EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Lista di controllo attacchi cibernetici

Misure preventive

1. Sensibilizzare e formare i collaboratori. Questo può avvenire con l'ausilio di test di phishing e di corsi di formazione sulla cibersicurezza.
2. Verificare costantemente la protezione dell'infrastruttura IT. Installare regolarmente patch e aggiornamenti.
3. Eseguire regolarmente backup e controllare il firewall.
4. Utilizzare software anti-malware.
5. Limitare le autorizzazioni per l'installazione di software.
6. Utilizzare password sicure. Cambiare regolarmente le password.
7. Attivare, laddove possibile, l'autenticazione multi-fattore (MFA).
8. **Prestare attenzione** sui Social Media.
9. Utilizzare sempre un **collegamento Internet sicuro** (VPN) e ricorrere in generale la crittografia.

Lista di controllo in caso di attacco cibernetico

1. Innanzitutto **mantenere la calma** e procedere con cautela. Non cedere **mai** alle richieste dei criminali. In caso contrario, l'azienda sarà considerata come un obiettivo lucrativo e potrebbero seguire ulteriori attacchi. Importante! Ogni passo deve essere **documentato** per poter ricapitolare la procedura in un secondo momento.
2. Scollegare immediatamente dalla rete i sistemi infetti. Per farlo, staccare il cavo di rete dal computer ed eventualmente spegnere l'adattatore WLAN disponibile. Avviare misure per impedire la diffusione del potenziale attacco (trasferimento del traffico di rete, filtraggio o blocco del traffico dati e isolamento di parti o di tutta la rete possibilmente compromessa).
3. Informare telefonicamente i **superiori** e il **reparto IT**.
4. Verificare si si tratta davvero di un attacco cibernetico o se è un guasto tecnico. Fino ad allora evitare eventuali comunicazioni verso l'esterno. Se si tratta di un attacco cibernetico, informare la polizia e coinvolgere gli specialisti.
5. Verificare quali sistemi sono coinvolti e scoprire come si è verificato l'attacco. Inoltre è opportuno verificare se e **quali dati** sono stati sottratti e quali reti sono interessate. Controllare quali nodi sono stati compromessi e quali servizi sono stati interrotti e valutare l'estensione e il tipo di danno ai sistemi.
6. In caso di furto di dati sensibili che comportano gravi rischi per la personalità o per i diritti fondamentali delle persone interessate, è necessario informare l'**incaricato federale della protezione dei dati (IFPDT).**
7. Chiudere tutte le falle di sicurezza sfruttate dall'hacker.
8. Informare i **collaboratori** o i **clienti** interessati.
9. Non negoziare in nessun caso con i criminali **senza il supporto della polizia**!
10. Cercare di avviare le misure per il ripristino dei dati e dei sistemi.
11. **Analisi**: in che modo sarebbe stato possibile impedire l'attacco? Quali misure devono essere attuate in futuro?

Data creazione: 20 maggio 2022