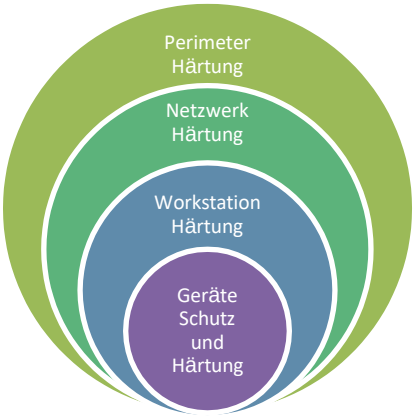
# Empfohlene Cybersecurity Best Practices

## Schneider Electric ist auf Cybersecurity fokussiert

Schneider Electric integriert die Best Practices und Lösungen der Cybersicherheit in seine Produkte, Systeme und Dienstleistungen. Unser "Security by Design"-Ansatz macht unsere Produkte widerstandsfähiger gegen Cyberattacken. Wir implementieren Mechanismen zur Minderung von Bedrohungen, zur Reduzierung ausnutzbarer Schwächen und zur Verteidigung gegen vermeidbare Datenschutzverletzungen und Cyberattacken.

## Empfohlene Cybersecurity Best Practices

Um die Sicherheit und den Schutz Ihrer Produkte von Schneider Electric zu gewährleisten, empfehlen wir Ihnen, diese Best Practices zur Cybersicherheit zu implementieren. Die Befolgung dieser Empfehlungen kann dazu beitragen, das Cybersicherheitsrisiko Ihres Unternehmens deutlich zu reduzieren.




## Perimeter-Härtung

### Einrichtung von Firewalls

Platzieren Sie Systeme und Geräte von Schneider Electric immer hinter Firewalls und anderen Sicherheitsvorrichtungen, die den Zugriff nur auf berechtigte Remote-Verbindungen beschränken. Der Aufbau eines hochgeschützten Netzwerks, das den Zugriff von außen verhindert, ist die kritischste Verteidigungslinie gegen Cyberattacken. Wir empfehlen Ihnen, diese Richtlinien zu befolgen.

- Beschränken Sie den Zugang zu den Netzen, in denen sich die Geräte von Schneider Electric befinden.
- Stellen Sie sicher, dass die Systeme und Geräte von Schneider Electric nicht über das Internet erreichbar sind, es sei denn, sie befinden sich hinter Firewalls und anderen Sicherheitsschutzvorrichtungen.
- Schränken Sie die externe Netzwerkkonnektivität auf die Systeme und Geräte von Schneider Electric ein.
- Überwachen Sie kontinuierlich auf Ereignisse, die auf einen versuchten unbefugten Zugriff hinweisen könnten.
- Beschränken Sie den Zugriff auf interne Netzwerke, in denen sich Geräte befinden.
- Isolieren Sie Kontroll- und Sicherheitssystemnetzwerke und Remote-Geräte vom Unternehmensnetzwerk.

## Netzwerk-Härtung

### Sichere Zugangskontrollen implementieren

Reduzieren Sie die Wege in und innerhalb Ihrer Netzwerke und implementieren Sie Sicherheitsprotokolle auf den vorhandenen Pfaden, um es einer Bedrohung zu erschweren, in Ihr System einzudringen und Zugang zu anderen Bereichen zu erhalten. Vergewissern Sie sich, dass alle Laptops und andere Systeme, die mit einem anderen Netzwerk verbunden sind, mit vollständig aktualisierten Softwareprogrammen und Virenschutz ordnungsgemäß gesäubert sind. Ziehen Sie in Betracht, Ihre Netzwerke und Geräte in voneinander isolierte Gruppen aufzuteilen und den Zugriff einzuschränken.

### Sichere Fernzugriffsmethoden verwenden

Implementieren Sie sichere Methoden, um einen Fernzugriff auf das Netzwerk für Remote-Benutzer zu ermöglich. Es sollte von allen Remote-Benutzern verlangt werden, dass sie sich über eine einzige, verwaltete Schnittstelle verbinden und authentifizieren, bevor sie Software-Upgrades, Wartung und andere System-Support-Aktivitäten durchführen.

### Einrichten von Maßnahmen zur Erkennung von Gefährdungen

Minimieren Sie die Chancen auf eine Gefährdung durch stetige Überwachung und Prüfung von Systemereignissen. Verwenden Sie Intrusion-Detection-Systeme (IDS), Intrusion-Prevention-Systeme (IPS), Antiviren-Software und Nutzungsprotokolle, damit Sie Angriffe bereits im frühesten Stadium erkennen können. Trotz der Implementierung dieser Präventivmaßnahmen kann es dennoch zu Angriffen auf Ihr System kommen. Halten Sie einen Plan bereit, um das Problem schnell zu erkennen und darauf zu reagieren.

## Computer Härtung

### Implementierung strenger Authentifizierungs- und Autorisierungskontrollen

Ändern Sie Standardpasswörter, wenn neue Software installiert wird und danach regelmäßig. Dies ist besonders wichtig für Administratorkonten und Steuergeräte des Systems. Verwenden Sie den rollenbasierten Zugriff mit Multi-Faktor-Authentifizierung, um Sicherheitsverletzungen zu verhindern und ein Protokoll der Zugriffsaktivitäten zu erstellen. Erwägen Sie das Hinzufügen von Passwort-Sicherheitsfunktionen, wie z.B. eine Kontosperre, die aktiviert wird, wenn ein Kennwort zu oft falsch eingegeben wird.

### Einrichtung einer Block-Liste, um bekannten verdächtigen oder böswilligen Instanzen den Zugang zu verweigern

Blocklisting kann dazu beitragen, bekannte Viren, Spyware, Trojaner, Würmer und andere Arten von Malware daran zu hindern, auf Ihr System zuzugreifen. Antiviren-Tools, Spam-Filter, Einbruchserkennungssysteme und andere Sicherheitssoftware enthalten in der Regel Blocklisting, um den Zugriff zu kontrollieren. Einer der größten Vorteile von Blocklisting ist ihre Einfachheit. Jede Instanz, die nicht auf der schwarzen Liste steht, erhält Zugriff, aber alles, was als Bedrohung bekannt ist oder erwartet wird, wird blockiert. Die meisten Organisationen verwenden Listen, die von Dritten, z.B. Sicherheitsdienstleistern, erstellt wurden. Darüber hinaus sollten Sie Ihre eigene schwarze Liste mit Benutzern, IP-Adressen, Anwendungen, E-Mail-Adressen, Domänen und allem anderen erstellen, was Sie von Ihrem System fernhalten möchten.

### Fügen Sie Allowlisting hinzu, um Ihre Systeme vor unerwünschter Software zu schützen

Fügen Sie Allowlisting-Software zu Ihrer Verteidigung hinzu, um sicherzustellen, dass nur Software, die Sie kennen und der Sie vertrauen, auf Ihrer Workstation ausgeführt werden darf. Allowlisting-Software arbeitet mit Ihrer Blocklisting-Software zusammen, um sicherzustellen, dass nur bekannte Software ausgeführt werden darf. Durch das Hinzufügen von Allowlisting-Software können Sie sicher sein, dass installierte Dateien und geladene ausführbare Dateien ihre Integrität und Authentizität beibehalten haben. Dieser zusätzliche Schutz führt zu einem höheren Maß an Vertrauen für die Workstation, indem er dazu beiträgt, ausgeklügelte Angriffe zu verhindern.

### Ermutigen Sie zu sicheren Arbeitsplatzgewohnheiten

Jeder in Ihrem Unternehmen kann zu den Bemühungen um Cybersicherheit beitragen, indem er seine Workstations so sicher wie möglich hält. Scannen Sie alle Geräte, die für den Datenaustausch verwendet werden, wie z. B. externe Festplatten oder USB-Laufwerke, bevor Sie sie in einem an das Netzwerk angeschlossenen System verwenden. Entfernen Sie unnötige Programme und Dienste von den Workstations und speichern Sie sensible Daten auf einem Server. Sichern Sie regelmäßig Daten von Festplattenlaufwerken.

Schließlich sollten Sie dafür sorgen, dass sich jeder daran gewöhnt, seinen Bildschirm zu sperren, wenn er nicht in Gebrauch ist.

## Geräteschutz und -härtung

### Richten Sie physische Kontrollen ein, um unbefugten Zugriff zu verhindern

Dies ist zwar nicht nur eine Frage der Cybersicherheit, aber es ist wichtig, physische Kontrollen einzurichten, damit kein Unbefugter auf Ihre Geräte zugreifen kann. Bewahren Sie alle Steuerungen in verschlossenen Schränken auf und beschränken Sie den Zugriff auf alle nicht-verschlossene Geräte.

### Prüfen Sie die Dokumentation auf produktspezifische Informationen

Schneider Electric stellt zu jedem Produkt detaillierte Informationen zur Verfügung. In den Produktleitfäden auf der Website von Schneider Electric oder in den Produktleitfäden, die Ihren Produkten beiliegen, finden Sie Cybersicherheitsempfehlungen und Best Practices, die sich direkt auf Ihre Produkte von Schneider Electric beziehen.

## Mehr Best Practices zur Risikominimierung

### Verwalten von Patches und Updates

Die meisten Anbieter arbeiten fleißig an der Entwicklung von Patches für identifizierte Schwachstellen. Selbst nach der Veröffentlichung von Patches und Updates bleiben viele Systeme anfällig, weil Unternehmen diese Korrekturen entweder nicht kennen oder diese nicht implementieren wollen oder können. Effektives Patching kann eine große Anzahl von Angriffen stoppen. Implementieren Sie daher ein Überwachungssystem, um sicherzustellen, dass Sie immer die neuesten Patches und Updates für Betriebssysteme, Antiviren-Tools und jede andere Software anwenden.

## Seien Sie sich der Schwachstellen bewusst

Schneider Electric veröffentlicht regelmäßig Sicherheitsbenachrichtigungen mit Informationen über Schwachstellen und Patches, die es von Einrichtungen wie dem ICS-CERT des US-Heimatschutzministeriums, Computer Emergency Readiness Teams (CERTs) aus verschiedenen Ländern, Cybersicherheits-ISACs (Information Sharing and Analysis Centers) auf der ganzen Welt und Cybersicherheitsfirmen erhält. Diese Updates sollen bekannte Schwachstellen beheben und sind für jedes Gerät mit Internetanschluss empfehlenswert. Sie können auch unseren Newsletter abonnieren, um Sicherheitsbenachrichtigungen zu erhalten.

## Pflegen Sie aktuelle Backups und testen Sie Ihre Wiederherstellungsverfahren

Backups sind der effektivste Weg, um sich von einem Malware-Angriff zu erholen. Neben der häufigen Sicherung von Systemen und Daten ist es wichtig, Ihre Wiederherstellungsverfahren zu testen. Stellen Sie sicher, dass Sie im Laufe der Zeit über mehrere Backups verfügen, damit Sie von einer Version vor einer Infektion wiederherstellen können.

## Ihr Personal ausbilden

Bieten Sie Ihren Mitarbeitern Cybersicherheitsschulungen an, um die Sicherheit Ihres Unternehmens zu gewährleisten. Erklären Sie Phishing-E-Mails, infizierte Anhänge, bösartige Websites und andere Methoden, die diese direkt angreifen. Verlangen Sie von allen Auftragnehmern oder Anbietern von verwalteten Diensten, dass sie eine entsprechende Cybersicherheitsschulung absolvieren.

## Für weitere Informationen und Unterstützung

Für Einzelheiten und Hilfe zum Schutz Ihrer Installation wenden Sie sich bitte an Ihre lokale Schneider Electric Industrial Cybersecurity Services Organisation oder besuchen Sie Cybersecurity Services auf der Schneider Electric Website

Weitere Informationen über bewährte Praktiken im Bereich der Cybersicherheit finden Sie in folgenden Ressourcen.

Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
ISA Global Cybersecurity Alliance (ISAGCA)

Cybersecurity Best Practices Center for Internet Security

IEC 62443 Security for Industrial Automation and Control Systems International Society of Automation (ISA)

e-Guide: Building a Cybersecurity Strategy for the Digital Economy
© 2019 Schneider Electric

Cybersecurity by Design: Building a Company Culture to Strengthen a Digital Business
© 2019 Schneider Electric

Document # 7EN52-0390-03 - Juni 2020

DIESES DOKUMENT SOLL DAZU BEITRAGEN, ALLGEMEINE SICHERHEITSEMPFEHLUNGEN ZU GEBEN, UND WIRD AUF EINER "IST"-BASIS OHNE JEGLICHE GARANTIE ZUR VERFÜGUNG GESTELLT. SCHNEIDER ELECTRIC LEHNT JEDE GEWÄHRLEISTUNG, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIEßLICH DER GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AB. IN KEINEM FALL IST SCHNEIDER ELECTRIC HAFTBAR FÜR SCHÄDEN JEGLICHER ART, EINSCHLIESSLICH DIREKTER, INDIREKTER, BEILÄUFIGER, ZUFÄLLIGER ODER FOLGESCHÄDEN, ENTGANGENER GEWINNE ODER BESONDERER SCHÄDEN, SELBST WENN SCHNEIDER ELECTRIC AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. DIE VERWENDUNG DIESES DOKUMENTS, DER DARIN ENTHALTENEN INFORMATIONEN ODER VON MATERIALIEN, DIE MIT DIESEM DOKUMENT VERLINKT SIND, ERFOLGT AUF EIGENE GEFAHR. SCHNEIDER ELECTRIC BEHÄLT SICH DAS RECHT VOR, DIESES DOKUMENT JEDERZEIT UND NACH EIGENEM ERMESSEN ZU AKTUALISIEREN ODER ZU ÄNDERN.