Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Segreteria generale

Centro nazionale per la cibersicurezza NCSC
www.ncsc.admin.ch

NCSC

Telelavoro

Accesso remoto più sicuro

Sommario

1 Introduzione

Le imprese utilizzano sempre più spesso la possibilità di accedere alla rete aziendale dall'esterno. Con questa tecnologia aumenta però anche il rischio di ciberattacchi.
Gli aggressori procedono in modi diversi per accedere alle reti aziendali:

- tentativi di phishing (classico phishing di password o «phishing in tempo reale»[1] nel caso di autenticazione a due fattori);
- attacchi contro le password (attacchi a servizi di elenchi, modifiche di password o attacchi «brute force»);
- attacchi contro gateway non protetti;
- attacchi malware (che spesso passano inosservati se non vi è un protocollo di «tunneling» per tutto il traffico).

2 Contromisure

2.1 Considerazioni sulla disponibilità

L'utilizzo di software per l'accesso remoto deve essere verificato scrupolosamente, perché può portare a un forte sovraccarico della larghezza di banda. Consigliamo di discuterne con il proprio fornitore di servizi Internet e con i propri specialisti IT. Inoltre, aumentare la larghezza di banda non è opportuno se i sistemi «secondari» (ad es. firewall, sistemi di prevenzione delle intrusioni, switch, server ecc.) non sono in grado di gestire il grande traffico di dati.

2.2 Protezione contro malware e phishing

- Utilizzate sempre un'**autenticazione a due fattori** per gli utenti, chiavette USB sicure («cryptostick»), smartcard o «password usa e getta» («one-time password», OTP) come token RSA o Mobile ID. Se non è possibile implementare nessuna di queste opzioni, sono adatte anche soluzioni basate su software come ad esempio Google Authenticator;
- imponete **password forti**; ricordate inoltre agli utenti di utilizzare password diverse per ogni servizio e di evitare le sequenze logiche (ad es. xyz2018, xyz2019, xyz2020);
- monitorate attentamente i file di log dei dispositivi con accesso remoto per individuare eventuali anomalie (ad es. indirizzi IP fuori della Svizzera se la maggior parte del vostro personale lavora in Svizzera, oppure indirizzi IP provenienti da nodi TOR, VPN o in generale da reti di hosting provider);
- imponete un protocollo di **tunneling** per tutti i dispositivi per garantire una comunicazione sicura e tenere d'occhio le connessioni Internet. Tenete presente che questa misura aumenta il carico sulla larghezza di banda;

[1] Rapporto semestrale MELANI 2019/1 n. 4.4.2.: https://www.ncsc,admin.ch/ncsc/it/home/dokumentation/berichte/lageberichte.html

- **sensibilizzate i collaboratori** sulle ciberminacce che incombono anche con il lavoro a domicilio e **fornite** loro **un contatto** a cui segnalare eventuali situazioni sospette;
- pianificate la **disponibilità per analisi forensi**, soprattutto se si consente ai collaboratori di accedere alla rete aziendale dai loro dispositivi;
- assicuratevi che tutti i dispositivi per l'accesso remoto siano **aggiornati** (patch) e definite un **piano per i rollout d'emergenza di patch** in caso di vulnerabilità critiche;
- i dispositivi utilizzati per l'accesso remoto devono poter essere aggiornati anche se non si trovano nei locali dell'azienda;
- assicuratevi che i collaboratori che lavorano da casa non possano **collegare la rete domestica alla rete aziendale**;
- pianificate il ripristino e la sostituzione a distanza dei **dispositivi infetti**, ad esempio tramite una linea DSL/fibra dedicata.
- oltre a queste raccomandazioni specifiche, osservate le misure di protezione contro gli attacchi ransomware pubblicate dall'NCSC [2].

2.3 Sicurezza dei dati

- Assicuratevi di disporre di **backup offline** in caso di attacchi ransomware;
- la salvaguardia dei dati deve essere possibile ed efficace anche quando i collaboratori salvaguardano **dati importanti localmente**.

Se l'utilizzo di dispositivi privati («bring your own decive», **BYOD**) dovesse aumentare, bisogna elaborare delle **istruzioni** per l'utilizzo di questi dispositivi. In particolare, bisogna assicurarsi che i dati aziendali vengano salvaguardati in modo sicuro (ad es. in un contenitore cifrato) in modo che possano essere cancellati definitivamente («wiping»). Questo punto è particolarmente importante nel caso in cui il dipendente intendesse vendere il proprio dispositivo. Va ricordato che i dati salvaguardati su un disco rigido non cifrato possono essere cancellati completamente solo con operazioni supplementari.

2.4 Sensibilizzazione

- Interrompete tutte le **campagne di sensibilizzazione** contro i phishing per evitare allarmismi;
- informate i vostri collaboratori sui **rischi aggiuntivi** e chiedete loro di segnalare all'help desk le e-mail e i siti web sospetti;
- assicuratevi che l'**help desk** disponga di sufficienti **risorse**;
- aiutate i collaboratori a configurare in modo sicuro una **rete WLAN**;
- spiegate ai collaboratori come **contattare l'help desk** e come l'help desk può contattare

[2] https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/ (in inglese)
https://www.ncsc.admin.ch/ncsc/it/home/aktuell/news/news-archiv/sicherheitsrisiko-durch-ransomware.html
https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/as- sets/blocked-filetypes.txt

loro, per evitare di esporli alla truffa «della finta assistenza» («technical support scam», TTS)[3];

- adottate una procedura semplice per **identificare gli utenti** quando chiedono il ripristino della password.

2.5 Diversi

- **Documentate tutte le modifiche** apportate in modo che le versioni precedenti possano essere ripristinate in caso di bisogno;
- assicuratevi che i **compiti amministrativi** che richiedono dei **privilegi elevati** vengano svolti da **dispositivi sicuri** dedicati, dai quali non è possibile accedere a Internet. Se possibile utilizzate istanze server ad hoc;
- se notate **attività di phishing o malware**, segnalatele a www.antiphishing.ch;
- informatevi sulle minacce informatiche attuali utilizzando esclusivamente fonti **affidabili**[4];
- agevolate la **fornitura di strumenti o funzionalità** richiesti in situazioni d'emergenza. Se non potete fornire una soluzione internamente, indicate delle alternative, evitando che i collaboratori cerchino soluzioni individuali difficili da monitorare.

2.6 Riepilogo

La gestione dei rischi e la sicurezza operativa dovrebbero essere adattate rapidamente ai cambiamenti delle minacce e permettere l'introduzione di contromisure adeguate quando i rischi sono considerati elevati. Raccomandiamo di evitare cambiamenti complessi nella situazione attuale e di optare piuttosto per una riduzione del rischio aumentando le capacità di rilevamento. In caso di domande potete rivolgervi a outreach@ncsc.ch.

[3] https://www.ncsc.admin.ch/ncsc/it/home/cyberbedrohungen/fake-support.html
[4] https://www.ncsc.ch; https://twitter.com/GovCERT_CH; https://www.bsi.bund.de/DE/Home/home_node.html; https://www.ssi.gouv.fr/ ecc.