Cyber attack, Vulnerability Assessment & Penetration, il decalogo per prevenire attacchi informatici

È notizia recente l'attacco "multiplo" alle credenziali e ai dati di molte mail **Pec** di noti professionisti contenenti anche dati sensibili.

L'occasione può essere utile per focalizzarci ancora una volta su tema assai sottostimato e cioè la *cybersecurity*.

Abbiamo già detto che la componente umana è uno dei grimaldelli dei sistemi di sicurezza informatica.

Ribadiamo in questa sede l'importanza di una buona formazione del personale e, d'altro canto, è utile osservare come un sistema di prevenzione *tailor-made* sia l'arma più efficace per problemi simili.

1. Anzitutto dovrebbe essere effettuato un *general assessment* sulle vulnerabilità attuali del sistema.
2. Successivamente sarebbe utile implementare le misure di sicurezza del sistema informatico.
3. Infine sarebbe utile proteggersi con una buona polizza assicurativa contro i rischi di intrusione informatica.

Sotto quest'ultimo profilo è utile verificare che la copertura assicurativa e la relativa assistenza siano effettivamente utili (ad esempio bisognerebbe verificare le definizioni fornite dei vari attacchi informatici, la territorialità della copertura, la durata, le clausole di esclusione ed il

massimale).

I. Ad ogni modo potremo così sintetizzare un decalogo per proteggere il nostro sistema informatico:

1. stabilire la qualità e la consistenza del sistema informatico;
2. effettuare una prima analisi del sistema informatico per individuarne eventuali vulnerabilità;
3. stilare un rapporto sulle vulnerabilità del sistema informatico;
4. aggiornare i sistemi operativi e degli applicativi finalizzati alla protezione del sistema informatico e dei dati informatici (quali ad esempio antivirus, firewall e simili);
5. verificare le connessioni in uscita del sistema informatico;
6. configurare un sistema di ripristino (ad esempio il backup);
7. installare un sistema software finalizzati a limitare le conseguenze di un attacco informatico (ad esempio per gestire un ransomware);
8. stilare un protocollo delle misure di sicurezza attuate e loro aggiornamento (ad esempio gestione, aggiornamento delle password) e stilare un protocollo di gestione di attacco informatico e costituzione di un team dedicato;
9. monitoraggio del funzionamento del sistema di protezione;
10. simulazioni di aggressioni con cadenza programmata.

II. Accanto all'implementazione del sistema informatico è utile o addirittura sovrapponibile un sistema di protezione e gestione dei dati personali.

Sul punto osserviamo che già un sistema di trattamento dei dati conforme alla normativa vigente sarebbe sufficiente a porre in sicurezza il nostro sistema informatico.

Non guasta sul punto applicare lo standard internazionale **ISO 27001.**

Infatti, applicando gli obblighi previsti dal GDPR (oltre al novellato codice) e seguendo le *best practice* ISO 27001 è possibile costruire un sistema integrato di gestione sicura dei dati aziendali.

Sarebbe utile dimostrare particolare sensibilità all'**Audit** con cadenza programmata per identificare le modalità di inosservanza degli obblighi in materia di protezione dei dati personali contenuti nel sistema informatico.

Infine sarebbe utile ipotizzare scenari di ripristino e impatti sul business, creando un sistema di *cyber resilient*.

A questo punto si potrebbe dare origine ad un unico "**ecosistema" di protezione dei dati** sia personali che aziendali capace di sopportare i più comuni attacchi informatici.

Per approfondire

In corso attacco hacker all'Ordine degli Avvocati di Roma (inclusa Virginia Raggi). Password in chiaro e PEC violate

https://www.key4biz.it/cyber-attack-vulnerability-assessment-penetration-il-decalogo-per-prevenire-attacchi-informatici/257107/