Rischio informatico e emergenza Covid-19: le contromisure del CNI

Cyberterrorismo e rischio informatico, pronto un vademecum per la fase di transizione da processi di lavoro fisici a modalità immateriali

Il **Coronavirus** ha reso di fatto istantanei un buon numero di **processi aziendali di adattamento allo smart working.** Questi avrebbero richiesto, in condizioni normali,

anni per una transizione funzionale. **Distanziamento sociale e telelavoro** sono due concetti ormai inseparabili l'uno dall'altro. Insieme però al rischio informatico.

I mille rivoli del rischio informatico ai tempi del Coronavirus

Ma il lavoro smart massivo – come tutti i cambiamenti troppo rapidi e troppo gargantueschi – nasconde insidie di cui s'iniziano a intravedere solo ora i contraccolpi tangibili. Aziende dall'anima poco digital e lavoratori non predisposti dal punto di vista professionale e/o dell'esperienza personale pregressa si sono visti costretti a una **digitalizzazione forzata e istantanea.** Questo con **rischi per la privacy individuale** e per la **sicurezza delle reti informatiche** da non trascurare.

Le nuove procedure di lavoro celano criticità per la sicurezza dei **dati aziendali.** I danni – in caso di **data breach** – per imprese e studi professionali potrebbero essere rilevanti quanto quelli che hanno colpito l'economia ad altri livelli meno immateriali. Gli hacker, consapevoli del caotico meltin pot digital venutosi a creare in fretta e furia, potrebbero cogliere l'occasione per **sistematizzare e affinare i propri attacchi**, visto il maggior numero di informazioni sensibili che viaggiano ogni giorno via Internet. In un'epoca in cui la lotta al virus si fa con la resistenza sociale online – in attesa dell'arrivo dell'agognato vaccino – sarebbe scriteriato non trovare **antivirus digital** altrettanto funzionali per la nostra sopravvivenza nell'etere.

Per combattere la minaccia del **cyberterrorismo** il **CNI** – e nello specifico il comitato interno **C3I**, Comitato Italiano Ingegneria dell'Informazione – ha pubblicato un **vademecum contenente le linee di condotta** da adottare in questa difficile fase di transizione da processi di lavoro fisici a modalità immateriali.

CNI e C3I per la sicurezza digitale

Queste le 10 regole per una maggiore **cybersicurezza**:

1. **backup**: effettuare giornalmente il backup dei propri dati;
2. **password**: utilizzare password robuste (almeno 8 caratteri e con caratteri speciali), in particolare quando si condividono dati con l'esterno;
3. **antivirus**: installare sistemi di antivirus sia sui computer che sugli smartphone ed effettuare aggiornamenti costanti;
4. **allegati**: fare attenzione alle email ingannevoli e non aprire allegati sospetti. Cancellare le email a rischio e notificare l'accaduto ai responsabili aziendali per la sicurezza;
5. **social engineering**: fare attenzione agli attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati;
6. **VPN**: usare sempre connessioni sicure (Virtual Private Network) tra il proprio pc e server contenenti dati sensibili;
7. **condivisione**: non usare strumenti di condivisione di dati pubblici (es. WeTransfer); preferire l'utilizzo di cloud privati (Google Cloud, Azure, DropBox) e proteggere sempre i dati con password robuste;
8. **crittografia**: utilizzare strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili;
9. **procedure**: implementare e seguire procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita di

dati);

10. **accessi**: implementare e assicurarsi di tracciare gli accessi (log-in e log-out) degli utenti ai sistemi e postazioni di lavoro.

Le aziende, nello specifico, devono:

- 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**.

Da prevedere anche l'**aggiornamento continuo del personale dipendente** sulle nuove minacce cyber. E un invito costante al rispetto delle **regole di policy aziendale** in tema di sicurezza informatica.

Come affrontare il futuro e il rischio informatico?

Superata la fase emergenziale, il CNI-C3I suggerisce tre iniziative di più ampio respiro:

- **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;
- **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;
- **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.