L'emergenza COVID-19 ha costretto molte aziende a lavorare secondo la modalità dello smart working.

Ma conosciamo realmente le minacce e i rischi che questa modalità comporta?

L'articolo di approfindimento è a cura della nostra docente FIAss, **Laura Lucchi, Criminologa e esperta Risk Management GDPR.**

Smartworking e Cyber Security: il lavoro ai tempi del COVID-19 -rischi e minacce

Le restrizioni per la prevenzione dei contagi da **COVID**, imposte dal Governo, **hanno costretto ad adottare la formula "Smart Working"**
- lavoro agile - con un poderoso impulso alla diffusione di pratiche di lavoro e didattica da remoto: in Italia il ricorso a tale modalità lavorativa - pur già esistente da diversi anni, **ha visto nei due mesi appena trascorsi un'impennata del 40%.**

La maggior parte delle soluzioni adottate prevedono **lo sfruttamento dei dispositivi e della connessione alla rete degli stessi lavoratori.**
Il fenomeno, già esistente come abbiamo anticipato e precedentemente definito con l'allocuzione inglese
BYOD, "Bring Your Own Device"
-Porta il Tuo Dispositivo-, era già stato adottato
da alcune aziende in via sperimentale perché le prestazioni dei dispositivi mobili, sono equiparabili a quelle delle postazioni di lavoro fisse.

L'utente li usa con molta facilità e, inoltre, **si evita la duplicazione in termini di investimento tecnologico** per acquisto e manutenzione di ulteriori dispositivi e i costi relativi alla connessione alla rete.
I benefici che derivano dallo
Smart Working
a distanza sono oramai un dato assodato per le aziende e per i lavoratori, una necessità impellente per il periodo di emergenza che stiamo vivendo.

Oltre a innegabili vantaggi, il lavoro da remoto presenta numerose aree di **rischio sul fronte della cybersecurity** :
l'attività da svolgere in modalità Smart Working non prevede generalmente e a maggior ragione adesso,
particolari restrizioni tecniche e di sicurezza,
ne consegue un alto rischio per la privacy e per eventuali attacchi hacker. La struttura che connette allo smart working fra azienda e lavoratore in rete, implica infatti, che si acceda dall'esterno al sistema e alla rete aziendale,
coinvolgendo dispositivi dei lavoratori non sicuri e fuori dal controllo dell'azienda.

Se sul luogo di lavoro si è protetti dalla rete aziendale, quando si lavora da remoto bisogna fare molta attenzione: **gli Hacker, lo ricordiamo, sfruttano le debolezze dei sistemi** per accedere ai dispositivi e introdurre applicazioni infette, piuttosto che attacchi di phishing e messaggi dannosi.

La pandemia in corso ha fatto aumentare gli attacchi cyber: le campagne di phishing sono in preoccupante aumento e i **social media sono oggetto di attacchi differenziati ad esempio fake news e attività finalizzate a manipolare consensi o destabilizzare le comunicazioni.**
Attacchi cyber di grande portata potrebbero disconnettere intere comunità, interrompendo la normale operatività dei servizi erogati dal sistema sanitario- come già avvenuto in Inghilterra in tempi non sospetti - o da altri operatori essenziali, ad esempio sito
INPS a fine marzo.

Già nel mese di marzo, in Italia sono state diffuse **mail che contengono Trickbot in documenti Word** , con cui si promettono informazioni utili sul coronavirus e altre contenenti allegati con il banking trojan

Emotet
(si basa sull'invio di e-mail mal estremamente plausibili e quindi maggiormente ingannevoli, così da indurre le vittime a eseguire i loro allegati dannosi contenenti documenti Office).

Ginp , il mobile banking trojan che**, in cambio di una piccola somma di denaro, promette di visualizzare la posizione delle persone risultate positive al Coronavirus.**
In realtà il suo scopo è quello di rubare i dati delle carte di credito delle vittime.
Per convincere la vittima ad utilizzare questo particolare "servizio", Ginp usa un'esca particolarmente subdola: la pagina Coronavirus finder, infatti, afferma che 12 persone infettate dal Covid-19 si trovano nelle sue vicinanze e promette di mostrare la loro esatta posizione. Se la vittima accetta di visualizzare queste informazioni, viene reindirizzata ad una nuova pagina Web sulla quale può effettuare il pagamento. Una volta inseriti i dati della carta di credito, però, la vittima non riceve le informazioni relative alle persone "infette": lo scopo dei criminali informatici è infatti, esclusivamente quello di entrare in possesso delle credenziali della carta di credito dell'utente nel momento in cui vengono inserite per effettuare il pagamento. (Fonte: Paolo Tarsitano - Editor Cybersecurity360.it)

Definire, quindi, **buone pratiche di sicurezza informatica e Cyber security è necessario**, ma l'approccio a queste tematiche non è semplice per le parti – impresa e lavoratore – che, al solito hanno visioni contrapposte: da un lato l'azienda necessita di raggiungere affidabilità e sicurezza come se il lavoratore operasse al suo interno, ad esempio con policy aziendali di sicurezza informatica ai dispositivi di loro proprietà, come l'utilizzo della VPN per la connessione sicura alla rete aziendale, l'installazione dello stesso Endpoint aziendale, l'aggiornamento del software.

D'altro canto, **il lavoratore gradisce poco i meccanismi necessari ad ottenere quanto sopra auspicato** in quanto recepiti come invasione della propria privacy o una limitazione alla libertà di autogestione, tipica invece del lavoro a domicilio, inoltre il dispositivo

del lavoratore, solitamente contiene informazioni e applicazioni private che l'utente non gradisce che vengano conosciute dall'azienda.

Le organizzazioni più avvedute, pur adeguandosi in emergenza, **hanno acquisito prodotti per il remote working, anche open source, dotati di un minimo di sicurezza come i Software per lo Smart Working, VPN.**
Le imprudenti hanno abilitato i protocolli di Remote Desktop – RDP - sulle postazioni aziendali, per consentire ai propri collaboratori di collegarsi da remoto alle postazioni in ufficio, oppure sfruttano i programmi utilizzati ordinariamente per l'assistenza remota; sono software portatori di bug.

Smart Working e Cyber Security: possibili soluzioni

Organizzazioni complesse e rigide nella tutela i propri asset e, indirettamente, anche i dati del lavoratore adottano misure di prevenzione e protezione cyber prevedono il logging dell'attività dell'utente e del dispositivo. Ciò, tuttavia, impatta con il diritto alla privacy e del proprietario del dispositivo fuori dal contesto lavorativo

Nei casi in cui le aziende non abbiano strutture complesse e necessità di preservare dati particolarmente sensibili, come ad esempio il settore sanitario e quello delle transazioni economiche, possono limitarsi ad indicare ai propri dipendenti **delle linee guida, sia durante l'utilizzo personale che lavorativo.**

Questa soluzione, presenta incertezza sulla compliance alle politiche di sicurezza aziendali, sul tema della riservatezza (documenti classificati), la tutela dei dati personali (GDPR), la business continuity e il disaster recovery (NIS), pur tutelando i diritti del lavoratore.

Una revisione dei protocolli di sicurezza e la formazione capillare delle persone coinvolte appaiono urgenti
per scongiurare il concreto rischio che il cybercrime approfitti di questa ghiotta occasione per attaccare, a scopo di profitto o destabilizzazione politica, reti e sistemi pubblici, aziendali o personali.

Link utili:

Corsi FIAss Aggiornamento IVASS 2020 Cyber Security

News Intermediari Assicurativi

Seguici s ulle nostre pagine social

Facebook

LinkedIn