COVID-19 Raccomandazioni per la gestione dei dati e delle informazioni rispetto ad attacchi Cibernetici e rischi per la produzione italiana

Abstract

In questo periodo di grande sofferenza ed incertezza, causate dal diffondersi del virus COVID-19, in Italia ed in tutto il mondo, ci troviamo ad affrontare nuovi scenari di rischio legati alla sicurezza dei nostri dati e delle informazioni che trattiamo ogni giorno. L'adozione massiccia di soluzioni di Smartworking ha sicuramente creato un'accelerazione alla trasformazione Digitale nel nostro Paese, ma al contempo ha aperto le "porte" a possibili nuovi attacchi, in quanto non tutti i cittadini, liberi professionisti, docenti o dipendenti di aziende erano preparati ad un cambiamento cosi dirompente. L'utilizzo di tecnologie digitali necessarie allo Smartworking, come sistemi di videoconference (es. Teams, Webex, Zoom, GotoMeeting, Slack, etc), e sistemi di file transfer (es. WeTransfer, etc) non può che portare ad un'attenta riflessione degli addetti ai lavori in relazione alla sicurezza informatica. Capita, infatti, sempre più di frequente, di trasmettere dati sensibili su canali non convenzionali e di usare strumenti informatici, non sempre adottando un livello di sicurezza adeguato. Spesso le postazioni di lavoro sono prive di Antivirus, mancano canali di comunicazione sicura VPN, sistemi di Backup centralizzati e crittografia delle email, ovvero gli elementi di base per una corretta sicurezza dei nostri dati e delle nostre informazioni.

La mancata adozione, parziale o totale, di soluzioni centralizzate e locali da parte di alcune aziende e/o di alcuni cittadini, liberi professionisti, potrebbe favorire attività malevoli da parte di gruppi criminali. Questi potrebbero perpetrare azioni di Phishing, con l'obiettivo di crittografare i dati dei singoli presenti sui PC (es. Ransomware), o addirittura, effettuando attacchi di ingegneria sociale, carpire informazioni sensibili da sfruttare in un secondo momento, superata la pandemia, per generare, un attacco più sofisticato (es. Advanced Persistent Threat) con pesanti ricadute sulle infrastrutture critiche del Paese e un possibile ulteriore blocco delle attività produttive.

La raccomandazione è quella di potenziare i propri device utilizzando soluzioni di sicurezza adeguate in relazione al livello di rischio, operatività e trattamento dei dati.

Contesto

Come in altri Paesi anche in Italia si stanno diffondendo campagne di phishing e malspam, che sfruttano le preoccupazioni che la pandemia di Coronavirus sta generando nelle persone. I

criminali del web approfittano di questo momento di grande vulnerabilità psicologica per colpire le ignare vittime con attività legate al COVID-19.

La Polizia postale e delle comunicazioni scopre ogni giorno frodi informatiche basate sull'invio di email a firma di presunti esperti dell'Organizzazione mondiale della Sanità. Questi messaggi di posta elettronica, dal linguaggio professionale e contenuto assolutamente credibile, invitano le vittime ad aprire un allegato infetto, che conterrebbe indicazioni per evitare l'infezione da Coronavirus.

Nel frattempo le aziende si stanno adoperando per rendere sempre più sicure le loro infrastrutture, attraverso l'adozione di sistemi di sicurezza centralizzati per il monitoraggio delle anomalie delle singolo postazioni di lavoro.

Rischi

Un rapporto del Clusit (Associazione Italiana per la Sicurezza Informatica) afferma che in Italia, nell'83% dei casi la causa degli attacchi è il Cybercrime, fenomeno che nell'ultimo anno è cresciuto del 12,3% rispetto al 2018 e del 162% rispetto al 2014. Andando a monitorare le tecniche utilizzate negli attacchi, si parla di Ransomware nel 46% del totale, in crescita del 21% rispetto al 2018.

I rischi sono legati al tipo di vittima e al possibile impatto nella perdita dei dati. In tal senso è possibile distinguere due macrocategorie di soggetti a rischio:

- Cittadino, Libero professionista, docente, etc
- Dipendenti di aziende di piccole, media e grandi dimensione

Entrambi i soggetti, possono essere coinvolti:

- in attacchi di phishing con lo scopo di carpire informazioni o estorcere denaro (es. Ransomware)
- in attacchi di ingegneria sociale, volti a recupero di informazioni altamente sensibili utilizzabili per successivi crimini informatici più sofisticati;
- nell'inconsapevole rivelazione di informazioni di rilevanza strategica aziendale, utilizzando strumenti di file share non autorizzati, senza l'ausilio di adeguati strumenti di protezione in

grado di monitorare lo scambio di dati sensibili e bloccarne la diffusione non autorizzata su canali non leciti;

- nell'inconsapevole utilizzo di non idonei sistemi di backup di dati sensibili.

Raccomandazioni

Esistono soluzioni di breve e di lungo termine. Le soluzioni di breve termine sono in parte rappresentate dai suggerimenti già imposti dal GDPR o da standard internazionali tipo ISO27001.

Anche in questo caso va fatta una distinzione tra cittadino, libero professionista, docente e etc., e realtà aziendali.

Nel breve periodo le azioni da intraprendere possono essere così riassunte:

- Primo livello: dotarsi di strumenti di protezione come antivirus, aggiornandoli costantemente, effettuare backup ogni giorno ed evitare di trasmettere informazioni sensibili tramite canali non sicuri di file sharing pubblici. Se proprio non si dispone di sistemi di sharing sicuro accettarsi di proteggere i propri dati con password robuste, usare sistemi di crittografia delle email e fare attenzione alle email ingannevoli.

- Secondo livello: dotarsi di sistemi di analisi dei log degli accessi alle applicazioni da parte dei dipendenti, sistemi di monitoraggio dei dati sensibili attraverso Data Loss Prevention, sistemi di web filtering per evitare spam e phishing e, infine, di sistemi di backup altamente affidabili. A questo va affiancato il continuo aggiornamento del personale dipendente, informando sulle novità riguardo le minacce cyber e invitando al rispetto delle policy aziendali in tema di sicurezza informatica.

Ulteriori elementi da considerare sono illustrati nelle raccomandazioni di ENISA, Agenzia europea per la sicurezza delle reti e dell'informazione, (*https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home)* e dell'Europol, l'agenzia per la lotta al crimine dell'Unione europea (*https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold*)

Nel lungo periodo le possibili azioni da intraprendere potrebbero essere:

- Creazione di campagne di sensibilizzazione su scala nazionale, attraverso i principali media, per informare la collettività sulle primarie minacce informatiche.

- Formazione di gruppi di lavoro ad hoc, a livello di Protezione Civile, Difesa e Interno, per l'attuazione di scenari di crisi nel caso di attacchi Cyber su scala Nazionale.

- Predisposizione di un comitato tecnico strategico che includa, oltre il DIS (Dipartimento informazione sicurezza) e i competenti Ministeri, anche i rappresentanti delle Università, delle Aziende specializzate e degli Ordini professionali, nonché di agenzie europee come ENISA e Europol.