Come comportarsi in caso di attacco informatico

Rischi informatici e misure di protezione

Secondo alcuni sondaggi, una PMI su tre in Svizzera ha già subìto un attacco informatico andato a buon fine. Ogni azienda, per quanto piccola, dovrebbe essere consapevole dei rischi della pirateria digitale, come la negazione dell'accesso a risorse informatiche, una grave perdita di immagine dovuta alla pubblicazione di dati rubati o addirittura conseguenze penali in caso di violazione dell'obbligo di diligenza. È quindi fondamentale implementare misure preventive, per esempio configurando o adeguando la propria dotazione tecnica, definendo i processi interni in modo che non possano subire influenze esterne e sensibilizzando il personale. La presente scheda informativa intende invitare i responsabili ad agire.

Indice

Bahnhofstrasse 94, 5000 Aarau
T +41 44 388 53 00
info@jardinsuisse.ch | jardinsuisse.ch

JardinSuisse
Associazione svizzera imprenditori giardinieri
Qui germoglia il futuro.

1. Misure per una protezione efficace dagli attacchi informatici

- Adempiere i compiti manageriali e condividere le responsabilità.
- Eseguire backup esterni regolari (protezione dal furto). Intervallo di tempo: secondo quanto è possibile garantire l'attività senza l'ausilio di applicazioni informatiche.
- Aggiornare regolarmente i software.
- Proteggere l'accesso a internet con un firewall.
- Aggiornare gli antivirus.
- Utilizzare password sicure (almeno dodici caratteri, con lettere maiuscole e minuscole, numeri e simboli) in combinazione con una cassaforte per password e l'autenticazione a due fattori.
- Comunicare le direttive per gli utenti informatici a tutto il personale.
- Classificare i dati e verificare i diritti di accesso.
- Controllare le modifiche ai sistemi di produzione mediante la gestione dei cambiamenti (processo di pianificazione, attuazione e controllo dei cambiamenti nei sistemi informatici per garantire la transizione).
- Proteggere l'infrastruttura IT (p.es. controllo degli accessi, protezione contro le intrusioni).

2. Come riconoscere un attacco informatico

Gli hacker sono scassinatori: cercano di destare meno sospetti possibile e di nascondere le tracce. Spesso, l'intrusione nel sistema da parte di un criminale informatico non è immediatamente riconoscibile, possono passare settimane o addirittura mesi prima che il software dannoso venga attivato.

Segnali di un attacco informatico

- Il sistema è lento.
- I dati non sono accessibili.
- Le password non funzionano più.
- Lo schermo presenta uno sfarfallio.
- Il computer sembra eseguire autonomamente determinate operazioni.
- I programmi non si avviano o non reagiscono correttamente.
- Il computer genera molti messaggi di errore.
- Sullo schermo appare una richiesta di riscatto.

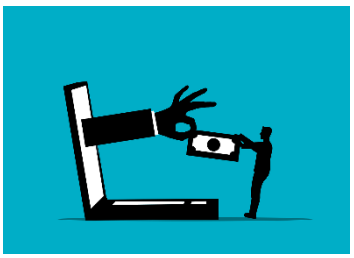
In presenza di segnali di questo genere, occorre reagire tempestivamente. L'elenco non è esaustivo.

3. Come reagire a un attacco informatico

1. Disconnettere immediatamente tutti i sistemi dalla rete e spegnere la WLAN.
2. Informare le persone addette alla sicurezza informatica.
3. Informare il personale.
4. Analizzare il problema e i danni (eventualmente in collaborazione con specialisti).
5. Contattare un'eventuale assicurazione informatica. Le compagnie si avvalgono di partner specializzati che possono fornire sostegno. Nel caso ideale, l'assicuratore copre i costi della pulizia del sistema, del ripristino dei dati e dell'interruzione d'esercizio.

In caso di attacchi di ampia portata, prima di procedere alla pulizia e al ripristino del sistema occorre aspettare che la polizia raccolga le prove. Anche in assenza di danni, è opportuno informare la polizia e il Centro nazionale per la cibersicurezza (https://www.report.ncsc.admin.ch/it/). Benché sia raro che i criminali vengano individuati, la segnalazione può servire a prevenire e sensibilizzare altre potenziali vittime.
Importante: non pagate alcun riscatto! Chi paga una volta, infatti, diventa una vittima interessante per gli hacker.

3.1. I cinque errori più gravi in caso di attacco informatico



- Non scollegare il sistema informatico dalla rete, lasciare la WLAN accesa.
- Non fare niente e aspettare che l'attacco finisca.
- Pagare il riscatto.
- Non informare nessuno per evitare danni alla reputazione.
- Credere che un attacco riguardi solo gli altri e non implementare alcuna misura di sicurezza informatica.

4. Formazioni per sensibilizzare il personale sulla sicurezza informatica

Basta poco: un collaboratore apre distrattamente un'e-mail e di colpo tutta l'azienda è bloccata. È quindi fondamentale informare e sensibilizzare il personale sull'utilizzo di internet e della posta elettronica. Non mancano le formazioni per le aziende, proposte anche da assicurazioni. Alcuni corsi includono pure simulazioni con e-mail di phishing per osservare il comportamento delle e dei dipendenti, e determinare così la necessità di altre misure.

5. Link

Il Centro nazionale per la cibersicurezza (www.ncsc.admin.ch/ncsc/it/home.html) fornisce ragguagli su misure organizzative e tecniche per le aziende.

Fonti: «dergartenbau» numero 20/2023, www.mobiliare.ch