Telelavoro: proteggere l'accesso remoto

NCSC

Versione:	v 1.0
Autore:	NCSC
Ultimo aggiornamento:	24 marzo 2020

Introduzione

In considerazione dell'aumentato utilizzo di soluzioni di accesso remoto per il telelavoro, è opportuno rammentare alcune *best practice* per ridurre al minimo il rischio associato a queste tecnologie. Riteniamo che i rischi aumentino con la crescita dei differenti accessi remoti. Gli aggressori conoscono la situazione attuale e tentano di ottenere l'accesso alla rete di organizzazioni in diversi modi:

- tentativi di phishing (sia che si tratti del classico phishing di password o del cosiddetto phishing in tempo reale[1] nel caso di autenticazione a due fattori);
- attacchi contro le password (attacchi al dizionario, di password spraying o attacchi brute force);
- attacchi contro dispositivi gateway non aggiornati;
- attacchi malware (che spesso non vengono rilevati se non viene effettuato un tunneling di tutto il traffico)

Contromisure

Considerazioni sulla disponibilità

L'utilizzo di soluzioni di telelavoro può portare ad un notevole aumento della larghezza di banda. È consigliato discuterne con il proprio fornitore di servizi di telecomunicazione e con la squadra interna. Aumentare la larghezza di banda potrebbe non essere sufficiente. Infatti anche i cosiddetti dispositivi *downstream* (ad esempio firewall, sistemi di prevenzione delle intrusioni, ma anche switch o server) possono subire un sovraccarico se le loro capacità non vengono adattate alle attuali necessità.

Misure contro malware e phishing

- Utilizzate sempre un'autenticazione forte, cioè con almeno **due fattori d'autenticazione** per i vostri utenti. Le soluzioni migliori sono una chiavetta USB (Cryptostick), una Smartcard, un token OTP ("*one time password*") basato su hardware come RSA o un MobileID. Se non è possibile implementare nessuna di queste opzioni, si prestano anche i token OTP basati su software come Google Authenticator.
- Implementate e fate rispettare le **buone prassi in materia di password**. In particolare ricordate agli utenti di non riutilizzare le password per differenti servizi e di evitare le sequenze di password (ad es. xyz2018, xyz2019, xyz2020).

[1] Vedi Rapporto semestrale 2019/1, cap. 4.4.2, https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2019-1.html.

- **Monitorate** attentamente i **log degli accessi** remoti per individuare eventuali anomalie (ad es. indirizzi IP al di fuori della Svizzera se la maggior parte del vostro staff lavora in Svizzera oppure Indirizzi IP provenienti da nodi TOR, VPN o in generale da reti di hosting provider).
- Effettuate un **tunnel VPN** per tutti i dispositivi al fine di rendere sicura la comunicazione e di mantenere la visibilità delle connessioni verso Internet. Tenete però presente che questa misura aumenterà notevolmente i requisiti di larghezza di banda.
- **Informate gli utenti** riguardo ai pericoli del telelavoro e **fornite** loro **un contatto** a cui segnalare eventuali situazioni sospette.
- Abbiate pronti dei **piani di analisi forense**, soprattutto se si consente agli utenti di accedere alle risorse aziendali dal proprio dispositivo.
- Assicuratevi che tutti i dispositivi per l'accesso remoto siano **aggiornati** e definite un **piano per gli aggiornamenti d'emergenza** ("*emergency patch roll-out*") in caso di vulnerabilità critiche.
- Assicuratevi che tutti i dispositivi utilizzati per l'accesso remoto possano venir aggiornati senza essere fisicamente sul posto, preferibilmente al di fuori delle ore di lavoro e rispettando la larghezza di banda disponibile.
- Assicuratevi che gli utenti in telelavoro non colleghino la propria **rete domestica** con la rete aziendale.
- Pianificate il ripristino/sostituzione a distanza dei **dispositivi infetti**, ad esempio tramite una linea dls/fibra dedicata.

Oltre queste raccomandazioni vi segnaliamo i documenti relativi alla protezione contro li attacchi ransomware mirati che abbiamo pubblicato recentemente:

- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes
- https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/sicherheitsrisiko-durch-ransomware.html
- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

Sicurezza dei dati

- Assicuratevi di disporre di **backup offline** in caso di un attacco ransomware.
- Assicuratevi che le soluzioni di backup funzionino correttamente e siano efficaci anche nel caso in cui gli utenti inizino a **memorizzare localmente** i dati importanti.
- Nel caso in cui a causa della situazione dovesse aumentare l'utilizzo di dispositivi privati (**BYOD**), mettete a punto delle **linee guida** per l'utilizzo di questi dispositivi. In particolare assicuratevi che i dati appartenenti all'organizzazione siano memorizzati in modo sicuro (ad esempio in un contenitore cifrato) in modo che possano essere can-

cellati efficientemente se necessario, ad esempio se il dipendente intendesse rivendere il proprio dispositivo. Ricordiamo che i dati memorizzati su un disco rigido non cifrato possono essere cancellati completamente solo con uno sforzo supplementare.

Sensibilizzazione

- Interrompete tutte le **campagne di sensibilizzazione** contro i phishing per ridurre le perturbazioni.
- Informate i vostri utenti dei **rischi aggiuntivi** e chiedete loro di segnalare al vostro help desk qualsiasi email o sito web sospetto.
- Assicuratevi che l'**help desk** disponga di sufficienti **risorse**.
- Istruire i vostri utenti su come configurare in modo sicuro una **rete WiFi**.
- Istruire gli utenti su come **contattare l'help desk** e su come l'help desk può contattarli, per evitare di esporli alla truffa del finto supporto[2].
- Mette in pratica una procedura semplice per **identificare gli utenti** quando richiedono il reset della password.

Diversi

- **Documentate tutte le modifiche** apportate durante la situazione di emergenza in modo che possano essere ripristinate quando la situazione lo permette.
- Assicuratevi che i **compiti amministrativi** che richiedono dei privilegi elevati vengano svolti da **dispositivi sicuri** che non siano autorizzati a navigare contemporaneamente in Internet. Utilizzate se possibile istanze server dedicate.
- Se notate **attività di phishing o malware**, segnalatele a www.antiphishing.ch.
- **Informatevi** riguardo alle attuali minacce informatiche utilizzando esclusivamente fonti affidabili, come https://www.ncsc.ch , https://www.govcert.ch o https://twitter.com/GovCERT_CH, https://www.bsi.bund.de/DE/Home/home_node.html, https://www.ssi.gouv.fr/.
- Facilitate le **richiese di funzionalità e di strumenti** ("*feature and tool request*") al vostro help desk. Se non potete fornire una soluzione interna, è raccomandabile fornire le istruzioni per una soluzione alternativa, evitando che i dipendenti cerchino soluzioni individuali che rendano impossibile il monitoraggio.

[2] Finte chiamate di supporto tecnico: https://www.melani.admin.ch/melani/it/home/themen/fake_support.html.

Conclusione

La gestione dei rischi e la sicurezza operativa dovrebbero adattarsi rapidamente al mutato scenario attuale. Adottate le contromisure adeguate in particolare quando i rischi sono considerati elevati. Raccomandiamo di evitare cambiamenti complessi nella situazione attuale ma piuttosto di ridurre il rischio aumentando le capacità di rilevamento. Se avete delle domande, non esitate a rivolgervi a outreach[at]ncsc.ch.