LA GUERRA NEL PC

L'ASSOCIAZIONE È PREVENZIONE: V+ PARLA DI RISCHIO INFORMATICO CON STEFANO VERGANI, PRESIDENTE AISOM

A CURA DELLA REDAZIONE DI **V+**

Gli attacchi informatici ai sistemi informativi di Senato e Ministero avvenuti nella prima metà di maggio, e poi quelli a ospedali e aziende, hanno ormai definitivamente svelato le contromosse della guerra cibernetica scaturita dal conflitto Russia-Ucraina.
Infatti, se sui territori vicini la guerra è visibile giornalmente con attacchi militari, quella a distanza si gioca con altri mezzi e strategie.
Perché ne parliamo qui? Perché ne dovremmo parlare subito e fattivamente nelle aziende?
Il fatto è che in questa epoca e in questa civiltà tecnologica, siamo tutti interconnessi e interdipendenti, e quello che succede "là" non solo ci tocca, può farci molto male.

L'informatica non riguarda più i computer. Riguarda la vita.

(Nicholas Negroponte)

IL FRONTE DEI DATI

È chiaro (anche perché affermato dagli organi ufficiali russi) che l'attacco all'Occidente correrà sul filo dei dati. I nuovi mercenari delle guerre cibernetiche si indirizzeranno ad hackerare provider e i loro cloud systems, sia per sistemi produttivi che per le comunicazioni email (ma anche telefoniche). Il messaggio è stato lanciato, sollecitando il mondo economico a proteggere i propri dati in ingresso e in uscita.

Abbiamo intervistato Stefano Vergani, Presidente AISOM – Associazione Italiana per lo Sviluppo Organizzativo e Manageriale delle Imprese, per chiedere come una associazione di PMI suggerisca ai propri associati di raddoppiare gli sforzi affinché il singolo socio, di qualsiasi dimensione e segmento di apparenza, possa prevenire e gestire situazioni che fino a poco tempo fa erano considerate di lontano accadimento.

Il rischio cyber era già un tema caldo nelle agende degli imprenditori, diventato rovente nei due anni di pandemia tra blocchi operativi, furti di dati (anche con riscatto), phishing... Cosa stavate già facendo, e ora cosa è cambiato
Fin dallo scorso autunno AISOM ha moltiplicato i suggerimenti ai soci, invitandoli a perseguire un piano di emergenza e ad avere un'attenzione più responsabile. La guerra scoppiata a Est ha confermato che il conflitto sarà molto lungo e cruento. Come può uno Stato invasore colpire gli alleati del Paese invaso? Non certo spostando cannoni o sparando missili intercontinentali: è evidente che l'Occidente può essere combattuto da lontano e nei propri confini utilizzando le strategie che l'informatizzazione diffusa ormai consente.
In questa drammatica evoluzione, il 24 maggio AISOM ha organizzato un webinar con relatori di primissimo piano che possono dare una nuova luce su quanto ci si può aspettare. Anche con punti di vista molto, molto reali e operativi: vedi l'esperienza del Centro di Sicurezza Telematica dell'Arma dei Carabinieri (in cui ho militato anche io), insieme a realtà specializzate in questioni di cyber sicurezza – oltre che di management.

Cosa è cambiato sul tema rispetto anche a soli 12 mesi fa?
Le aziende si sono intanto sempre più informatizzate, e se si sono automatizzare da un lato, dall'altro prestano il fianco a nemici invisibili e quasi impossibile da localizzare.
I sistemi di ogni azienda possono essere a questo punto il vero tallone di Achille per la sua stessa sopravvivenza. Ormai si è passati dalla fase di hackeraggio con riscatto alla fase di hackeraggio

per distruggere: nessuno è più indenne. Sistemi automatici di ferrovie e i loro clienti e fornitori, aeroporti e logistica con i loro clienti e fornitori, fornitori di servizi di aziende pubbliche, aziende di produzione, aziende di servizi: tutti sono possibili target di chi ha il compito di bloccare l'economia di un Paese. Se quindi la mancanza di materie prime – o il loro aumento spropositato come costo e le crisi di reperimento energetico – spingono le aziende a rivedere i loro programmi, ora gli scenari sono ancora più critici.
E questo è lo scenario più visibile o più percepito, anche perché se si blocca un ospedale o le ferrovie, se ne parla; ma nessuno è immune (siamo tutti collegati e tutti impreparati). Per una piccola o media azienda, come anche uno studio professionale, essere oggetto di un attacco informatico può avere effetti in proporzione ancora più gravi. Le spalle sono meno larghe: se mi blocchi la logistica si ferma tutto, se mi rubi il gestionale insieme ai miei dati, rubi anche quelli di fornitori e clienti...

Come rispondono le imprese ai vostri alert – e suggerimenti?

Le imprese attente all'innovazione e allo sviluppo tecnologico sono sempre le prime a sensibilizzarsi e ad agire, ma la maggior parte (ahimè!) si trova spiazzata, anche per la velocità con la quale le cose si sono evolute. Ecco perché abbiamo il compito di continuare a spingere.
Uno studio USA uscito qualche mese fa ha chiaramente segnalato come il prossimo target della guerra informatica sarà proprio il mondo delle imprese. E siccome in Italia l'economia – sia old che new economy – è fatta essenzialmente da PMI, è previsto che gli attacchi non saranno rivolti solo alle grandi organizzazioni.
Anche la finanza è un target primario. Bloccare la finanza è una tattica voluta e perseguibile, proprio perché è una delle poche armi non militari che dall'Est gli aggressori possono attrezzare in poco tempo e con grande virulenza, per spianare un Paese.
Pensate a quante imprese ferme, lavoratori messi in cassa integrazione e poi licenziati!

HIGHLIGHTS DAL WEBINAR DEL 24 MAGGIO

Il nuovo scenario geopolitico in Europa. Prospettive per l'economia italiana tra vincoli da dazi, sanzioni economiche e rischi informatici.

Il Ten. Col. **Marco Mattiucci**, Capo del Centro Sicurezza Telematica del Comando Generale - Arma dei Carabinieri, ha trasferito la sua esperienza e visione al mondo delle imprese.
"In Italia ci sono ancora molti stakeholder convinti che la telematica sia solo un supporto: mentre è un fattore abilitante globale."
"La cyber security è fatta da cyber defence (le barriere che mettiamo) e cyber operations (la risposta agli eventi). Per una piccola azienda sono cose gravose. Per me un'arma indispensabile e "accessibile" è quella del Cloud – smettiamola di essere "gelosi" dei nostri dati e scegliamo subito questa soluzione. Significa anche che gestire nuovi modelli di efficienza e rispondere a possibili attacchi sarà questione di chi detiene il Cloud."

L' Ing. **Gianmarco Biagi**, Presidente AICIM e Membro AISOM, ha parlato dei limiti attuali della cultura imprenditoriale italiana nell'information risk.
"Si parla ancora di innovazione semplicemente passando a un gestionale più evoluto, in un contesto in cui per fare impresa si ragiona già in termini di realtà virtuale. Come parlare ancora di fax in un contesto di prossimo Metaverso."
"Fare impresa è il compito principale degli imprenditori, non dei loro consulenti: è un errore strategico enorme non considerare la digitalizzazione e la cyber come partner del nostro business."

Matteo Gatti, Unit Manager Milano Mentor & Faber, ha parlato dei requisiti e dei compiti che devono avere le figure professionali oggi necessari in azienda.
"Nell'ultimo mese in un solo canale professionale si sono aperte oltre 1.200 ricerche per figure professionali in grado di la sicurezza informatica in azienda."
"Prima ancora di chi ha competenze operative, servono figure manageriali, in modo che sappiamo costruire tutto il sistema di evoluzione digitale e di cyber sicurezza in una azienda. Ad oggi non sempre avere un attestato significa essere davvero esperti o in grado di gestire tutti gli aspetti, tecnici e trasversali - dagli aspetti legali alla gestione del team: per le aziende si tratta di scelte urgenti, ma a cui prestare speciale attenzione in fase di selezione."

L'avvocato **Alessandro Continiello**, Capo Divisione Ethics & Compliance Studio Legale Martinez & Novebaci, ha parlato dei rischi delle aziende verso i clienti e i fornitori in questo nuovo scenario di guerra cibernetica.
"La sicurezza informatica viene ancora spesso vista come un costo: ma il vero costo invece è quello giuridico ed economico, in caso di attacchi, sia per l'impresa che per le sue figure apicali – in quanto responsabili anche oltre il furto di dati, vedi in caso di appropriazione indebita di fondi o altre truffe."
"La prossima diffusione del Metaverso apre ulteriori problematiche e scenari, e non solo sul fronte della privacy."

Come garantire alle aziende la continuità in caso di criticità? A questo rovente tema ha dato risposte **Grazia Bruno**, Direttore Operativo Expandi IT.
Tra le azioni di sicurezza c'è la protezione anche attraverso una polizza assicurativa, a tutela anche della continuità operativa: e se le aziende in ambito IT si sono già attivate, le altre sono ancora spesso "in attesa". In molti casi il reparto IT interno delle piccole aziende si fa sponsor di questa necessità, ma il tutto resta in stallo sulla scrivania del titolare: la crescita degli attacchi e l'alta probabilità di rischio su più fronti (operativo, logistico, dati), non viene ancora percepito come reale e tangibile.
"In molti casi la protezione assicurativa è la variabile che consente di superare o mitigare l'attacco, anche in termini di servizi di assistenza operativa sia sul fronte tecnico, che su quello legale e della comunicazione."

La tavola rotonda è stata moderata da **Giulio Valeri**, Membro AISOM e CEO Software Solutions.