Cyber Crime
L’attacco ai nostri sistemi informatici digitali nei momenti di maggiore vulnerabilità e debolezza

Avv. Antonio Bana

In questo particolare contesto i nostri sistemi informatici - da quelli più avanzati a quelli più semplici come il nostro cellulare - risultano maggiormente vulnerabili soprattutto perché il grado di attenzione degli utenti si abbassa a causa di molteplici fattori per i casi di crisi ad esso contingenti.

Basta ricordare che il 60% dei cyber attacchi viene ancora realizzato con il furto delle credenzali o sfruttando le vulnerabilità dei software.

Il Centro Nazionale Anticrimine Informatico ha diramato, già in tempi non sospetti, un alert sulla diffusione del malware (tipologia di software intrusivo inclusi virus informtici, worm, trojan, spyware, ecc...) con riferimento all'epidemia da coronavirus.

Cosa comporta un virus in rete?

Banale a dirsi, ma un danno ingente!

Soprattutto quando veniamo attaccati da campagne massive di messaggi di posta elettronica nella nostra rete aventi ad oggetto file che apparentemente potrebbero essere a noi utili nella loro comunicazione informativa, ma aprendoli avviamo un download che infetta i nostri apparecchi elettronici.

Veniamo in questo modo bombardati da messaggi pseudo rassicuranti che potrebbero indurci ad aprire messaggi di posta contenenti documenti in formato Excel e/o Power Point sfruttando il lato debole e psicologico di molti di noi.

Proprio in questo momento abbiamo inconsapevolmente abbassato queste difese perchè siamo alla ricerca di notizie di conforto e di conoscere il perchè tutto ciò accade.

Si può creare un’altra vulnerabilità nei nostri sistemi informatici anche per il lavoro da remoto
e per l’”intrusione controllata”
nei server aziendali.

L’importanza della norma ISO27001 come strumento di prevenzione e difesa dai rischi informatici.

Bisogna alzare il livello di sicurezza anche attraverso una policy di sicurezza informatica aziendale seria.

Può venirci in aiuto anche l’adozione delle certificazioni come la ISO27001 quale standard internazionale per la sicurezza delle informazioni che è strutturata per essere compatibile con altri sistemi di gestione quali ISO9001 e tecnologicamente indipendente da qualsiasi piattaforma di information technology.

Quali possono essere dei punti fermi in una politica di organizzazione e sicurezza aziendale quale strumento di prevenzione e difesa dai rischi informatici?

- Gestione della sicurezza delle informazioni
- Sicurezza delle attività operative
- Sicurezza delle comunicazioni
- Sicurezza delle risorse umane
- Sicurezza delle attività operative
- Gestione della sicurezza applicativa
- Relazione con i fornitori coinvolti nella gestione della sicurezza delle informazioni
- Trattamento degli incidenti relativi alla sicurezza informatica
- Controllo degli accessi
- Sicurezza fisica ed ambientale

Alla base di queste procedure gestionali si otterrà un vantaggio competitivo soddisfando i requisiti contrattuali dei propri clienti con particolare attenzione alla sicurezza delle loro informazioni.

Questo porterà a gestire regolarmente la valutazione e la gestione dei rischi dell'organizzazione aziendale, formalizzando e proceduralizzando l'organizzazione dei processi della documentazione relativa alla sicurezza dell'apparato informativo in generale.

Grazie per l’attenzione.

Avv. Antonio Bana

Studio Legale Bana