Remote Access/Fernwartung

Problembeschreibung und Ursache

Externe Zugänge zu OT-Netzwerken sind für Wartungszwecke weit verbreitet. Leider sind diese Zugänge aber mit geringer Sicherheit ausgestattet, so sind Default-Zugänge mit Standard-Passwörtern oder fest kodierten Passwörtern in vielen OT-Netzen noch vorhanden. Auch wenn der Zugang zum OT-Netz über VPN geregelt ist, ist dieser Zugang oft nicht beschränkt, d.h. man kann über einen Wartungszugang für ein bestimmtes System auf weitere Systeme zugreifen, die nicht für den Zweck des Zugangs vorgesehen sind. Die zentralen Ursachen für dieses Problem sind mangelnde Authentisierung und Autorisierung, sowie flache Netzwerkhierarchien (wurde bereits im Level Netzwerksegmentierung behandelt). Zudem stellt die Einbeziehung von externen Dienstleistern eine Herausforderung für das Sicherheitsmanagement dar, da die Sicherheitskonzepte mehrerer Parteien übereinstimmen müssen.

Bedrohungsszenarien

Externe Zugänge für Remote Access sind sehr riskant und können selbst bei höchsten Sicherheitsvorkehrungen trotzdem eine Gefahr darstellen. Daher wird zur Verwendung/Implementierung von Remote Access im OT-Netzwerk grundsätzlich abgeraten und sollte daher nur bei absoluter Notwendigkeit umgesetzt werden. Die Bedrohungen können in direkte und indirekte Angriffe unterteilt werden. Direkte Angriffe auf Wartungszugänge erfolgen z.B. über Brute-Force-Attacken auf passwortgeschützte Zugänge, über Wiederverwendung von zuvor aufgezeichneten Tokens oder über web-spezifische Angriffe auf Zugänge, die zu Wartungszwecken verwendet werden. Indirekte Angriffe erfolgen über IT-Systeme des Dienstleisters, für den der externe Zugang geschaffen wurde, z.B. mithilfe eines Trojaners, durch Diebstahl eines Passworts oder durch die Verwendung von gestohlenen Notebooks, auf denen eine Software für den externen Zugriff konfiguriert ist.

Gegenmaßnahmen und Sicherheitsvorkehrungen

Im Folgenden wird aufgelistet, welche Maßnahmen man ergreifen sollte, um einen Remote Access so gut wie möglich abzusichern.

Allgemeine Gegenmaßnahmen

- Standardnutzer/-passwörter eines Herstellers sperren/löschen
- Nutzung von sicheren Authentisierungsverfahren wie z. B. Pre-Shared-Keys, Zertifikate, Hardwaretoken, Einmalpasswörter und Mehr-Faktor-Authentisierung durch Besitz und Wissen
- Schutz des Übertragungsweges durch Verschlüsselung, z.B. mit SSL/TLS
- Netzwerksegmentierung zur Minimierung der „Reichweite“ von Fernzugängen

- Einrichtung von Zugriffspunkten für Fernwartung in einer demilitarisierten Zone (DMZ), sodass sich Dienstleister statt ins ICS-Netz zunächst in eine DMZ verbinden und von dort ausschließlich den benötigten Zugriff auf das Zielsystem erhalten
- Fernzugänge müssen immer über eine Firewall geführt werden, die den Zugang zum Zielsystem erteilt und überwacht
- Freischaltung von Fernzugängen durch internes Personal nur für die Dauer und den Zweck der Fernwartung
- Protokollierung von Fernzugriffen zur Gewährleistung der Nachvollziehbarkeit, diese Logdaten auswerten und archivieren
- Alle Zugänge sind zu personalisieren, d. h. Verzicht auf Funktionskonten, die von mehreren Personen benutzt werden
- Durchführung von Audits für solche Systeme / Zugänge

Fernzugriffsanwendungen

Die Fernzugriffsanwendung wird am Ende diejenige Software sein, die die Fernanmeldung an Arbeitsstationen und Geräten ermöglicht. In der Vergangenheit wurden diese Anwendungen oft mit nicht ausreichender Sicherheit entwickelt. Daher sollte die Fernzugriffsanwendung vor der Verwendung im ICS auf ihre Sicherheit überprüft werden.

Fernzugriffsverbindungen

Bei der Verwendung von Remote-Access sollte sichergestellt werde, dass alle Fernzugriffsverbindungen autorisiert, authentifiziert, verschlüsselt und dokumentiert sind. Die Dokumentation muss dabei folgendes umfassen:

- Zweck
- verwendete Fernzugriffsanwendung
- verwendete Verschlüsselungs- und Authentifizierungs Technologien
- wie die Verbindung hergestellt werden soll
- die Umstände, die die Verbindung erfordern
- die Länge der Zeit, in der die Verbindung offen sein muss, einschließlich erwarteter Inaktivitätsperioden
- den Standort und die Identität des dezentralen Client-Geräts, der Anwendung und des Benutzers

Die Gefahr bei mangelnder Autorisierung und Authentifizierung besteht darin, dass ein Laptop, der mit Schadsoftware infiziert ist, das ICS angreifen/infizieren kann. Um dies zu vermeiden, sollten Verfahren zur Beantragung einer Fernzugriffsverbindung zwischen einem Client und einem Server, sowie ein Validierungs- und Genehmigungsverfahren für die Verbindung auf der Grundlage ihrer erwarteten Nutzung umgesetzt werden.

Beenden des Fernzugriffs

Ein wichtiger Punkt, der nicht zu vernachlässigen ist, ist das Beenden des Fernzugriffs. Genauso wie ein PC bei Verlassen des Raums nicht offen gelassen werden soll, darf ein

Fernzugriff bei Inaktivität ebenfalls nicht offen gelassen werden. Dies birgt ein unnötiges Risiko, da ein Angreifer diesen Zugang unbemerkt ausnutzen kann. Daher sollten Fernzugriffsverbindungen ab einer bestimmten Inaktivitätsperiode automatisch abgebaut werden, und zudem sollte die Verbindung nur für einen bestimmten Zeitraum zugelassen sein.

Methoden zur Umsetzung von Remote Access

Es gibt unterschiedliche Arten, wie man einen Remote Access einrichtet, welche unterschiedliche Sicherheitsniveaus haben. Bei der unsicheren Variante sind OT- und IT-Netz miteinadner verbunden, getrennt mit einem Zugang über eine Firewall. Warum diese Variante unsicher ist, wurde bereits im Level Netzwerksegmentierung behandelt. Die sichere Variante läuft folgendermaßen ab: Zuerst verbindet man sich über einen VPN in die IT-DMZ, über der man dann Zugang zu einem Jump-Client in der OT-DMZ erhält. Das OT-DMZ bietet dann den direkten Zugang zum ICS. Dieser Prozess bietet die maximal mögliche Sicherheit und Kontrolle über den Fernzugriff.

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente SPE3 - Netzwerk- und Kommunikationssicherheit: NET3 - Sicherer Fernzugriff, einem Dokument des BSI über Top 10 Bedrohungen und Gegenmaßnahmen für ICS (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1), sowie einer Präsentation von William Perez, Connecticut Water Co. (https://www.youtube.com/watch?v=YBS6B3HfqIo)