PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4727 di Venerdì 26 giugno 2020

Il mondo del lavoro in smart working: cyber security

Scopriamo le implicazioni sulla sicurezza informatica che il lavoro agile ha portato con sé.

Abbiamo parlato in questo articolo delle implicazioni psicologiche e fisiche associate all'uso massivo dello smart working durante i mesi di quarantena.

Ma il fenomeno dell'adozione di massa e "frettolosa" del lavoro da casa ha fatto emergere criticità e best practices anche in tema di sicurezza informatica e difesa dal cybercrime.

Smart working e criminalità informatica

La fretta con cui aziende e professionisti hanno dovuto cambiare le modalità di lavoro, convertendo in online e a distanza tutto ciò che prima si poteva fare in ufficio o di persona, ha creato nuovi rischi di **sicurezza informatica**.

Tutti i principali esperti di **cyber security** - tra cui quelli del Clusit, l'associazione della sicurezza informatica italiana - hanno lanciato allarmi: la diffusione improvvisa dello smart working ha aumentato i rischi di attacchi hacker in cerca di soldi e dati riservati.

"Il lavoratore in smart working corre pericoli maggiori online. Non è in ufficio, dove può contare sul supporto diretto dei tecnici se incorre in un malware, ad esempio. Può essere privo di molte delle protezioni aziendali, che funzionavano bene in ufficio, ma non a casa propria", spiega Alessio Pennasilico, esperto e membro del consiglio direttivo del Clusit.

Il problema è esacerbato dal contesto: "Lavoriamo più ore online, gestiamo più mail, siamo sempre in video conferenza: di conseguenza siamo più stanchi e più soggetti a fare errori di sicurezza", aggiunge. Errori basilari in tema cyber security: come cliccare su link o aprire allegati di email di phishing; scaricare app o programmi da siti non affidabili e potenzialmente pieni di malware che possono rubarci dati personali, password, credenziali di accesso.

Se nello smart working sono usati "PC domestici per collegarsi alla rete aziendale, le conseguenze sono ancora più disastrose: veicolano infezioni ovunque. Se salvi tutto sul pc casalingo e un malware blocca il disco, non puoi contare sul backup aziendale. Il furto della password della mail, del sistema di videoconferenza ora ti taglia completamente fuori dal mondo, dato che tutti i rapporti con colleghi, clienti e fornitori devono passare da internet", continua Pennasilico, esperto di cyber security.

Giorgio Sbaraglia, consulente informatico, conferma: "Lo smart working aumenta notevolmente il rischio di attacco informatico e di violazione e furto dei dati. Per chi lavora da remoto i maggiori rischi sono - ancora una volta - legati al fattore umano ed al social engineering. E la maggior parte delle minacce (circa il 90% come ha confermato anche un recente rapporto di Yoroi) arrivano attraverso l'**email**", dice.

Potremmo ricevere un'email che sembra inviata dall'indirizzo personale del capo o di un collega. Vista la situazione di smart working, non saremo più di tanto insospettiti che il capo non usi l'email aziendale (anche lui in smart working). "Ma se l'indirizzo email è stato falsificato a scopo malevolo, il clic sul link o sull'allegato avrà come risultato l'intrusione del malware nel computer della vittima. Questo rischio sarebbe stato molto meno probabile se il dipendente si fosse trovato in ufficio, dove - tra l'altro - avrebbe avuto la possibilità di chiedere un consiglio al servizio IT su cosa fare di fronte ad un'email del genere", dice Sbaraglia.

Inoltre, i cyber criminali sono abili a cogliere le tendenze del momento. Per questo motivo le email di phishing utilizzano i temi più attuali: in circa 230 mila campagne di **spam e phishing** rilevate in questi ultimi mesi (il 6% ha colpito l'Italia), le parole chiave più frequenti sono state: Covid-19, coronavirus, OMS o WHO (Organizzazione mondiale della Sanità) e le diverse piattaforme di videoconferenza.

Per fortuna, passata la fase più emergenziale, adesso lavoratori e aziende possono predisporre migliori difese contro il **rischio informatico**.

Gli esperti sono d'accordo: la consapevolezza dell'utente rispetto ai rischi informatici è il punto nodale della **cyber security**. "Il fattore umano è la causa di oltre il 95% di tutti gli attacchi informatici", dice Sbaraglia. "Dovrà essere anche l'azienda a fornire ai propri collaboratori un adeguato livello di **formazione e consapevolezza sull'uso degli strumenti informatici**. Consapevolezza che si può sintetizzare nel modello Zero Trust (fidarsi è bene, non fidarsi è meglio), per evitare che un clic affrettato o distratto blocchi un'azienda".

A tal fine, è molto utile il **corso online "aggiornamento lavoratori Cyber Security"** della durata di un'ora.

Per prevenire attacchi, in modo basilare, tutti dovrebbero attivare l'**autenticazione a due fattori** per tutti i servizi dov'è possibile farlo (social, account Google, mail). "Se anche le aziende fornissero device completamente blindati, dovrebbero comunque garantire allo stesso tempo anche sistemi wifi e routing protetti e sicuri direttamente a casa del dipendente. Il tutto governato da policy e procedure del corretto utilizzo dei sistemi e dotazione aziendale", dice Iezzi. E aggiunge: "Ma non sarebbe sufficiente. La rete domestica può essere messa a rischio anche dai comportamenti di altri membri del nucleo familiare del dipendente. Per questo motivo, le attività di formazione che periodicamente vengono effettuate ai dipendenti potrebbero essere allargate anche ai familiari".

A parere degli esperti, le policy più tecniche che le aziende dovrebbero adottare sono quelle finalizzate a:

- determinare il sistema aziendale di videoconferenza e di chat;
- fare periodicamente analisi del rischio tecnologico;
- condurre costantemente attività di asset e software inventory allo scopo di identificare oggetti hardware o software non "aziendali";
- adottare sistemi di monitoraggio della rete al fine di identificare tramite sistemi di early warning anomalie a livello di traffico della rete aziendale;
- avere un adeguato sistema di disaster recovery o almeno un efficace sistema di backup in cloud;
- attivare sul PC domestico una partizione separata per gestire e conservare i dati aziendali.

Sarebbe ancora meglio optare per soluzioni e applicativi "**cloud based**": l'applicativo è nel cloud del fornitore ed è necessario solo un collegamento internet ed un'interfaccia di collegamento (un browser). In questo modo il dipendente può usare il computer senza installare alcun software e minimizzando i rischi di cui sopra. Tuttavia, questa soluzione non può essere improvvisata: richiede tempo e programmazione. Sarà opportuno adottare prodotti di fornitori affidabili, evitando soluzioni improvvisate e gratuite anche nella scelta della **VPN** (Virtual Private Network). Il consiglio è preferire VPN che utilizzano la crittografia dei dati trasmessi, in modo da avere una comunicazione protetta. Infine, se si utilizza il collegamento con Desktop Remoto (RDP), sarà indispensabile impostare password forti e - come ulteriore sicurezza - abilitare l'autenticazione a due fattori.
