremo di affrontare è quello tecnologico. Le imprese negli ultimi anni, soprattutto direi a seguito dell'incremento della digitalizzazione che si è determinata a valle del periodo pandemico, anche le micro le piccole imprese hanno capito che è necessario investire in Cyber Security. Notiamo che oggi siamo al 36% delle imprese che hanno fatto interventi in Cyber Security, ma soprattutto il dato interessante è che si ha avuto un incremento negli ultimi anni del 9% di investimenti in questo processo, in Cyber Security. Quindi si ha avuto un incremento del 9% delle imprese che hanno fatto investimenti in Cybersecurity ed è l'ambito tecnologico nel quale maggiormente sono intervenute le imprese.
La Cyber Security non si delega. Le competenze per la Cyber Security non sono qualcosa che può essere riservato a qualcuno è qualcosa che deve essere diciamo insito nelle attività di ciascuno. Per ciascuno a un diverso livello di approfondimento e in di ampiezza, ma deve coinvolgere tutti.
L'obiettivo è una democrazia della Cyber Security che riguarda tutti. Se si pensa agli attacchi che si sono verificati a enti pubblici ed aziende, si sono verificati proprio agendo su personale che gestiva processi anche diversi rispetto a quelli dell'ICT.
In Italia esiste un canale formativo da 20 anni, in forma più formalizzata da 15 anni, che è quello del sistema degli istituti tecnici superiore (ITS), tuttavia questo tipo di canale è cresciuto molto poco finora.
Il Parlamento ha approvato una legge di riforma del sistema ITS e attraverso il PNR prevedono significativi finanziamenti per il sistema ITS con l'obiettivo di formare una fascia

di tecnici che possono essere operativi per svolgere determinate funzioni appunto livello intermedio.
L'agenzia di Cyber Security sta promuovendo tutte le varie iniziative, dando una specifica attenzione al sistema degli ITS, attraverso una convenzione con il Ministero dell'Istruzione per promuovere il sistema degli ITS.
Tra le iniziative di promozione, anche un sistema di certificazione per gli ITS che si affianchi all'accreditamento che è di competenza della Regioni, che possa contribuire a dare una maggiore visibilità di questi corsi.
L'obiettivo è che questa collaborazione per il prossimo futuro possa diventare uno strumento per mettere professionalità e delle procedure anche su Cyber Security e non solo più In generale sul digitale nelle imprese.
Nel 2021, abbiamo rilevato un incremento del 200% di attacchi informatici alle imprese, attacchi che hanno colpito fino alle piccole micro imprese, (incremento + 20% attacchi a e-commerce).
La strategia dovrebbe prevedere quindi:

1. una maggior impegno alla sensibilizzazione sulla cyber security
2. superamento della fragilità dei sistemi informatici
3. convenzioni con professionisti e assicurazioni
4. semplicità e accessibilità delle soluzioni