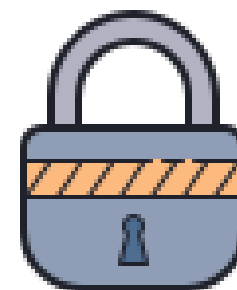


CYBER SECURITY TIPS #25

COME GESTIRE LA CYBER SECURITY NEL 2020.

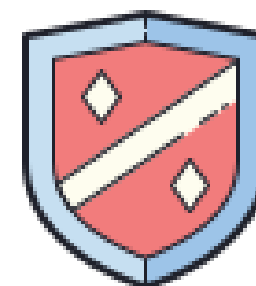


LEGGI SUBITO LE NOSTRE TIPS!



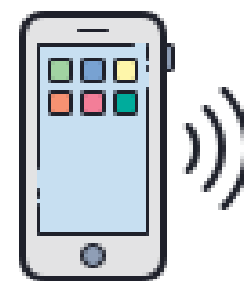
1. SAPPI CHE I GIOCHI SONO CAMBIATI.

Il perimetro informatico aziendale non combacia più con la sede di lavoro, grazie all'adozione di soluzioni Cloud e Smart Working. Questo vuol dire che proteggere i dati aziendali è diventato più complesso.



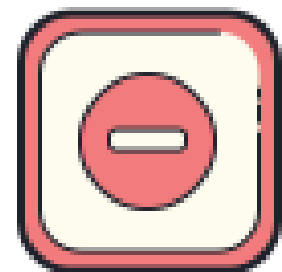
2. GARANTISCI L'END POINT PROTECTION.

Dal 2020 diventa necessario proteggere gli end point dei dipendenti in remote working attraverso nuove politiche di sicurezza e limitazione degli accessi in termini di autorizzazioni.



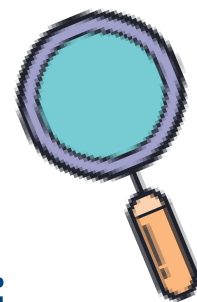
3. APPROCCIO ZERO TRUST.

Non è più possibile riconoscere un processo come sospetto basandosi sul semplice fatto che provenga al di fuori della rete aziendale. Ogni attività deve essere controllata in quanto potenzialmente malevola.



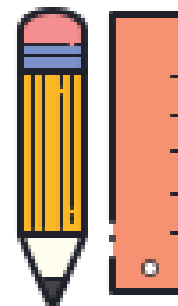
4. VIVA LA MICROSEGMENTAZIONE.

In ottica Zero Trust, la microsegmentazione permette di segmentare i singoli processi a livello server e le singole comunicazioni a livello rete, garantendo un miglior controllo delle attività e di prevenire, dunque, attacchi hacker.



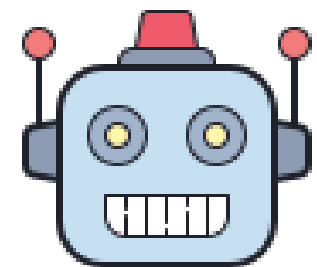
5. SECURITY BY DESIGN.

Per la serie, prevenire è meglio che curare: occorre progettare infrastrutture e applicativi in modo da garantire che la risorsa sia sicura, priva di falle e vulnerabilità.



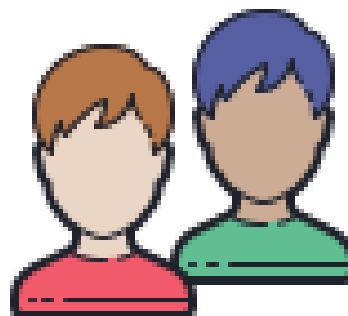
6. L'IT AUTOMATION È TUA AMICA.

Automatizzare i processi di sicurezza permette di garantire un controllo più puntuale delle attività e di liberare risorse (che possono dedicarsi a task a maggiore valore aggiunto).



7. SENSIBILIZZA I TUOI COLLABORATORI.

Con l'emergenza Covid-19 sono aumentati gli attacchi Phishing, Defacements, Bec e tutte quelle tecniche che fanno leva su ansia, fretta e paura. Prepara le tue persone affinché sappiano come comportarsi in tali evenienze.



TI È STATO UTILE QUESTO POST?



Sharing is
Caring

lumit.it