QUOTIDIANO DI SICILIA

Quotidiano

Data 03-04-2020
Pagina 20
Foglio 1

Telelavoro e attacchi cyber, i consigli per proteggersi

ROMA - Nei giorni in cui la pandemia di Coronavirus impone il "distanziamento sociale", Internet e telelavoro sono ormai diventati strumenti indispensabili. Purtroppo però molti lavoratori inesperti - che non immaginavano di doversi adattare così rapidamente a nuove procedure di lavoro - si trovano più che in passato esposti a rischi per la sicurezza dei propri dati, con la prospettiva di danneggiare la produttività di aziende e studi professionali. Questo in un momento in cui si prevede un aumento dei crimini informatici, se non di vere e proprie azioni di cyber terrorismo. Ad evidenziare questo pericolo è il Comitato Italiano Ingegneria dell'Informazione (in sigla C3I), organismo del Consiglio nazionale Ingegneri, che suggerisce alcune soluzioni. Anzitutto l'invito a dotarsi di strumenti di protezione come antivirus, aggiornandoli costantemente, effettuare backup ogni giorno ed evitare di trasmettere informazioni sensibili tramite canali pubblici di file sharing non sicuri.

Se proprio non si dispone di sistemi di condivisione sicuri ,occorre proteggere i propri dati con password più robuste (in rete sono presenti numerosi suggerimenti adatti allo scopo), usare sistemi di crittografia dei messaggi di posta elettronica e fare grande attenzione alle e-mail ingannevoli. Per le aziende occorre dotarsi di sistemi di analisi dei log degli accessi alle applicazioni da parte dei dipendenti, attivare sistemi di monitoraggio dei dati sensibili attraverso Data Loss Prevention, prevedere sistemi di filtraggio per evitare spam e phishing, nonché rafforzare i sistemi di backup. Indispensabile è anche l'aggiornamento continuo del personale dipendente sulle nuove minacce cyber e inviti al rispetto delle regole di policy aziendale in tema di sicurezza informatica.

Superata la fase di emergenza, il C3I suggerisce iniziative di più ampio respiro tra cui: campagne di sensibilizzazione su scala nazionale, attraverso i principali media, per informare sulle minacce informatiche e sui rischi concreti che esse comportano per la vita della collettività. L'istituzione di gruppi di lavoro ad hoc, a livello di Protezione Civile, Difesa e Interno, per l'attuazione di scenari di crisi nel caso di attacchi Cyber su scala nazionale. Un Comitato tecnico strategico che includa, oltre il Dis (Dipartimento informazione sicurezza) e i competenti Ministeri, anche i rappresentanti delle Università, delle Aziende specializzate e degli Ordini professionali, nonché di agenzie europee come Enisa ed Europol.