Centrum cyberbezpieczeństwa firmy Eaton
Rekomendacje dotyczące cyberbezpieczeństwa

# Wytyczne dotyczące bezpiecznej konfiguracji stacji ładowania pojazdów elektrycznych Green Motion Building firmy Eaton.

Powering Business Worldwide

## Dokumentacja umożliwiająca bezpieczne wdrożenie i konfigurację produktów firmy Eaton

**Stacje ładowania pojazdów elektrycznych Green Motion Building** firmy Eaton zostały zaprojektowane z uwzględnieniem cyberbezpieczeństwa jako ważnego czynnika. W produkcie oferowany jest szereg funkcji mających na celu przeciwdziałanie zagrożeniom związanym z cyberbezpieczeństwem. Niniejsze zalecenia dotyczące cyberbezpieczeństwa zawierają informacje, które mają pomóc użytkownikom we wdrożeniu i utrzymaniu produktu w sposób minimalizujący ryzyko związane z cyberbezpieczeństwem. Niniejsze zalecenia dotyczące cyberbezpieczeństwa nie mają na celu zapewnienia kompleksowego przewodnika po tym zagadnieniu, a raczej uzupełnienie istniejących programów cyberbezpieczeństwa naszych klientów.

Firma Eaton zaangażowana jest w minimalizowanie ryzyka cyberataków oraz stosuje najlepsze praktyki zabezpieczeń komputerowych w swoich produktach i rozwiązaniach, przez co są one bezpieczniejsze, bardziej niezawodne oraz konkurencyjne dla klientów.

Aby uzyskać więcej informacji na temat ogólnych najlepszych praktyk i wytycznych w zakresie cyberbezpieczeństwa,
można się zapoznać z następującymi publikacjami:

**Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN): (Kwestie cyberbezpieczeństwa w odniesieniu do systemów dystrybucji energii elektrycznej):**

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

**Cybersecurity Best Practices Checklist Reminder (WP910003EN): (Przypomnienie listy kontrolnej najlepszych praktyk w zakresie cyberbezpieczeństwa):**

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

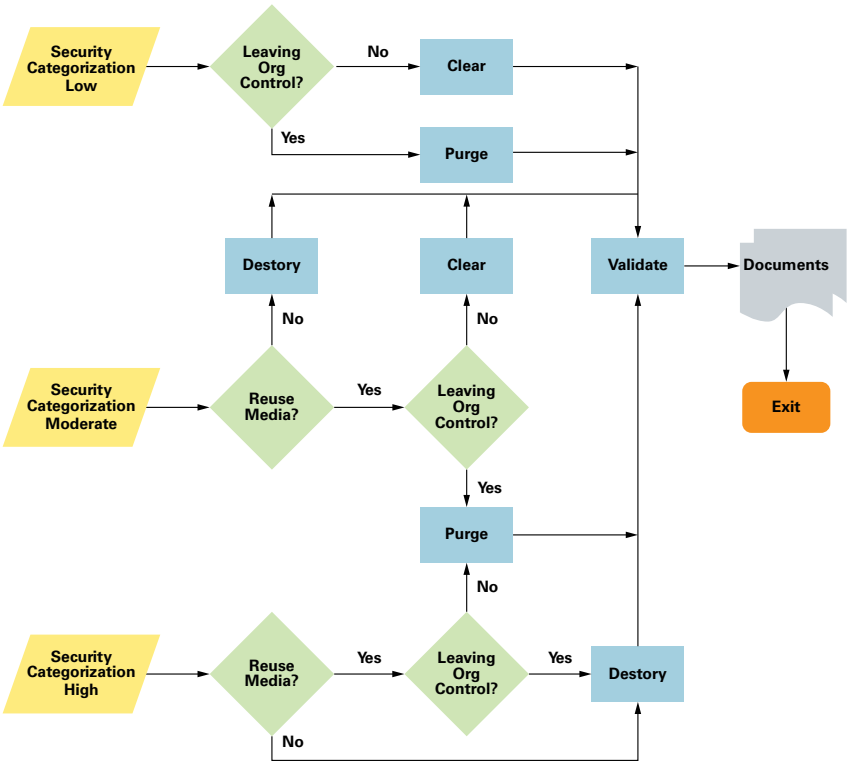
**Najlepsze praktyki w zakresie cyberbezpieczeństwa dla nowoczesnych pojazdów - NHTSA**

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

| Kategoria | Opis |
|---|---|
| Kontekst zamierzonego użycia i rozmieszczenia | Dotyczy stacji ładowania podłączonych do oprogramowania Charging Network Manager firmy Eaton (back-end) lub produktu podłączonego do back-endu innej firmy.<br>Stacje ładujące są wdrażane u klientów na parkingach, prywatnych lub publicznie dostępnych, aby umożliwić ładowanie pojazdów elektrycznych, uwierzytelnianie, rozliczanie itp.<br>Więcej informacji na temat bezpiecznego użytkowania, instalacji i uruchomienia produktu można znaleźć pod linkiem: www.eaton.pl/gmb |
| Zarządzanie zasobami | Śledzenie zasobów oprogramowania i sprzętu w środowisku informatycznym jest warunkiem koniecznym do skutecznego zarządzania cyberbezpieczeństwem. Firma Eaton zaleca prowadzenie ewidencji środków trwałych, która jednoznacznie identyfikuje każdy ważny element. Aby to ułatwić,**stacje ładowania pojazdów elektrycznych Green Motion Buliding** firmy Eaton obsługują następujące informacje identyfikacyjne:<br>Numer katalogowy produktu, numer seryjny (dostępny na produkcie), dane do logowania hotspotu fabrycznego i wersja zainstalowanego oprogramowania.<br>Powyższe informacje są dostępne na tabliczce znamionowej i stronie konfiguracji (więcej informacji w instrukcji montażu). |
| Ocena ryzyka | Firma Eaton zaleca przeprowadzenie oceny ryzyka w celu identyfikacji i oceny racjonalnie przewidywalnych wewnętrznych i zewnętrznych zagrożeń dla poufności, dostępności i integralności stacji ładowania pojazdów elektrycznych **Green Motion Building** firmy Eaton i ich otoczenia. Proces ten powinien być przeprowadzony zgodnie z obowiązującymi ramami technicznymi i regulacyjnymi, takimi jak IEC 62443 i NERC-CIP. Ocena ryzyka powinna być powtarzana okresowo. |
| Bezpieczeństwo fizyczne | Napastnik z nieautoryzowanym dostępem fizycznym może spowodować poważne zakłócenia w funkcjonowaniu systemu lub urządzenia. Ponadto przemysłowe protokoły sterowania nie zapewniają ochrony kryptograficznej, co sprawia, że komunikacje ICS i SCADA są szczególnie podatne na zagrożenia dla ich poufności. Bezpieczeństwo fizyczne jest w takich przypadkach ważnym narzędziem obrony.<br>**Stacje ładowania pojazdów elektrycznych Green Motion Building firmy Eaton** są przeznaczone do rozmieszczenia i obsługi w fizycznie bezpiecznym miejscu.<br>Poniżej przedstawiono kilka najlepszych praktyk, które firma Eaton zaleca do fizycznego zabezpieczenia systemu/ urządzenia:<br>• Należy zabezpieczyć obiekt i pomieszczenia lub szafy na sprzęt za pomocą mechanizmów kontroli dostępu, takich jak zamki, czytniki kart wstępu, strażnicy, pułapki, telewizja przemysłowa itp. w zależności od potrzeb.<br>• Ograniczyć fizyczny dostęp do szafek i/lub obudów zawierających **stację ładowania pojazdów elektrycznych Green Motion Building firmy Eaton**.<br>Stacje ładowania pojazdów elektrycznych są wyposażone w funkcję wykrywania sabotażowego. Po otwarciu urządzenia w stanie zasilania<br>do sieci back-endu zostanie wysłane powiadomienie.<br>• Fizyczny dostęp do linii telekomunikacyjnych i okablowania sieciowego powinien być ograniczony w celu ochrony przed próbami przechwycenia lub sabotażu łączności. Najlepszą praktyką jest stosowanie metalowych przepustów do okablowania sieciowego biegnącego między szafami sprzętowymi.<br>• **Stacje ładowania pojazdów elektrycznych Eaton Green Motion DC 22/44/66** obsługują następujące fizyczne porty dostępu: Port szeregowy (tylko dla pomocy technicznej), Ethernet. Dostęp do tych portów powinien być ograniczony.<br>• Nie należy podłączać nośników wymiennych (np. urządzeń USB, kart SD itp.) w celu wykonania jakiejkolwiek operacji (np. aktualizacji oprogramowania układowego, zmiany konfiguracji lub zmiany aplikacji rozruchowej), chyba że pochodzenie nośnika jest znane i zaufane.<br>• Przed podłączeniem jakiegokolwiek urządzenia przenośnego przez port USB lub gniazdo karty SD należy przeskanować urządzenie pod kątem złośliwego oprogramowania i wirusów. |

| Kategoria | Opis |
|---|---|
| Synchronizacja czasowa | Wiele operacji w sieciach energetycznych i informatycznych w dużym stopniu zależy od precyzyjnych informacji o czasie.<br>Należy się upewnić, że zegar systemowy jest zsynchronizowany z autorytatywnym źródłem czasu (przy użyciu konfiguracji ręcznej, NTP, SNTP lub IEEE 1588).<br>Synchronizacja czasu nastąpi automatycznie po podłączeniu urządzenia do sieci i uzyskaniu dostępu do OCPP Boot Notification i Heartbeat. |
| Bezpieczeństwo sieci | **Stacje ładowania pojazdów elektrycznych Green Motion Building** firmy Eaton obsługują komunikację sieciową z innymi urządzeniami w otoczeniu. Ta możliwość może stanowić zagrożenie, jeśli nie zostanie skonfigurowana w bezpieczny sposób. Poniżej przedstawiono zalecane przez firmę Eaton najlepsze praktyki pomagające w zabezpieczeniu sieci. Dodatkowe informacje na temat różnych strategii ochrony sieci są dostępne w dokumencie firmy Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. (Uwagi dotyczące cyberbezpieczeństwa w systemach dystrybucji energii elektrycznej.)<br>Firma Eaton zaleca segmentację sieci na logiczne enklawy, uniemożliwienie ruchu między segmentami z wyjątkiem tego, który jest specjalnie dozwolony, oraz ograniczenie komunikacji do ścieżek typu host-to-host (na przykład, przy użyciu list kontrolnych routera i reguł zapory). Pomaga to chronić wrażliwe informacje i krytyczne usługi oraz tworzy dodatkowe bariery w przypadku naruszenia obwodu sieci. Jako minimum, sieć Industrial Control Systems powinna być podzielona na trzy warstwy (zgodnie z zaleceniami NIST SP 800-82[R3]) dla lepszej kontroli bezpieczeństwa.<br>Ochrona komunikacji: **Stacje ładujące pojazdy elektryczne Green Motion Building** firmy Eaton zapewniają szyfrowanie swojej komunikacji sieciowej. To szyfrowanie jest zawsze domyślnie włączone (HTTPS dla strony konfiguracyjnej, profil bezpieczeństwa OCPP 2) i nie ma potrzeby jego konfigurowania.<br>Firma Eaton zaleca otwarcie tylko tych portów, **które są wymagane** do działania i ochrony komunikacji sieciowej za pomocą systemów ochrony sieci, takich jak zapory, systemy wykrywania włamań lub systemy zapobiegania włamaniom. Skorzystaj z poniższych informacji, aby skonfigurować reguły zapory sieciowej w celu umożliwienia dostępu potrzebnego do płynnego działania stacji ładowania<br>**Green Motion Building**<br>• Port TCP 5355 powinien być otwarty, aby umożliwić połączenie LLMNR (TCP/UDP)<br>• Port TCP 443 powinien być otwarty, aby umożliwić połączenie OCPP z back-endem CPO<br>Modem 4G podłączony przez port szeregowy USB do CPU, używa protokołu punkt-punkt (ppp). Zaleca się korzystanie z **kart SIM 4G IoT**, które obsługują poniższe funkcje bezpieczeństwa, aby zapewnić łączność internetową między stacją ładowania a serwerem.<br>**Zalecane funkcje bezpieczeństwa**<br>• Aby użyć prywatnej nazwy punktu dostępu (APN) podczas instalacji Green Motion Building i uruchamiania oprogramowania Charging network manager.<br>• Aby korzystać z dostawców usług 4G SIM, którzy zapewniają opcję szyfrowania transmisji danych za pomocą wirtualnej sieci prywatnej (VPN) lub zabezpieczeń IPSec, aby włączyć pin uniwersalnej karty zintegrowanej (UICC), aby zapobiec nieautoryzowanemu dostępowi do sieci. W przypadku protokołu Modbus TCP, stacja ładowania pojazdów elektrycznych oferuje funkcję bezpieczeństwa białej listy IP. Zaleca się, aby użytkownik dodał adres IP do białej listy. Więcej informacji na ten temat można znaleźć w instrukcji montażu w sekcji konfiguracja urządzenia i sieci. |
| Rejestrowanie i zarządzanie zdarzeniami | • Firma Eaton zaleca rejestrowanie wszystkich istotnych zdarzeń systemowych i aplikacyjnych, w tym wszystkich działań administracyjnych i konserwacyjnych.<br>• Dzienniki zdarzeń powinny być chronione przed manipulacją i innymi zagrożeniami dla ich integralności (na przykład poprzez ograniczenie uprawnień dostępu i modyfikacji dzienników, przesyłanie dzienników do systemu zarządzania informacjami i zdarzeniami bezpieczeństwa itp.)<br>• Upewnij się, że dzienniki zdarzeń są przechowywane przez rozsądny i odpowiedni okres czasu.<br>• Należy regularnie przeglądać dzienniki zdarzeń. Częstotliwość ich przeglądów powinna być rozsądna, biorąc pod uwagę wrażliwość i krytyczność systemu, urządzenia i wszelkich przetwarzanych przez nie danych.<br>• Dzienniki zdarzeń są dostępne w oprogramowaniu Charging Network Manager (back-end), w celu uzyskania dalszych szczegółów należy zapoznać się z dokumentacją techniczną produktu lub skontaktować się z lokalnym zespołem wsparcia. |
| Obrona przed złośliwym oprogramowaniem | Firma Eaton zaleca wdrożenie odpowiednich zabezpieczeń przed złośliwym oprogramowaniem, aby chronić produkt lub platformy używane do jego uruchomienia. |

| Kategoria | Opis |
|---|---|
| Bezpieczna konserwacja | Urządzenie zawiera połączenie SSH, aby umożliwić inżynierowi serwisu rozwiązywanie problemów z urządzeniem. Port SSH jest domyślnie wyłączony i powinien być włączony tylko wtedy, gdy jest to absolutnie konieczne przez inżyniera usługi.<br>**Najlepsze praktyki**<br>Przed wdrożeniem urządzenia do produkcji należy zaktualizować jego oprogramowanie sprzętowe. Następnie należy regularnie stosować aktualizacje oprogramowania sprzętowego i poprawki oprogramowania.<br>Firma Eaton publikuje poprawki i aktualizacje dla swoich produktów, aby chronić je przed błędami lub niebezpiecznymi lukami. Firma Eaton zachęca klientów do utrzymywania spójnego procesu szybkiego monitorowania i instalowania nowych aktualizacji oprogramowania sprzętowego.<br>Aktualizacje oprogramowania sprzętowego są zarządzane i instalowane wyłącznie za pośrednictwem oprogramowania Charging Network Manager firmy Eaton, które zapewnia korzystanie z zaufanych plików oprogramowania sprzętowego.<br>W przypadku urządzeń offline należy wykonać następującą procedurę:<br>1. Otwórz stronę internetową konfiguracji<br>2. Wybierz pakiet GM oprogramowania sprzętowego i naciśnij przycisk przesyłania<br>3. Urządzenie pobiera pakiet i sprawdza podpis<br>4. Po zweryfikowaniu podpisu skrypt powłoki aktualizuje oprogramowanie sprzętowe na urządzeniu<br>Lokalny serwer internetowy może być również używany do bezpiecznej aktualizacji oprogramowania sprzętowego. |
| Ujawnianie informacji poufnych | Firma Eaton zaleca, aby wrażliwe informacje (np. łączność, dane dziennika zdarzeń, dane osobowe), które mogą być przechowywane przez stację ładowania **Green Motion Building firmy Eaton**, były odpowiednio chronione poprzez wdrożenie praktyk bezpieczeństwa organizacyjnego.<br>Potencjalnie wrażliwe informacje przechowywane w stacjach ładowania to numer seryjny RFID ostatniego użytkownika stacji ładującej. |

| Kategoria | Opis |
|---|---|
| Wycofanie z eksploatacji lub zerowanie | Dobrą praktyką jest wykasowanie danych przed pozbyciem się jakiegokolwiek urządzenia je zawierającego. Wytyczne dotyczące wycofania z eksploatacji znajdują się w NIST SP 800-88. Firma Eaton zaleca, aby produkty zawierające wbudowaną pamięć flash były bezpiecznie niszczone, aby zapewnić, że dane są nie do odzyskania.<br>  <br><br>**Sanitization and disposition decision flow**<br>* Rysunek i dane z NIST SP800-88<br>Stacja ładowania zostanie poddana recyklingowi zgodnie z procesem ISO9001.<br>**Wbudowana pamięć flash na płytach i urządzeniach**<br>Firma Eaton zaleca następujące metody utylizacji płyt głównych, kart peryferyjnych, takich jak karty sieciowe lub innych adapterów zawierających nieulotną pamięć flash.<br>**Kasowanie:** Należy przywrócić stan do oryginalnych ustawień fabrycznych, naciskając i przytrzymując przycisk resetowania przez co najmniej 5 sekund. Więcej informacji można znaleźć w dokumentacji technicznej.<br>**Oczyszczanie:** Pamięć flash nie może być łatwo zidentyfikowana i usunięta z płyty. Z tego powodu firma Eaton zaleca zniszczenie całej płyty obliczeniowej.<br>**Niszczenie:** Należy rozdrobnić, rozłożyć, sproszkować lub spalić poprzez spalenie urządzenia w licencjonowanej spalarni. |

# Bibliografia

**[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 Electric Sp. z o.o.**
ul. Galaktyczna 30,
80-299 Gdańsk, Polska


Nr publikacji MZ191002PL
Sierpień 2023



Najnowsze informacje o nas i naszych produktach można uzyskać za pośrednictwem mediów społecznościowych.