Anlage

Technische Voraussetzungen für Netzwerkkopplungen

Medizinische Universität Lausitz – Carl Thiem

Version 2.0 (Review und Integration PAM-Lösung)

Inhaltsverzeichnis

1 Grundlagen

Aktuell bestehen folgende Möglichkeiten der Verbindung mit dem CTK-Netzwerk zu Fernwartungszugriffen

- Remote - Access via Privilege Access Management (PAM) -Lösung der MUL-CT
- Remote - Access VPN-Verbindung via Checkpoint-Client
- Site2Site VPN-Verbindung via IPSEC
- Fernwartungswerkzeug – vgl. zugelassener Anbieter

Grundlegend dürfen nur anerkannte und als sicher geltende Verfahren und Verschlüsselungsmethoden verwendet werden.

Alle Verbindungen MÜSSEN verschlüsselt erfolgen.

Für die verschiedenen Verfahren gelten verschiedene Voraussetzungen, welche durch den Netzwerkpartner einzuhalten sind.

2 Remote - Access via Privilege Access Management - Lösung

Die Medizinische Universität Lausitz – Carl Thiem MUSS den Zugang für Dritte kontrolliert und nach dem Least-Privilege – Prinzip umsetzen und setzt eine PAM-Lösung ein.

Diese PAM-Lösung MUSS vorrangig der Zugangslösungen per VPN C2S oder S2S betrachtet werden.

Für den externen Zugriff auf privilegierte IT-Ressourcen des MUL-CT gilt:

- Verpflichtung zur 2FA – Absicherung des Zugangs
- jede Aktion wird aufgezeichnet und protokolliert
- Zugang nur nach Freigabe oder in definierten Zeiträumen
- Zugang nur zu definierten IT-Ressourcen
- Grundsätzlich erfolgt der Zugang per Webschnittstellen oder speziellen Applikationen

Ein Zugang per RDP oder SSH **DARF NUR** in begründeten / technisch bedingten Einzelfällen erfolgen.

3 Remote - Access VPN-Verbindung via Checkpoint-Client

- Die Authentifizierung erfolgt nach telefonischer Freischaltung und Autorisierung der Verbindung beim CTK-Helpdesk.
- Es MUSS der vom CTK gestellte VPN-Client verwendet werden.
  Dieser kann unter der URL https://www.checkpoint.com/quantum/remote-access-vpn/#downloads jeweils vorab durch den Netzwerkpartner abgerufen und bis zu einer eventuellen Aktualisierung verwendet werden.
- Der VPN-Client ist im Checkpoint-Mobile-VPN Modus zu verwenden (installieren).
- Die Authentifizierungsmethode ist Username und Passwort (nur nach telefonischer Autorisierung).
- Die Verbindung erfolgt über den Gateway-Hostnamen sslvpn.ctk.de.
- Die Vertrauenswürdigkeit des Zertifikates MUSS bei der Einrichtung sichergestellt werden.

SHA256-Fingerabdruck:
28:56:50:C5:35:3E:37:D7:EE:87:9B:D1:74:CD:25:97:FA:7E:DF:0F:6B:28:82:E8:07:32:64:B6:C4:B6:DE:5C

- Eine TLS-Interception der Verbindung darf nicht stattfinden.
- Die Netzwerk-und Firewallsysteme des Netzwerkpartners MÜSSEN die Übertragung von UDP Kommunikation auf den Ports 500 und 4500 sowie AH und ESP-Traffic, sowie HTTPS-Traffic zu den Systemen sslvpn.ctk.de und vpngate.ctk.de zulassen.

4 Site2Site VPN-Verbindung via IPSEC

Dauerhafte Verbindungen für Systemkopplungen, Verbindung in beides Richtungen und Verbindungen zu Systemen, auf welchen aus technischen Gründen die Ausführung des Checkpoint-Clients nicht möglich ist, können als Site2Site IPSEC-Tunnel etabliert werden.
Änderungen an den vereinbarten Parametern sind mit mindestens drei Wochen Vorab mit dem CTK abzustimmen und in dem zugehörigen Formular zu erfassen.
Dabei sind folgende Mindeststandards VERBINDLICH.

- Die Verbindung erfolgt nur zu einer statischen IPV4-Adresse des Partners
- Die Empfehlungen der BSI-TR-02102-3 sind jeweils auch in aktualisierten Fassungen, einzuhalten.
- ausschließlich IKEv2 Anwendung
- Perfect Forward Secrecy etabliert
- IKE/PH1:
    - mindestens AES128
    - Integritätsprüfung SHA256 oder besser
    - Rekeying mindestens einmal pro 24h
- IPSEC/PH2
    - Verschlüsselung mindestens AES128 (CBC, GCM)
    - Integritätsprüfung SHA256 oder besser
    - Nur Tunnelmodus, kein Transportmodus
    - Rekeying mindestens einmal pro 4h
- DH-Schlüsselaustausch
    - ab Gruppe 19 oder höher
    - unterstützt sind derzeit 19 und 20

Das CTK teilt dem Netzwerkpartner eine RFC-1918-IP-Adresse zu. Dabei kommen Adressen aus den Bereichen 192.168.138.0/24 oder 192.168.183.0/24, 10.51.0.0/24, 10.50.0.0/16 nach Wahl des Netzwerkpartners zum Einsatz. Ist aus technischen Gründen die Verwendung mehrerer IP-Adressen notwendig, kann die Zuteilung eines /24-Netzwerkes aus dem Bereich 10.50.0.0/16 erfolgen.

Der Netzwerkpartner verwendet die zugeteilte IP-Adresse und muss allen Traffic auf und von dieser IP-Adresse übersetzen.

Auf der Seite des Netzwerkpartners sind entsprechende Übersetzungen einzurichten oder die IP-Adressen, wie zugeteilt, zu nutzen. Alternativ kann der Netzwerkpartner ihm oder seinem Provider durch das RIPE zugeteilte IP-Adressen benennen.

Auf der CTK Seite kommen IP-Adressen aus dem Bereich 172.16.0.0/19 zur Anwendung. Der Netzwerkpartner erhält vom CTK eine Prinzipskizze bzw. benannte Kommunikationsendpunkte. Die die Zieladressen umgebenden /24 Netzwerkblöcke müssen vom Netzwerkpartner der Encryption-Domain hinzugefügt werden. Insofern beim Netzwerkpartner die Verwendung der entsprechenden Adressen ausgeschlossen ist, kann ein NAT auf Seite des CTK eingerichtet werden, dazu ist eine Auswahl zu treffen.

Die Kommunikationsbeziehungen sind vor Einrichtung der VPN-Verbindung abzustimmen und auf Seite des CTK zu dokumentieren.

Für die Einrichtung der IPSec-Site2Site-Verbindung muss durch den Netzwerkpartner das Formular zur Beantragung eines VPN-Zugangs ausgefüllt werden, in welcher die verwendeten Parameter erfasst werden.

Systeme, welche dauerhafte Schnittstellen via VPN-Verbindung für einen Netzwerkpartner bereitstellen werden in einer DMZ aufgestellt bzw. über einen Proxyserver in der DMZ verfügbar gemacht (PAP-Struktur).

Das CTK baut die IPSec-Verbindung von der Gateway-Adresse 212.111.231.2 auf.

5 Verwendung eines zugelassenen Fernwartungswerkzeugs

Der Dienstleister kann ein Fernwartungswerkzeug unter Berücksichtigung der folgenden Voraussetzungen und Freigaben einsetzen.

Voraussetzungen:

- Es ist keine dauerhafte Installation von Software auf dem jeweiligen System notwendig bzw.
- ein Zugriff auf das System ist nur nach Freigabe im Einzelfall möglich.
- Sämtliche Verbindungen erfolgen verschlüsselt.
- Verschlüsselung erfolgt nach Stand der Technik orientiert an BSI TR-02102-1 in der jeweils aktuellen Fassung.
- Softwarelizenzen MÜSSEN und Softwarepakete SOLLTEN durch den Netzwerkpartner/Dienstleister gestellt werden.
- Es darf nur ein vertrauenswürdiger und EU-DSGVO-konformer Anbieter genutzt werden.
- Anbieter, welche durch das CTK bisher nicht geprüft wurden, benötigen die vorherige Genehmigung durch das CTK. Die erforderlichen Kommunikationsbeziehungen MÜSSEN in diesem Fall vorab nach Ziel (Domain, IP, URL), Port, Protokoll benannt werden.

Derzeit sind folgende Anbieter im CTK bereits geprüft:

- TeamViewer
- Bomgar
- AnyDesk
- GoToAssist