DAL PARLAMENTO

Smart working in sicurezza: serve attenzione e impegno

di **Redazione** · 21 marzo 2020, 00:01

**di Francesco Pagano, Consigliere Aidr e Responsabile servizi informatici Ales spa e Scuderie del Quirinale*

L'emergenza Covid-19 e la necessità di ridurre le frequentazioni sociali ha portato a un vero e proprio boom dello smart working. Il lavoro a distanza, in questa difficilissima situazione, rappresenta infatti uno degli strumenti più efficaci per favorire l'adozione di quei comportamenti virtuosi (e necessari) per contenere la diffusione della pandemia influenzale.
Una fase difficile, anche perché il nostro paese sconta (ancora) un notevole ritardo per quanto riguarda la connettività a banda larga. Un tema, questo, aggravato dal fatto che in Italia una buona fetta della popolazione si "accontenta" di accedere a Internet attraverso la connessione mobile, che in questa situazione risente però di limiti (primo tra tutti il limite di traffico per i contratti) che emergono con tutta la loro prepotenza in uno scenario di smart working.
Questo repentino passaggio a una forma di lavoro in remoto, però, apre anche numerose questioni legate al tema della cyber security. Un aspetto che, nella fretta di implementare strumenti per favorire l'attività a chi può rimanere a casa, rischia di essere trascurato.
In questi giorni, decine di migliaia di persone stanno utilizzando strumenti (dai sistemi di videoconferenza a quelli di condivisione su cloud) che non conoscono, o che comunque non sono abituati a utilizzare in maniera intensiva. Soprattutto nel settore della pubblica amministrazione, dove l'adozione di modalità di lavoro flessibile non hanno ancora "sfondato" e in cui le infrastrutture non sono quindi pronte a offrire un ecosistema adeguato.
In un'ottica di cyber-security, il primo rischio è quello legato all'utilizzo di prodotti gratuiti poco sicuri, magari "pescati" su Internet dopo una frettolosa ricerca. Il Web, purtroppo, pullula di programmi offerti gratuitamente che nella migliore delle ipotesi utilizzano protocolli poco sicuri, nella peggiore contengono funzioni indesiderate, come la visualizzazione di annunci pubblicitari o la registrazione di informazioni personali.
I responsabili IT e di cyber security dovrebbero quindi predisporre una "cassetta degli attrezzi" a

disposizione di dipendenti e collaboratori, in modo che questi possano utilizzare gli strumenti più adatti sia in termini di efficienza, sia in termini di sicurezza.
Un ulteriore problema riguarda il corretto utilizzo degli strumenti di telelavoro. Se l'uso intensivo di strumenti di comunicazione come l'e-mail e i vari messenger apre la strada a una maggiore esposizione a eventuali attacchi di phishing e malware, quelli per la condivisione di documenti e informazioni portano con sé anche il rischio di un'errata gestione di dati.
Un semplice errore, come la condivisione di un collegamento a una cartella interna ai sistemi della propria organizzazione, può avere conseguenze anche molto gravi e mettere a repentaglio l'integrità stessa dei dati conservati sui sistemi informativi.
Per evitare incidenti legati alla gestione dei dati è necessario prevedere delle policy rigorose, che consentano di regolare l'accesso a documenti e informazioni attraverso la creazione di permessi basati sul ruolo e limitare la possibilità di condivisione verso l'esterno dei dati sensibili.
Più ampio il capitolo riguardante il cyber-crimine. La cronaca recente riporta infatti di azioni intraprese da numerosi gruppi di pirati informatici che stanno sfruttando la situazione per trarne il massimo vantaggio. In quest'ottica, l'adozione di modelli di Smart working improvvisati rappresenta un fattore di rischio enorme.
La gestione dei dati e dei dispositivi al di fuori del perimetro IT dell'organizzazione comporta di per sé un esponenziale aumento della superfice d'attacco a disposizione degli hacker, che hanno la possibilità di agire senza dover affrontare tutti quei sistemi di protezione (come firewall e sistemi di analisi del traffico) che normalmente garantiscono la sicurezza delle comunicazioni all'interno delle reti.
L'adozione di una VPN in grado di proteggere la connessione da remoto, oltre alla predisposizione di controlli rigorosi per quelle parti di infrastruttura che devono essere necessariamente aperte per consentire l'accesso a servizi e dati, rappresentano di conseguenza un passaggio fondamentale per offrire ai lavoratori un ecosistema sicuro ed evitare di lasciare "scoperte" intere aree.
In assenza di sistemi di device management, sia per i dispositivi mobili che per i "classici" computer, si apre anche il tema della vulnerabilità degli endpoint utilizzati. Un tema che richiede, come minimo, una gestione attraverso software di protezione che siano in grado di offrire una copertura adeguata anche in una situazione di lavoro "casalinga".
La soluzione migliore, però, sarebbe quella di utilizzare strumenti in grado di compartimentare i dispositivi, creando un ambiente separato dedicato all'ambito lavorativo, implementare forme di protezione dei dati basati su sistemi di crittografia dei dati. Qualcosa che è possibile fare attraverso software specifici e che garantirebbe di separare in maniera netta l'ambito lavorativo dalla sfera della vita privata, mitigando così il rischio di attacchi provenienti da social network, e-mail

privata e altri potenziali vettori esterni.

Insomma: in una situazione come quella attuale richiede, anche in corso d'opera, un'attenta attività volta alla predisposizione di strumenti affidabili (e ben configurati) che abilitino il passaggio allo smart working. Considerando anche che, in una prospettiva futura, questa difficile emergenza può trasformarsi in un'opportunità per creare una base solida che consenta di sfruttare al meglio le opportunità offerte dal digitale.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2020/03/21/smart-working-in-sicurezza-serve-attenzione-e-impegno/

© 2026 Istituzioni24