Sicherheit bei Remotezugriffen auf OT-Geräte

Remotezugriffe auf OT-Geräte eröffnen viele potenzielle Angriffspunkte für Cyberattacken. Um die OT-Systeme effektiv zu schützen, ist eine umfassende Sicherheitsstrategie erforderlich, die verschiedene Schutzmechanismen kombiniert.

Quelle: BOLL Europe

Die Covid-19-Pandemie hat weltweit zu erheblichen Veränderungen geführt, insbesondere im Bereich der Arbeitspraktiken. Organisationen waren gezwungen, ihre Geschäftsprozesse anzupassen, um den Anforderungen des Lockdowns gerecht zu werden. Für Unternehmen, die operative Technologie (OT) nutzen, war der Remotezugriff auf OT-Geräte eine entscheidende Massnahme, um die Kontinuität ihrer Geschäftsabläufe sicherzustellen. Obwohl der Remotezugriff zweifellos Vorteile bietet, birgt er auch erhebliche Risiken. Dieser Artikel untersucht die Sicherheitsprobleme im Zusammenhang mit dem Remotezugriff auf OT-Geräte und stellt Lösungsansätze wie Privileged Access Management (PAM), Virtual Private Network (VPN) und Zero Trust Network Access (ZTNA) vor, um einen sicheren Fernzugriff zu gewährleisten.

Bild: istock.com

Die Sicherheit von OT-Systemen ist von entscheidender Bedeutung, doch der Remotezugriff auf OT-Geräte eröffnet viele potenzielle Angriffspunkte für Cyberangriffe.

OT-Sicherheit ist Pflicht

Die Sicherheit von OT-Systemen ist von entscheidender Bedeutung, da sie häufig kritische Infrastrukturen wie Energieversorgung, Transport- und Fertigungseinrichtungen unterstützen. Der Remotezugriff auf OT-Geräte eröffnet jedoch viele potenzielle Angriffspunkte für Cyberangriffe, die schwerwiegende Folgen haben können.

Zu den wichtigsten drei Angriffsvektoren zählt unter anderem eine schwache Authentifizierung. Unzureichende oder unsichere Authentifizierungsmechanismen ermöglichen es Angreifern, Zugriff auf OT-Geräte zu erlangen. Dies kann zu unbefugten Manipulationen der Geräte oder sogar zur Sabotage der betroffenen Systeme führen. Schwache Passwörter oder fehlende Multi-Faktor-Authentifizierung öffnen Tür und Tor für Angreifer. Andererseits ist es oft auch gar nicht möglich, auf teils jahrzehntealten Anlagen moderne Methoden zur Authentifizierung zu implementieren. Eine adäquate Authentifizierung erfolgt dann meist über den Netzwerkzugriff selbst.

Die Abschottung des gesamten Netzwerkes hilft auch beim zweitwichtigsten Einfallstor: der unverschlüsselten und meist einfach aufgebauten Kommunikation im OT-Umfeld. In offenen Netzwerken ist es möglich, Abhörversuche und Datenmanipulation durchzuführen. Somit haben Angreifer die Möglichkeit, vertrauliche Informationen zu stehlen oder schädli-

chen Code einzuschleusen. Die Zugangskontrolle ist daher von entscheidender Bedeutung – sobald ein Zugriff von extern erfolgen soll, muss die gesamte Kommunikationskette bis zum zugreifenden Endgerät verschlüsselt werden.

Sobald das Netzwerk nach «aussen» geöffnet wird, sind der Zeitpunkt und die Häufigkeit des Zugriffs nicht mehr durch die physikalischen Barrieren regel- und kontrollierbar. Remotezugriffslösungen sollten daher eine umfassende Überwachung und Protokollierung von Aktivitäten ermöglichen, um verdächtige Handlungen zu erkennen und nachvollziehen zu können. Das Fehlen dieser Funktionen erschwert die Identifizierung von Angriffen und die Durchführung einer forensischen Analyse im Falle eines Vorfalls. Eine fehlende Überwachung kann dazu führen, dass bösartige Aktivitäten unbemerkt bleiben.

VPN, ZTNA und PAM

Um diese Sicherheitsprobleme zu bewältigen, können verschiedene Lösungsansätze implementiert werden. Im Folgenden werden drei vielversprechende Ansätze vorgestellt: Virtual Private Network (VPN), Zero Trust Network Access (ZTNA) und Privileged Access Management (PAM). Ein VPN bietet eine sichere verschlüsselte Verbindung zwischen Remotezugriffsgeräten und OT-Geräten. Durch die Nutzung eines VPN wird die Netzwerkkommunikation vor potenziellen Abhörversuchen und Datenmanipulation geschützt. VPNs ermöglichen auch die Authentifizierung und Autorisierung der Benutzer. So ist sichergestellt, dass nur vertrauenswürdige Personen Zugriff auf das Netzwerk erhalten. Durch die Implementierung eines VPN können Unternehmen gewährleisten, dass der Remotezugriff auf OT-Geräte sicher und geschützt bleibt. Allerdings ist hierbei noch nicht garantiert, dass die gesamte Kommunikationskette verschlüsselt ist, da nach der VPN-Gegenstelle der Verkehr unverschlüsselt weitergeleitet werden kann. Darüber hinaus wird bei einem VPN zumeist das gesamte Netzwerk freigegeben und nicht nur einzelne Benutzer auf einzelne Geräte. So kann ein einzelner Mitarbeiter einer externen Wartungsfirma auf eine Vielzahl von Geräten der kritischen Infrastruktur zugreifen.

Die Fortführung des VPN-Konzepts und die entsprechende tiefergehende Regulierung der Netzwerkzugriffe ist ZTNA. Dies ist ein moderner Ansatz zur Netzwerksicherheit, der auf dem Prinzip des «vertrauenswürdigen Zugriffs» basiert. Mit dem «Zero Trust Network Access»-Ansatz werden Benutzer grundsätzlich immer überprüft und autorisiert – unabhängig davon, wo sie sich befinden oder von welchem Gerät aus sie zugreifen. ZTNA ermöglicht eine granulare Kontrolle über den Zugriff auf OT-Geräte und minimiert das Risiko unbefugten Zugriffs. Durch die Implementierung von ZTNA können Unternehmen sicherstellen, dass ausschließlich autorisierte Benutzer Zugriff auf die ihnen zugewiesenen OT-Geräte erhalten, unabhängig von ihrem Standort.

PAM ist neben den Netzwerklösungen eine Sicherheitslösung, die den Zugriff auf privilegierte Konten und Ressourcen überwacht und steuert. Durch die Implementierung von PAM können Unternehmen sicherstellen, dass nur autorisierte Benutzer Zugriff auf OT-Geräte erhalten. PAM ermöglicht eine granulare Kontrolle über die Berechtigungen sowie auf die Authentifizierungsmethoden, was das Risiko von Angriffen durch gestohlene oder kompromittierte Zugangsdaten verringert. Das PAM-System ist hierbei der einzige Einstiegspunkt für alle wichtigen Systeme. Hier können neben den Zielsystemen auch die Protokolle und Einschränkungen für diese definiert werden. So ist es beispielsweise möglich, im Microsoft-Remote-Desktop-Protokoll die gemeinsame Zwischenablage und Medienwiedergabe zu unterbinden. So lässt sich gewährleisten, dass einerseits die Arbeit nicht beeinträchtigt wird und andererseits das Risiko eines Datenabflusses minimiert wird.

Umfassende (OT-)Sicherheitsstrategie erforderlich

Der Remotezugriff auf OT-Geräte hilft Unternehmen, ihre Geschäftsprozesse aufrechtzuerhalten. Allerdings birgt er auch erhebliche Sicherheitsrisiken. Durch die Implementierung von Sicherheitslösungen wie PAM, VPN und ZTNA können Unternehmen jedoch die Sicherheit ihrer OT-Systeme maximal optimieren. Es ist wichtig, anzumerken, dass keine einzelne Technologie allein ausreicht, um alle Sicherheitsrisiken abzudecken. Eine umfassende Sicherheitsstrategie, die verschiedene Schutzmechanismen kombiniert, ist erforderlich, um die OT-Systeme effektiv zu schützen. In einer Zeit, in der Remotezugriff und Remotearbeit immer häufiger werden, ist es von grösster Bedeutung, dass Organisationen die Sicherheit im Auge behalten und angemessene Massnahmen ergreifen, um potenzielle Sicher-

Bild: BOLL Engineering

«Eine regelmässige Aktualisierung von Software und Firmware auf OT-Geräten ist entscheidend, um Sicherheitslücken zu schliessen. »

Marcel Schick, Experte für OT-Sicherheit, BOLL Europe GmbH

heitsrisiken so weit wie möglich auszuschalten. Nur durch geeignete Sicherheitslösungen können Unternehmen sicherstellen, dass der Remotezugriff auf OT-Geräte sicher und geschützt bleibt.

OT-Sicherheit vom kompetenten Partner
Der IT-Security-Distributor BOLL, der sowohl für die vertretenen Produkte als auch für die hoch qualifizierten Spezialisten bekannt ist, hat genau für diese Anwendungsfälle ein breites Spektrum an Lösungen im Portfolio. So erfüllen die PAM-Systeme der Hersteller Fudo, Claroty und WALLIX die Anforderungen bezüglich der sicheren Gestaltung des Remotezugriffs. Auch Lösungen für ZTNA werden von den BOLL-Spezialisten unterstützt. Hier sind unter anderem die Lösungen der Hersteller Fortinet und Palo Alto Networks zu nennen.

Darüber hinaus gibt es zur Überwachung der Firmwarestände und Konfigurationen noch ein umfangreiches Produkt von Claroty, das die Nachvollziehbarkeit in entsprechenden Anlagen um ein Vielfaches verbessert und somit Sichtbarkeit in diesen Bereich bringt.

Interview mit Marcel Schick, Experte für OT-Sicherheit, BOLL Europe GmbH

at: Welche Herausforderungen sehen Sie in Bezug auf die Sicherheit bei Fernwartungsanschlüssen?
Marcel Schick: Der Remotezugriff auf OT-Geräte ist zweifellos eine wichtige Massnahme, um Geschäftskontinuität (auch während einer Pandemie) zu gewährleisten. Allerdings bringt dies auch erhebliche Sicherheitsrisiken mit sich. Eine der grössten Herausforderungen besteht darin, eine sichere Authentifizierung und Autorisierung der Benutzer sicherzustellen. Schwache Passwörter oder fehlende Multi-Faktor-Authentifizierung sowie unregulierte Netzwerke können dazu führen, dass unbefugte Personen Zugriff auf OT-Geräte erhalten.

Welche Lösungsansätze empfehlen Sie, um diese Sicherheitsprobleme zu bewältigen?
M. Schick: Es gibt verschiedene Lösungsansätze, die Unternehmen in Betracht ziehen sollten. Eine wichtige Massnahme ist die Implementierung von Privileged Access Management (PAM). Dadurch kann der Zugriff auf privilegierte Konten und Ressourcen kontrolliert und überwacht werden. Eine granulare Kontrolle über die Berechtigungen und eine sichere Authentifizierung sind essenziell, um das Risiko von Angriffen durch gestohlene Zugangsdaten zu minimieren. Ein moderner Ansatz, den ich nebst dem PAM-System empfehle, ist Zero Trust Network Access (ZTNA). Dabei wird der »vertrauenswürdige Zugriff« implementiert. Das bedeutet, dass Benutzer immer überprüft und autorisiert werden müssen, unabhängig von ihrem Standort oder Gerät. ZTNA bietet eine granulare Kontrolle über den Zugriff auf OT-Geräte und minimiert das Risiko unbefugten Zugriffs.

Welche weiteren Massnahmen sollten Unternehmen ergreifen, um die Sicherheit ihrer OT-Systeme zu gewährleisten?
M. Schick: Neben den genannten Lösungsansätzen sollten Unternehmen eine umfassende Sicherheitsstrategie entwickeln, die verschiedene Schutzmechanismen kombiniert. Eine regelmässige Aktualisierung von Software und Firmware auf OT-Geräten ist entscheidend, um Sicherheitslücken zu schliessen. Zudem sollte eine kontinuierliche Überwachung des Netzwerkverkehrs implementiert werden, um verdächtige Aktivitäten zu erkennen. Schulungen und Sensibilisierungsmassnahmen für Mitarbeiter sind ebenfalls von grosser Bedeutung. Mitarbeiter sollten über bewährte Sicherheitspraktiken informiert und darin geschult werden, verdächtige Aktivitäten sollten unverzüglich gemeldet werden. Eine umfassende Incident-Response-Strategie sollte vorhanden sein, um im Falle eines Vorfalls schnell und angemessen reagieren zu können.

Vielen Dank für Ihre wertvollen Einblicke, Herr Schick. Gibt es noch abschliessende Worte, die Sie unseren Lesern mitgeben möchten?
M. Schick: Gerne. Unternehmen sollten eine ganzheitliche, robuste Sicherheitsstrategie entwickeln, in der OT- und IT-Umgebungen gemeinsam betrachtet und geschützt werden. Neben technischen Massnahmen ist auch eine positive Sicherheitskultur zu etablieren und in regelmässige Aus- und Weiterbildung der Mitarbeiter zu investieren, um das Sicherheitsbewusstsein zu stärken. Des Weiteren sollten regelmässige Überprüfungen (durch interne und externe Stellen) das aktuelle Sicherheitsniveau kontrollieren, und für einen Ernstfall sollte ein Incident-Response-Team zur Verfügung stehen, das entsprechende (Gegen-)Massnahmen einleitet. Kurz gesagt: Sicherheit ist als ganzheitlicher Prozess zu verstehen, bei dem technische Massnahmen mit organisatorischen Massnahmen optimal zusammenspielen und den Faktor Mensch miteinbinden.

boll-europe.com