Smart working: le buone pratiche per la sicurezza digitale
Cosa possono fare le aziende?

LEONARDO

COSA POSSIAMO FARE	OVVERO
1  **Creare consapevolezza nella popolazione aziendale**	Informare e formare la popolazione aziendale sui rischi che la nuova situazione comporta, su quali siano le possibili vulnerabilità che essa induce e su quali siano i comportamenti rischiosi da non adottare e quali quelli virtuosi da adottare responsabilmente.
2  **Usare il più possibile dispositivi aziendali**	Quando possibile usare i dispositivi aziendali che a differenza di quelli domestici sono più sicuri e con protocolli adeguati per evitare data leaks e possibili intrusioni.
3  **Aggiornare frequentemente la sicurezza dei dispositivi aziendali**	Mantenere aggiornati i dispositivi aziendali forniti con le ultime patch di sicurezza e adeguatamente equipaggiati con SmartWorking antivirus e sistemi EDR (End Point Detection & Response).
4  **Intensificare l'uso di strumenti di vulnerability management**	Rispondere alle nuove necessità di sicurezza con un monitoraggio più intenso e frequente intensificando la periodicità di scansioni perimetrali ed interne con strumenti di vulnerability management allo scopo di identificare vulnerabilità.
5  **Aggiornare i dispositivi di protezione perimetrale**	Verificare che i gateway VPN e i dispositivi di protezione perimetrale in genere siano aggiornati all'ultima release e all'ultima patch resa disponibile dal vendor; eliminare servizi e funzionalità non necessari; utilizzare protocolli sicuri per la cifratura e "cypher suite" robuste.
6  **Limitare le funzionalità dei dispositivi hardware aziendali alle sole esigenze lavorative**	Prevedere una corretta hardenizzazione dei dispositivi ovvero imporre dei limiti di funzionalità agli hardware aziendali, applicando una configurazione che ne impedisca un utilizzo diverso da quello lavorativo.
7  **Virtualizzare i desktop**	Applicare tecniche di virtualizzazione dei desktop (VDI) adottando soluzioni che consentano l'accesso ad asset virtualizzati.
8  **Cifrare i dati**	Prevedere sistemi di cifratura dei dati locali (File System/Disk Encryption) al fine di prevenire la perdita di dati critici.
9  **Usare solo connessioni VPN (Virtual Private Network)**	Utilizzare esclusivamente connessioni cifrate (Virtual Private Network) per la connessione alle reti aziendali, utilizzando "cypher suite" con l'adeguato grado di robustezza.
10  **Adottare misure che mitighino gli attacchi volumetrici**	Adottare sistemi anti DDoS (Distributed Denial of Service) per essere pronti a mitigare eventuali attacchi volumetrici mirati a saturare la banda di comunicazione delle vittime.
11  **Comunicare tempestivamente le vulnerabilità**	Adottare soluzioni di tipo Early Warning per la tempestiva comunicazione di vulnerabilità e minacce sulle tecnologie particolarmente esposte dallo smart working (boundary protection, VPN gateway, workstation & endpoint).
12  **Adottare soluzioni di comunicazione a continuità garantita**	Adottare soluzioni che prevedano l'uso di diversi provider per i servizi di comunicazione (multi-carrier) a garanzia della continuità dei servizi erogati e della operatività del proprio personale remoto.