Eaton Cybersecurity Center of Excellence
Empfehlungen zur Cybersicherheit

RICHTLINIEN FÜR DIE SICHERE KONFIGURATION VON EATON PRODUKTEN

Powering Business Worldwide

Dokumentation zur sicheren Installation und Konfiguration von Eaton-Produkten

Eaton Green Motion AC Home wurde so entwickelt, dass die Cybersicherheit einen hohen Stellenwert genießt. Deswegen bietet dieses Produkt Funktionen, um Cybersicherheitsrisiken zu beseitigen. Diese Cybersicherheitsempfehlungen liefern Informationen, die den Benutzern helfen, das Produkt so einzusetzen und zu warten, dass Cybersicherheitsrisiken minimiert werden. Diese Cybersicherheitsempfehlungen sind kein umfassender Leitfaden zur Cybersicherheit, sondern sie ergänzen die bestehenden Cybersicherheitsprogramme unserer Kunden.

Eaton ist bestrebt, das Cybersicherheitsrisiko in seinen Produkten zu minimieren und Best Practices für die Cybersicherheit in allen seinen Produkten einzusetzen, um sie für unsere Kunden sicherer, zuverlässiger und wettbewerbsfähiger zu machen.

Die folgenden Whitepaper bieten weitere Informationen zu allgemeinen Best Practices und Richtlinien für die Cybersicherheit:

Cybersicherheitsbetrachtungen für die Informations- und Kommunikationstechnik (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Erinnerungshilfe für die Cybersicherheit Best Practices Prüfliste (WP910003DE):

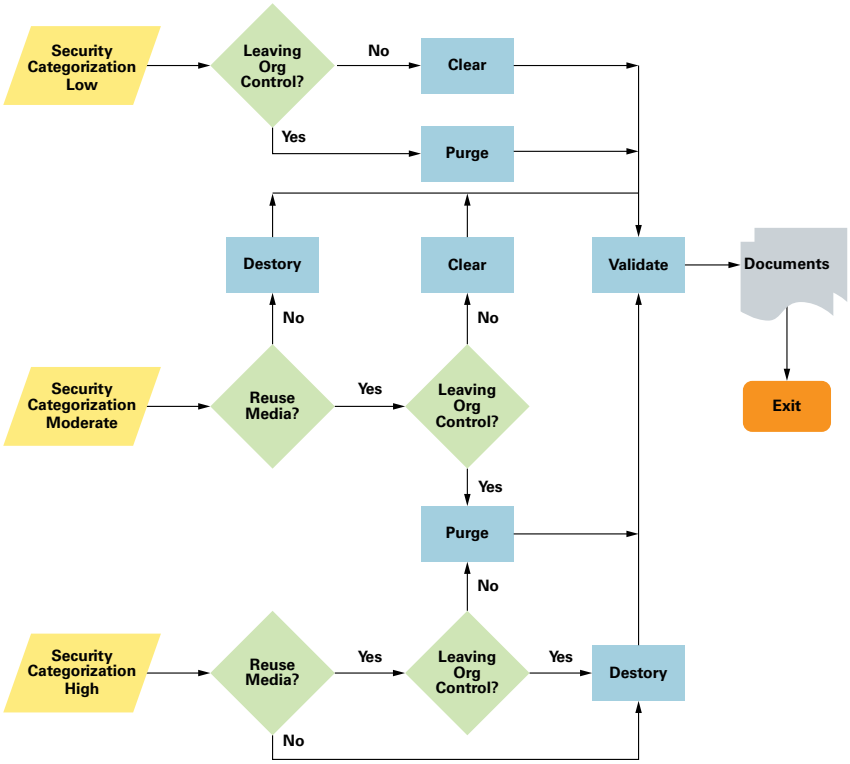
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

Cybersecurity Best Practices for Modern Vehicles – NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Kategorie	Beschreibung
Verwendungszweck und Einsatzumgebung	Dieses Produkt ist zum Aufladen von Elektrofahrzeugen für Privatanwender vorgesehen. Das Produkt wird auf dem Grundstück des Kunden installiert und kann wie folgt verwendet werden: 1. Offlinemodus (keine Internetverbindung) 2. Online-Modus (mit Internet/Backend verbunden) Weitere Informationen zur sicheren Verwendung und Installation des Produkts finden Sie unter: www.eaton.com/greenmotionhome
Ressourcenverwaltung	Eine umfassende Bestandsverwaltung der Soft- und Hardware-Ressourcen in Ihrer Umgebung ist eine Grundvoraussetzung für ein effektives Cybersicherheitsmanagement. Eaton empfiehlt, eine Anlageninventur durchzuführen, bei der jede wichtige Komponente eindeutig identifiziert wird. Um dies zu erleichtern, unterstützt **Eaton Green Motion AC Home**die folgenden Identifizierungsinformationen: Produktkatalognummer, Seriennummer, (auf dem Produkt verfügbar) Fabrik-Hotspot-Details, eindeutige Geräte-ID (mit dem Produkt gelieferte Broschüren, die für zukünftige Anforderungen sicher aufbewahrt werden). Weitere Informationen finden Sie im Installationshandbuch.
Physische Sicherheit	Ein Angreifer mit unbefugtem physischem Zugriff kann schwerwiegende Störungen der Funktionalität des Systems oder des Geräts verursachen. In diesen Fällen ist die physikalische Sicherheit eine wichtige Sicherheitsstufe. **Eaton Green Motion AC Home** wurde für den Einsatz und Betrieb an einem physisch sicheren Ort entwickelt. Im Folgenden finden Sie einige bewährte, von Eaton empfohlene Verfahren, um Ihr System oder Gerät physisch zu sichern: • Sichern Sie die Räumlichkeiten und Geräte mit Zugangskontrollmechanismen wie Schlössern, Zutrittskartenlesern, Wachpersonal, Personenschleusen, Videoüberwachung usw., falls erforderlich. • Der physische Zugang zu den Telekommunikationsleitungen und den Netzwerkkabeln sollte zum Schutz vor Abhör- oder Sabotageversuchen eingeschränkt werden. Es ist eine bewährte Vorgehensweise, Metallkanäle für die Netzwerkkabelführung zwischen den Geräteschränken zu verwenden. • **Eaton Green Motion AC Home** unterstützt die folgenden physischen Zugriffsports: Ethernet, serielle Schnittstelle, USB-Anschluss. Der Zugriff auf diese Ports sollte für nicht autorisierte Benutzer eingeschränkt werden. • Schließen Sie keine Wechselmedien an (z. B. USB-Geräte, SD-Karten usw.)
Kontoverwaltung	Der logische Zugriff auf das System | Gerät sollte auf legitime Benutzer beschränkt sein. Und ihnen sollten nur die Berechtigungen zugewiesen werden, die für die Erledigung ihrer Aufgaben/Funktionen erforderlich sind. Einige der folgenden Best Practices müssen möglicherweise implementiert werden: • Stellen Sie sicher, dass die Standard-Anmeldeinformationen bei der Erstanmeldung geändert werden. Sollte nicht in Produktionsumgebungen mit Standard-Anmeldeinformationen eingesetzt werden, da Standard-Anmeldeinformationen anderen Nutzern bekannt sind. • Keine Kontenfreigabe - Jedem Benutzer sollte ein eindeutiges Konto zugewiesen werden, anstatt Konten und Passwörter zu teilen. Die Sicherheitsüberwachungs- und Protokollierungsfunktionen des Produkts werden basierend auf jedem Benutzer mit einem individuellen Konto eingerichtet. Wenn Benutzer Anmeldeinformationen gemeinsam nutzen können, wird die Sicherheit beeinträchtigt. • Stellen Sie sicher, dass die Länge, Komplexität und Ablaufzeiten der Passwörter angemessen eingestellt sind, insbesondere für alle Verwaltungskonten (z.B. mindestens 10 Zeichen, Mischung aus Groß- und Kleinbuchstaben und Sonderzeichen, und verfallen alle 90 Tage oder anderweitig in Übereinstimmung mit den Richtlinien Ihres Unternehmens). - Unterstützte Kennwort- und Kontorichtlinien: - Hotspot, 16 Zeichen, A-F, 0-9 und Sonderzeichen sind nur innerhalb der Wi-Fi-Reichweite zugänglich, Zeitüberschreitung 30 Minuten, Sperrsystemverzögerung Der Benutzer sollte auf seinem Heimrouter ein komplexes Passwort einrichten. Das serielle und das SSH-Konto sind nur für die Verwendung durch den technischen Support von Eaton zwecks Debugging/Fehlerbehebung vorgesehen.

Kategorie	Beschreibung
Zeitsynchronisation	Viele Vorgänge in Stromnetzen und IT-Netzen sind stark von präzisen Zeitinformationen abhängig. Stellen Sie sicher, dass die Systemuhr mit einer autoritativen Zeitquelle synchronisiert ist (mit manueller Konfiguration, NTP, SNTP oder IEEE 1588). Im Online-Modus erfolgt die Zeitsynchronisierung automatisch, sobald das Gerät Zugriff auf OCPP Boot Notification und Heartbeat erhält. Im Offline-Modus erfolgt die Zeitsynchronisierung bei einer Verbindung zur mobilen App. Alle Zeitstempel sind mit UTC-Zeitzonenreferenz versehen.
Netzwerksicherheit	**Eaton Green Motion AC Home** unterstützt die Netzwerkkommunikation mit anderen Geräten in der Umgebung. Diese Funktion kann Risiken bergen, wenn sie nicht sicher konfiguriert wurde. Im Folgenden werden von Eaton empfohlene Best Practices zur Sicherung des Netzwerks aufgeführt. Weitere Informationen zu den verschiedenen Netzschutzstrategien finden Sie (auf Englisch) in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton empfiehlt die Segmentierung von Netzwerken in logische Enklaven, wodurch der Datenverkehr zwischen den Segmenten mit Ausnahme desjenigen, der ausdrücklich erlaubt ist, verweigert wird, und die Kommunikation auf host-to-host-Pfade beschränkt wird (z.B. durch Verwendung von Router-ACLs und Firewall-Regeln). Dies trägt zum Schutz sensibler Informationen und kritischer Dienste bei und schafft zusätzliche Barrieren im Falle einer Netzwerkperimeterverletzung. Ein Netzwerk von industriellen Steuerungssystemen für Versorgungsunternehmen sollte mindestens in eine dreistufige Architektur (wie von NIST SP 800-82[R3] empfohlen) unterteilt werden, um die Sicherheitskontrolle zu verbessern. Schutz der Kommunikation: **Eaton Green Motion AC Home** ermöglicht die Verschlüsselung der Netzwerkkommunikation. Diese Verschlüsselung ist standardmäßig aktiviert. Eaton empfiehlt, nur die Ports freizugeben, die für den Betrieb erforderlich sind, und die Netzwerkkommunikation mit Netzwerkschutzsystemen wie Firewalls und Zugangskontrollsystemen / Intrusion Prevention Systemen zu schützen. Im Online-Modus verbindet sich die Ladestation mit dem Backend über das OCPP-Protokoll. Im Offline-Modus verbindet sich die Ladestation über WLAN mit der mobilen App.
Fernzugriff	Der Fernzugriff auf Geräte/Systeme schafft einen weiteren Einstiegspunkt in das Netzwerk. Eine strenge Verwaltung und Validierung der Beendigung eines solchen Zugriffs ist unerlässlich, um die Kontrolle über die gesamte IKS-Sicherheit zu behalten. • Die Fernzugriffsfunktionen werden durch das Secure Protocol OCPP über TLS 1.2 bereitgestellt. • Das Gerät überträgt die unter Systemprotokolle aufgezeichneten Aktivitäten über das OCPP-Protokoll an das Backend. • Firmware-Updates werden vom Backend über OCPP an die Geräte übertragen, wenn das Gerät mit dem Internet verbunden ist. • Weitere Informationen finden Sie in den Best Practices von Eaton Cybersecurity [R2]
Protokoll- und Eventmanagement	• Die Ladestatistik steht dem Benutzer in der mobilen App zur Überprüfung zur Verfügung. • Überprüfen Sie die Protokolle regelmäßig. • Protokolle sind über den Charging Network Manager erhältlich. Weitere Informationen finden Sie in der technischen Dokumentation, oder wenden Sie sich an Ihr Support-Team vor Ort.
Schutz vor Malware	Eaton empfiehlt den Einsatz geeigneter Malware-Abwehrmaßnahmen zum Schutz des Produkts oder der Plattformen, auf denen das Eaton-Produkt betrieben wird.

Kategorie	Beschreibung
Sichere Wartung	Das Gerät verfügt über eine lokale SSH-Verbindung. Das ermöglicht einem Servicetechniker die Fehlerbehebung der Gerätefunktion mit Hilfe des Standortadministrators. SSH-Port ist standardmäßig deaktiviert. Dieser Anschluss ist nur für Servicetechniker bestimmt. Der Kunde soll diese Funktion nicht verwenden. **Hinweis:** Die Aktivierung von TCP-Port 22 dient nur zu Diagnosezwecken und darf nicht aktiviert bleiben. **Best Practices** Aktualisieren Sie die Geräte-Firmware, bevor Sie das Gerät in Betrieb nehmen. Danach sollten Sie regelmäßig Firmware-Updates und Software-Patches installieren. Eaton veröffentlicht Patches und Updates für seine Produkte, um sie vor entdeckten Schwachstellen zu schützen. Firmware-Updates werden ausschließlich über den Charging Network Manager verwaltet und installiert. So ist sichergestellt, dass Sie vertrauenswürdige Firmware-Dateien verwenden. • Bei Ladegeräten im Online-Modus (mit Internet verbunden) wird der EV Charger automatisch aktualisiert, sobald ein Update verfügbar ist. • Bei Ladegeräten im Offline-Modus (nicht mit dem Internet verbunden) informiert die mobile Anwendung über die Verfügbarkeit und den Aktualisierungsvorgang. Während des Herunterladens und Upgrades der Firmware ist der EV Charger nicht verfügbar.
Außerbetriebnahme oder Nullstellung	Es ist eine bewährte Vorgehensweise, Daten zu bereinigen, bevor Sie ein Gerät mit Daten entsorgen. Dazu gehören vertrauliche Informationen wie Anmeldedaten, Protokolle, RFID-Informationen usw. Der Flash-Speicher kann mithilfe der Funktion zum Zurücksetzen auf die Werkseinstellungen gelöscht werden. Weitere Informationen finden Sie im Installationshandbuch.  **Abbildung 1:** Sanierungs- und Entsorgungsentscheidungen * Abbildung und Daten aus NIST SP800-88 Die Ladestation wird nach dem ISO9001-Prozess recycelt. **Integrierter Flash-Speicher in Platinen und Geräten** Eaton empfiehlt die folgenden Verfahren zur Entsorgung von Motherboards, Peripheriekarten wie Netzwerkadaptern oder anderen Adaptern mit nichtflüchtigem Flash-Speicher. **Zurücksetzen:** Setzen Sie den Zustand auf die ursprünglichen Werkseinstellungen zurück, indem Sie die Reset-Taste mindestens 5 Sekunden lang gedrückt halten. Weitere Informationen finden Sie in der technischen Dokumentation. **Löschen:** Der Flash-Speicher kann nicht leicht erkannt und von der Platine entfernt werden. Aus diesem Grund empfiehlt Eaton, die gesamte Rechnerplatine zu zerstören. **Zerstören:** Schreddern, desintegrieren, pulverisieren oder verbrennen Sie das Gerät, indem Sie es in einer lizenzierten Verbrennungsanlage verbrennen.

Hinweise

Sollwerte

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] Cybersecurity Best Practices for Modern Vehicles - NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Threat Modeling for Automotive Security Analysis
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Eaton Industries Manufacturing GmbH
Place de la Gare 2
1345 Le Lieu, Schweiz

Publikationsnummer: MZ191002DE
Oktober 2022

Folgen Sie uns in den sozialen Netzwerken, und erhalten Sie aktuelle Produkt- und Supportinformationen.