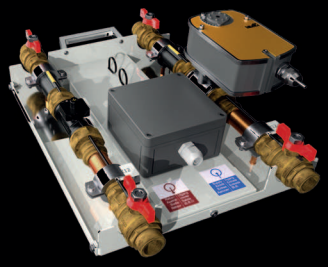
Rittal – The System.

Faster – better – everywhere.

LCP Rear Door CW





Aktivmodul

3314.020

3314.025

System Hardening Guide

DE

Inhaltsverzeichnis

1 Überblick 3
1.1 Was bedeutet Systemhärtung? 3
1.2 Ziele der Systemhärtung 3
1.3 Zweck des Dokuments 3
1.4 Geltungsbereich 3

2 Initiales Setup 3
2.1 Ändern Sie das Default Passwort 3
2.2 Verwenden Sie sichere Passwörter 3
2.3 Ungenutzte USB-Ports abschalten 3
2.4 Halten Sie die Software auf dem neuesten Stand 4

3 Services 4
3.1 Zeitsynchronisierung 4
3.2 HTTP deaktivieren und HTTPS konfigurieren 4
3.3 FTP deaktivieren und FTPS nur während aktiver Nutzung einschalten 4
3.4 Telnet deaktivieren 4
3.5 SNMPv1/v2 deaktivieren und SNMPv3 nur bei Bedarf abgesichert nutzen 5
3.6 Modbus TCP nur bei Bedarf abgesichert nutzen 5
3.7 OPC UA nur bei Bedarf abgesichert nutzen 5

4 Logging Einstellungen 6

5 Zugriff und Autorisierung 6

6 Netzwerk und Sicherheit 6
6.1 Halten Sie die Firmware der vernetzten Geräte auf dem aktuellen Stand 6
6.2 Produkte und Systeme nicht in öffentliche Netzwerke einbinden 6
6.3 Aktuelle Sicherheits-Software verwenden 6
6.4 Regelmäßige Bedrohungsanalyse durchführen 6

7 Quick Hardening Checkliste 7

1 Überblick

1.1 Was bedeutet Systemhärtung?

Das Bundesamt für Sicherheit in der Informationstechnik bezeichnet als Härten in der IT-Sicherheit „…die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind“.

Anders ausgedrückt: Die Systemhärtung dient dazu, Angriffsmöglichkeiten zu eliminieren, indem Schwachstellen gepatcht und nicht benötigte Dienste abgeschaltet werden.

1.2 Ziele der Systemhärtung

Die obersten Ziele der Systemhärtung sind die Reduzierung der Möglichkeiten zur Ausnutzung von Schwachstellen sowie die Minimierung von möglichen Angriffsmethoden. Als Nebeneffekt führt die Härtung oftmals zu einer Komplexitätsreduzierung und damit einhergehend zu einer Verringerung von Administrationsfehlern.

Produkte, Netzwerke und Systeme müssen vor unbefugtem Zugriff geschützt werden, um die Verfügbarkeit, Vertraulichkeit und Integrität von Daten zu gewährleisten.

1.3 Zweck des Dokuments

Die untenstehenden Handlungsleitlinien haben zum Ziel, eine sichere Konfiguration für das LCP Rear Door CW von Rittal einzurichten.

Das Dokument richtet sich an System- und Anwendungsadministratoren, Sicherheitsspezialisten, Auditoren sowie Helpdesk-Personal, das LCP Rear Door CW zu sichern.

Darüber hinaus können Sie weitere Informationen auf der offiziellen Website des Bundesamtes für Sicherheit und Informationstechnik finden:

– **BSI - IT-Grundschutz-Kompendium**
– **BSI - Allgemeine Empfehlungen**

1.4 Geltungsbereich

Die beschriebenen Maßnahmen beziehen sich hauptsächlich auf den sicheren Betrieb des LCP Rear Door CW im Netzwerk sowie die lokalen und netzwerkbasierten Schnittstellen.

2 Initiales Setup

Deaktivieren Sie grundsätzlich alle nicht benötigten Kommunikationskanäle auf dem Gerät. Für viele Protokolle stehen zudem sicherere Alternativen zur Verfügung – wir empfehlen, unsichere Varianten konsequent abzuschalten. In einigen Fällen kann das Sicherheitsniveau zusätzlich durch geeignete Konfigurationseinstellungen erhöht werden.

Um angemessene Schutzmaßnahmen zu definieren, ist es hilfreich, dass Sie sich einen vollständigen Überblick über alle vorhandenen Kommunikationswege und Schnittstellen verschaffen, da diese potenzielle Angriffsflächen darstellen können.

2.1 Ändern Sie das Default Passwort

Beschreibung:

Ähnlich wie bei Routern kommt auch beim LCP Rear Door CW von Rittal ein Standardpasswort zum Einsatz, mit dem auf das Gerät, während der Ersteinrichtung zugegriffen werden kann. Bleibt das ab Werk eingerichtete Passwort unverändert oder der damit verbundene Zugang trotz zusätzlichem Nutzer bestehen, ist die Angriffsfläche denkbar groß.

Empfehlung:

Standardkennwörter sind eine Art Platzhalter und sollten nur bei der Erstkonfiguration zum Einsatz kommen. Admins und Anwender sollten in jedem Fall bei der ersten Konfiguration das Standardkennwort ändern, um das Risiko zu reduzieren.

Abhilfe:

Seit der Softwareversion V8.23.00 wird der Benutzer beim erstmaligen Anmelden dazu aufgefordert, ein neues und sicheres Passwort zu vergeben. Sollte eine andere Softwareversion in Gebrauch sein, finden Sie weitere Informationen hierzu in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 7.2.2.

2.2 Verwenden Sie sichere Passwörter

Beschreibung:

Hacker haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um dies zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Empfehlung:

Orientieren Sie sich an den Empfehlungen des Bundesamt für Sicherheit und Informationstechnik zur Erstellung und zum Umgang mit Passwörtern.

2.3 Ungenutzte USB-Ports abschalten

Beschreibung:

USB-basierte Malware ist ein einfaches und gängiges Mittel zur Netzwerkinfiltration und ein erster Schritt zur Etablierung einer dauerhaften Bedrohung in einer Netzwerkumgebung.

Empfehlung:

Das Einschränken des USB-Zugriffs auf dem System verringert die physische Angriffsfläche für das Gerät und dadurch die Möglichkeit Malware einzuschleusen. Jegliche Anschlüsse dürfen NICHT nach außen gelegt

(z. B. außerhalb eines verschlossenen Schaltschranks), da dies zu einem erheblichen Sicherheitsrisiko führt!

Abhilfe:
Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf die USB-Anschlüsse haben und dass diese abgeschaltet sind, sofern diese nicht genutzt werden.

2.4 Halten Sie die Software auf dem neuesten Stand

Beschreibung:
Aktuelle Software reduziert die Zeitspanne, in der bekannte Schwachstellen ausnutzbar sind, und verringert die gesamte Angriffsfläche. Zudem enthalten neuere Versionen häufig zusätzliche Sicherheitsfunktionen, die in älteren Versionen noch nicht vorhanden waren.

Empfehlung:
Wann immer möglich, sollten Sie die Software auf die neueste Version aktualisieren.

Abhilfe:
Die aktuelle Software ist über die Produktseite des LCP Rear Door CW oder über unseren Service erhältlich. Eine Anleitung zum Durchführen eines Updates finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3 Services

3.1 Zeitsynchronisierung

Beschreibung:
Die Systemzeit sollte zwischen allen Systemen in einer Umgebung synchronisiert werden. Dies geschieht in der Regel durch die Einrichtung eines maßgeblichen Zeitservers oder einer Reihe von Servern, mit denen alle Systeme ihre Uhren synchronisieren.

Empfehlung:
Die Zeitsynchronisierung ist wichtig, um zeitabhängige Sicherheitsmechanismen zu unterstützen und um sicherzustellen, dass die Protokolldateien im gesamten Unternehmen über konsistente Zeitangaben verfügen, was bei forensischen Untersuchungen hilfreich ist.

Abhilfe:
Stellen Sie die Verbindung zu einem NTP-Server her, sofern dieser in Ihrem System in Gebrauch ist. Eine Anleitung zum Aktivieren und Einrichten einer Verbindung zu einem NTP-Server finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.2 HTTP deaktivieren und HTTPS konfigurieren

Beschreibung:
Das Hypertext Transfer Protocol (HTTP) sowie das Hypertext Transfer Protocol Secure (HTTPS) dienen der Kommunikation zwischen Webbrowsern und vernetzten Geräten, beispielsweise zur Bereitstellung von Benutzeroberflächen oder Konfigurationsmöglichkeiten.

Empfehlung:
HTTP ist grundsätzlich unsicher, da Daten – einschließlich Zugangsinformationen – unverschlüsselt übertragen werden und somit von Angreifern mitgelesen oder manipuliert werden können. Es wird daher dringend empfohlen, ausschließlich HTTPS zu verwenden. Dabei sollte sichergestellt werden, dass HTTPS mit einer aktuellen und sicheren Konfiguration betrieben wird – dies beinhaltet das Security Level „Modern“, da hier TLS 1.3 verwendet wird.

Abhilfe:
Deaktivieren Sie HTTP in den Geräteeinstellungen und aktivieren Sie ausschließlich HTTPS mit dem Security Level „Modern“. Eine detaillierte Anleitung hierzu finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.3 FTP deaktivieren und FTPS nur während aktiver Nutzung einschalten

Beschreibung:
Das File Transfer Protocol (FTP) und das File Transfer Protocol Secure (SFTP) bieten vernetzten Computern und Geräten die Möglichkeit, Dateien zu übertragen.

Empfehlung:
FTP ist generell unsicher, da eingegebene Kennwörter im Klartext, also völlig unverschlüsselt, übertragen werden. Es wird daher empfohlen, SFTP zu verwenden, wenn eine Dateiübertragung erforderlich ist. Sobald SFTP nicht mehr genutzt wird, sollte dieses auch abgeschaltet werden, um die Angriffsfläche zu reduzieren.

Abhilfe:
Deaktivieren Sie FTP und SFTP in den Einstellungen und lassen Sie es nur während der aktiven Nutzungszeit eingeschaltet. Eine Anleitung hierzu finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.4 Telnet deaktivieren

Beschreibung:
Über das Telnet-Protokoll können Verbindungen zu anderen Systemen hergestellt werden. Es dient der Fernkommunikation, überträgt jedoch sämtliche Daten unverschlüsselt.

Empfehlung:
Telnet gilt als unsicher, da keine Verschlüsselung der übertragenen Daten erfolgt. Dadurch besteht das Risiko, dass Anmeldeinformationen und andere sensible Daten von unbefugten Dritten abgefangen und missbraucht werden. Der Einsatz sollte daher grundsätzlich vermieden werden.

Abhilfe:
Deaktivieren Sie das Telnet-Protokoll in den Geräteeinstellungen, sofern es nicht zwingend benötigt wird. Eine Anleitung zur Deaktivierung finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.5 SNMPv1/v2 deaktivieren und SNMPv3 nur bei Bedarf abgesichert nutzen

Beschreibung:
Der SNMP-Server (Simple Network Management Protocol) wird verwendet, um auf SNMP-Befehle von einem SNMP-Verwaltungssystem zu warten, die Befehle auszuführen oder die Informationen zu sammeln und dann die Ergebnisse an das anfragende System zurückzusenden.

Empfehlung:
Der SNMP-Server kann mit SNMPv1/v2c oder v3 kommunizieren. Die Versionen v1/v2c sind jedoch unsicher. SNMPv1 überträgt zum Beispiel Daten im Klartext und es wird keine Authentifizierung zur Ausführung von Befehlen erfordert. Es wird dringend empfohlen, den Server so zu konfigurieren, dass SNMPv1/v2c nicht zugelassen werden.
In der vorliegenden Implementierung erfolgt die Authentifizierung über MD5 oder SHA-1, wobei beide Hash-Algorithmen als veraltet gelten und Schwächen aufweisen. Die Verschlüsselung erfolgt über DES oder AES, wobei auch DES als veraltet gilt und Schwächen aufweist.
Der Einsatz sollte daher nur in vertrauenswürdigen und abgesicherten Netzwerken erfolgen.

Abhilfe:
Deaktivieren Sie SNMPv1/v2c in den Einstellungen und aktivieren Sie die SHA-Authentifizierung und die Verschlüsselungstechnik AES unter der SNMPv3 Konfiguration. Es wird außerdem empfohlen, im Abschnitt „Allowed Hosts“ alle Hosts einzutragen, die per SNMP auf das Gerät zugreifen dürfen und die Standard-Communitys „public“ für SNMP zu überschreiben. Ist die „Allowed Hosts“ Liste leer, können alle Systeme über SNMP mit dem Gerät kommunizieren. Vergeben sie den „Allowed Hosts“ die benötigten Rechte (entweder read oder read/write). Eine Anleitung dazu finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.6 Modbus TCP nur bei Bedarf abgesichert nutzen

Beschreibung:
Modbus TCP ist ein weit verbreitetes Kommunikationsprotokoll in der industriellen Automatisierung zur Übertragung von Steuerungs- und Prozessdaten über IP-basierte Netzwerke.

Empfehlung:
Modbus TCP bietet standardmäßig keine integrierten Sicherheitsmechanismen wie Authentifizierung oder Verschlüsselung. Dadurch können Daten im Klartext übertragen und potenziell von unbefugten Dritten gelesen oder manipuliert werden.
Es wird daher empfohlen, Modbus TCP nur dann zu aktivieren, wenn es zwingend erforderlich ist. Zusätzlich sollten geeignete Schutzmaßnahmen wie Netzwerksegmentierung, Firewalls oder VPN-Verbindungen eingesetzt werden, um den Zugriff auf vertrauenswürdige Systeme zu beschränken.

Abhilfe:
Deaktivieren Sie Modbus TCP, sofern es nicht aktiv benötigt wird. Wenn der Einsatz erforderlich ist, stellen Sie sicher, dass der Zugriff durch die „Allowed Hosts“ Liste eingeschränkt wird. Ist die „Allowed Hosts“ Liste leer, können alle Systeme über Modbus TCP mit dem Gerät kommunizieren. Vergeben sie dem „Allowed Host“ die benötigten Rechte (entweder read oder read/write). Weitere Informationen zur Konfiguration finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

3.7 OPC UA nur bei Bedarf abgesichert nutzen

Beschreibung:
OPC UA (Open Platform Communications Unified Architecture) ist ein plattformunabhängiges Kommunikationsprotokoll für den sicheren und zuverlässigen Datenaustausch in industriellen Anwendungen.

Empfehlung:
In der vorliegenden Implementierung erfolgt die einzige mögliche Absicherung ausschließlich über Benutzername und Passwort, ohne zusätzliche Verschlüsselung der übertragenen Daten.
Dadurch besteht das Risiko, dass Kommunikationsinhalte im Netzwerk mitgelesen oder manipuliert werden können. Es wird daher empfohlen, OPC UA nur in vertrauenswürdigen und entsprechend geschützten Netzwerken einzusetzen.

Abhilfe:
Aktivieren Sie OPC UA nur, wenn es für den Betrieb erforderlich ist, und beschränken Sie den Zugriff auf autorisierte Benutzer durch starke Zugangsdaten.

Setzen Sie das Protokoll ausschließlich in abgesicherten Netzwerkumgebungen ein und begrenzen Sie den Zugriff über geeignete Netzwerkmaßnahmen. Ergänzende Maßnahmen wie Netzwerksegmentierung, Firewalls oder VPN-Verbindungen sollten genutzt werden, um die Kommunikation zusätzlich abzusichern.
Eine Anleitung zur Konfiguration finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

4 Logging Einstellungen

Beschreibung:
Das LCP Rear Door CW generiert Protokolle über Ereignisse und Status und speichert sie auf dem Gerät ab. Zum Beispiel werden Login und Logout Ereignisse aufgezeichnet, die einem Systemadministrator Informationen über Brute-Force-Angriffe auf Benutzerkonten liefern können.
In der Regel werden in einer Netzwerkumgebung mit vielen verschiedenen Anwendungen und Systemen eine Vielzahl komplexer Informationen erzeugt, dessen Auswertung und Überprüfung sich durch die Administratoren als schwierig gestalten kann.

Empfehlung:
Verwenden Sie in diesem Fall einen Syslog-Server bzw. eine dedizierte Protokollsoftware, die alle relevanten Informationen an einem Ort sammelt und archiviert. Stellen Sie sicher, dass TLS aktiviert ist, um sicher zu gehen, dass alle Datensätze verschlüsselt sind und das TCP aktiviert ist, um einen sauberen Datenverkehr zu gewährleisten.

Abhilfe:
Eine Anleitung, um grundlegende Einstellungen zum Versenden von Log-Meldungen an Syslog-Server durchzuführen, finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

5 Zugriff und Autorisierung

Beschreibung:
Eine effiziente Benutzerverwaltung schützt IT-Systeme und Daten vor unbefugten Zugriffen und teilt jedem Benutzer eine eindeutige Identifizierung zu.

Empfehlung:
Verwenden Sie nach Möglichkeit ein externes Benutzerverwaltungssystem (LDAP oder Radius) oder legen Sie für jeden Benutzer, für den eine Autorisierung unbedingt erforderlich ist, ein Benutzerkonto auf dem Gerät an und eine dazugehörige Benutzergruppe. Halten Sie die Benutzerkonten und die Benutzergruppen immer aktuell und deaktivieren Sie nicht verwendete Benutzerkonten.
Legen Sie hier auch die notwendigen Berechtigungen für die Nutzerkonten, abhängig von den Tätigkeiten, fest.
Benutzer, die einer Gruppe mit aktivierter Administratorrolle angehören, haben über die Weboberfläche uneingeschränkten Zugriff auf die gesamte Gerätekonfiguration sowie auf alle Einstellungen und können diese jederzeit ändern.
Aus diesem Grund wird dringend empfohlen, die Anzahl der Administratoren auf ein Minimum zu beschränken.
Benutzer mit Datentransferberechtigung haben Zugriff auf alle gespeicherten Daten und können diese bei aktiviertem Schreibzugriff auch verändern – unabhängig von der zugewiesenen Gruppe.

Abhilfe:
Eine Anleitung, um grundlegende Einstellungen für Benutzergruppen, einzelne Benutzer oder Benutzerverwaltungssysteme festzulegen, finden Sie in der Betriebsanleitung des LCP Rear Door CW unter dem Kapitel 8.6.

6 Netzwerk und Sicherheit

6.1 Halten Sie die Firmware der vernetzten Geräte auf dem aktuellen Stand

Stellen Sie sicher, dass die aktuelle Firmware auf den Geräten installiert ist, da diese bekannte Sicherheitsrisiken patcht und teilweise auch einen größeren Funktionsumfang bietet. Die Firmware finden Sie auf der Produktseite des jeweiligen Produktes.

6.2 Produkte und Systeme nicht in öffentliche Netzwerke einbinden

Betreiben Sie das System nicht direkt im Internet, sondern nur in internen Netzwerken, die durch Firewalls nach außen abgesichert sind. Sollte eine Einbindung Ihrer Produkte und Systeme über ein öffentliches Netzwerk erforderlich sind, verwenden Sie ein VPN.

6.3 Aktuelle Sicherheits-Software verwenden

Für die Identifizierung und Eliminierung von Sicherheitsrisiken wie Viren, Trojaner und anderer Schadsoftware, sollte auf allen PCs eine Sicherheitssoftware installiert sein und auf aktuellem Stand gehalten werden.

6.4 Regelmäßige Bedrohungsanalyse durchführen

Es wird empfohlen, regelmäßig Bedrohungsanalysen durchzuführen, um festzustellen, ob Ihre getroffenen Schutzmaßnahmen wirksam sind.

7 Quick Hardening Checkliste

Systemhärtung

– Alle nicht benötigten Dienste sind deaktiviert
– USB-Ports sind deaktiviert oder physisch geschützt und nicht nach außen geführt

Zugriff & Authentifizierung

– Default-Passwort wurde geändert
– Starke, individuelle Passwörter werden verwendet
– Nicht benötigte Benutzerkonten sind deaktiviert
– Anzahl der Administratoren ist minimal gehalten
– Die Berechtigungen der Nutzerkonten wurden auf das Notwendigste beschränkt
– Externes Benutzerverwaltungssystem ist integriert

Netzwerk & Datenübertragung

– HTTP ist deaktiviert
– HTTPS ist aktiviert (mit dem Security Level Modern)
– FTP ist deaktiviert
– SFTP nur bei Bedarf aktiviert
– Telnet nur bei Bedarf aktiviert

Services & Protokolle

– SNMPv1/v2c ist deaktiviert
– SNMPv3 ist korrekt konfiguriert und nur bei Bedarf aktiviert und in abgesicherten Netzwerken genutzt
– Modbus TCP ist korrekt konfiguriert und nur bei Bedarf aktiviert und in abgesicherten Netzwerken genutzt
– OPC UA ist korrekt konfiguriert und nur bei Bedarf aktiviert und in abgesicherten Netzwerken genutzt

Logging & Monitoring

– Verbindung zu einem NTP-Server ist hergestellt
– Logging ist aktiviert
– Logs werden an einen zentralen Syslog-Server gesendet
– TLS für Log-Übertragung ist aktiviert

Netzwerk-Sicherheit

– Zugriff ist über Firewall eingeschränkt
– Netzwerksegmentierung ist umgesetzt
– Gerät ist nicht direkt im Internet erreichbar
– Zugriff nur über definierte „Allowed Hosts“ über Modbus TCP und SNMPv3

Betrieb & Wartung

– Software ist auf aktuellem Stand
– Regelmäßige Bedrohungsanalysen werden durchgeführt
– Sicherheitssoftware ist auf angebundenen Systemen aktiv
– Zugriff von außen erfolgt ausschließlich über VPN

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.

www.rittal.com/contact

06.2025/System Hardening Guide LCP Rear Door CW/V1.0

RITTAL GmbH & Co. KG
Auf dem Stuetzelberg · 35745 Herborn · Germany
Phone +49 2772 505-0
E-mail: info@rittal.de · www.rittal.com