Home-Office: Sicherer Umgang mit Fernzugriffen

NCSC

Version:	v 1.0
Autor:	NCSC
Zuletzt aktualisiert:	24 März 2020

Einleitung

Aufgrund der momentan sehr hohen Nutzung von Fernzugriffen möchten wir Sie an einige Grundsätze erinnern, um die Risiken im Umgang mit dieser Technologie zu minimieren. Mit der vermehrten Nutzung von Fernzugriffen in Unternehmensnetzwerke dürften diese Risiken stark zunehmen. Die Angreifer könnten die aktuelle Situation dazu nutzen, um mit verschiedenen Vorgehensweisen Zugriff auf Unternehmensnetzwerke zu erhalten:

- Phishingversuche (klassisches Passwort-Phishing resp. so genanntes «Echtzeit-Phishing [1]» bei Zwei-Faktor-Authentifikationen).
- Angriffe auf Passwörter (Angriffe auf Verzeichnisdienste, Ändern von Passwörtern, Brute Force).
- Angriffe auf ungesicherte Gateways.
- Angriffe mit Malware (diese bleiben häufig unentdeckt, wenn kein Tunnelling des gesamten Verkehrs eingerichtet ist).

Gegenmassnahmen

Überlegungen zur Verfügbarkeit

Der Einsatz von Fernzugriffssoftware kann zu einer starken Belastung der Bandbreiten führen. Besprechen Sie die Anforderungen mit Ihrem ISP und Ihren internen IT-Spezialisten. Eine Erhöhung der Bandbreite ist nicht zielführend, wenn nachgeschaltete Systeme (Firewalls, Intrusion Prevention Systeme, Switches, Server usw.) mit dem erhöhten Datenverkehr nicht umgehen können.

Schutz vor Malware / Phishing

- Verwenden Sie einen **zweiten Faktor** für die **Benutzerauthentifizierung**. Kryptosticks, Smartcards oder hardwarebasierte Einmalpasswörter (OTP) wie RSA-Tokens oder MobileID gelten hier als gute Lösungen. Sollten solche Lösungen nicht realisierbar sein, eignen sich auch software-basierte Lösungen wie beispielsweise der Google Authenticator.
- Erzwingen Sie die **Verwendung von starken Passwörtern** und erinnern Sie die Benutzer daran, für jeden Dienst ein separates Passwort zu verwenden sowie auf «Sequenzen» in Passwörtern zu verzichten (z.B. Passwort1, Passwort2 usw.).
- **Prüfen** Sie die **Logdaten** Ihrer Geräte mit Fernzugriff laufend auf Anomalien (z.B. ausländische IP-Adressen, wenn die meisten Mitarbeitenden in der Schweiz tätig

[1] Siehe MELANI Halbjahresbericht 2019/1 Kapitel 4.4.2., https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html

sind; IP-Adressen aus TOR Netzwerken; VPN oder generell Netzwerke von Hosting Providern).

- Erzwingen Sie ein **Tunneling** für alle Geräte, um die sichere Kommunikation zu gewährleisten und Verbindungen ins Internet sichtbar zu machen. Denken Sie daran, dass diese Massnahme die Belastung der Bandbreite entsprechend erhöht.
- **Sensibilisieren** Sie die **Mitarbeitenden** bezüglich Gefahren von Home-Office und **kommunizieren** Sie **Kontaktinformationen** für den Fall, dass die Mitarbeitenden etwas Verdächtiges feststellen.
- Planen Sie die **Bereitschaft für forensische Analysen**, insbesondere, wenn Sie Mitarbeitenden erlauben, mit ihren privaten Geräten auf das Unternehmensnetzwerk zuzugreifen.
- Stellen Sie sicher, dass alle für den Fernzugriff verwendeten Geräte auf dem **neuesten Stand** sind (Patches) und planen Sie den **notfallmässigen Rollout von Patches** im Falle von kritischen Sicherheitslücken.
- Die Aktualisierung der für den Fernzugriff verwendeten Geräte muss ohne physische Präsenz im Unternehmen möglich sein.
- Stellen Sie sicher, dass von zuhause aus arbeitendes Personal **keine Verbindung** zwischen **privatem** und **Unternehmensnetzwerk** herstellen kann.
- Planen Sie das Neuaufsetzen/Ersetzen von **infizierten Geräten** mittels Fernzugang, z.B. über dediziertes DSL/Glasfaser.

Abgesehen von diesen eher spezifischen Empfehlungen weisen wir Sie auf die kürzlich publizierten Schutzmassnahmen gegen Ransomware-Angriffe hin:

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

Datensicherheit

- Stellen Sie die Verfügbarkeit von **Offline Backups** im Falle von Ransomware Angriffen sicher.
- Die Datensicherung muss auch möglich und wirksam sein, wenn Mitarbeitende **wichtige Daten lokal** abspeichern.
- Sollte aufgrund der aktuellen Situation die Verwendung privater Geräte («*Bring your own device*» **BYOD**) zunehmen: Erstellen Sie **Anweisungen für den Umgang** mit diesen Geräten. Insbesondere ist darauf hinzuweisen, dass Unternehmensdaten sicher gespeichert werden (z.B. in einem verschlüsselten Container), so dass diese Daten später komplett gelöscht werden können («*wiping*»). Das ist besonders dann

wichtig, wenn die betreffende Person ihr privates Gerät später verkaufen will. Denken Sie daran, dass auf einer unverschlüsselten Festplatte gespeicherte Daten (wenn überhaupt) nur mit grossem Zusatzaufwand komplett gelöscht werden können.

Sensibilisierung

- Stoppen Sie alle **Phishing Awareness Kampagnen**, um Unruhe zu vermeiden
- Informieren Sie Ihre Mitarbeitenden über **zusätzliche Risiken** und fordern Sie die Mitarbeitenden auf, verdächtige E-Mails und/oder Websites Ihrem Helpdesk zu melden.
- Stellen Sie sicher, dass der **Helpdesk** entsprechend personell besetzt ist.
- Unterstützen Sie Ihre Mitarbeitenden bei der sicheren Konfiguration von **WLAN-Netzwerken.**
- Instruieren Sie Ihre Mitarbeitenden, wie diese den **Helpdesk kontaktieren** sollen und erläutern Sie, wie der Helpdesk die Mitarbeitenden kontaktiert. So vermeiden Sie die Gefahr, auf «Fake-Support»-Anrufe [2] hereinzufallen.
- Stellen Sie eine einfache Vorgehensweise sicher, um **Benutzer zu identifizieren**, wenn diese eine Rücksetzung des Passworts verlangen.

Verschiedenes

- **Dokumentieren Sie alle Veränderungen**, die Sie während der Notlage in die Wege geleitet haben. So stellen Sie sicher, dass sich diese Veränderungen einfach rückgängig machen lassen, wenn sich die Lage normalisiert.
- **Hoch privilegierte administrative Tätigkeiten** dürfen nur von speziell **gesicherten Geräten** aus erledigt werden, die keinen weiteren gleichzeitigen Internetzugriff erlauben. Verwenden Sie wenn möglich dedizierte Serverinstanzen.
- Wenn Sie **Phishing- oder Malware Aktivitäten** feststellen, melden Sie diese bitte an www.antiphishing.ch
- Verwenden Sie ausschliesslich **vertrauenswürdige** Quellen, wenn Sie sich über Cyberbedrohungen informieren wollen, wie z.B. https://www.ncsc.ch, https://www.govcert.ch oder https://twitter.com/GovCERT_CH, https://www.bsi.bund.de/DE/Home/home_node.html, https://www.ssi.gouv.fr/.
- Erleichtern Sie die **Auslieferung von Tools oder Features**, welche in Zusammenhang mit der Notlage angefragt werden. Können Sie keine unternehmenseigene Lösung anbieten, zeigen Sie mindestens alternative Lösungswege auf. Vermeiden Sie, dass die Mitarbeitenden individuelle Lösungswege suchen, die ein Monitoring verunmöglichen.

[2] Gefälschte Supportanrufe: https://www.melani.admin.ch/melani/de/home/themen/fake_support.html

Zusammenfassung

Risikomanagement und operationelle Sicherheit sollten sich schnell an die veränderte Bedrohungslage anpassen lassen und angemessene Gegenmassnahmen ermöglichen, wenn Risiken als kritisch hoch beurteilt werden. Nehmen Sie in der aktuellen Situation keine komplexen Änderungen vor, sondern stellen Sie die Risikominimierung mit erhöhten Detektionsfähigkeiten sicher. Bei Fragen kontaktieren Sie bitte outreach[at]ncsc.ch.