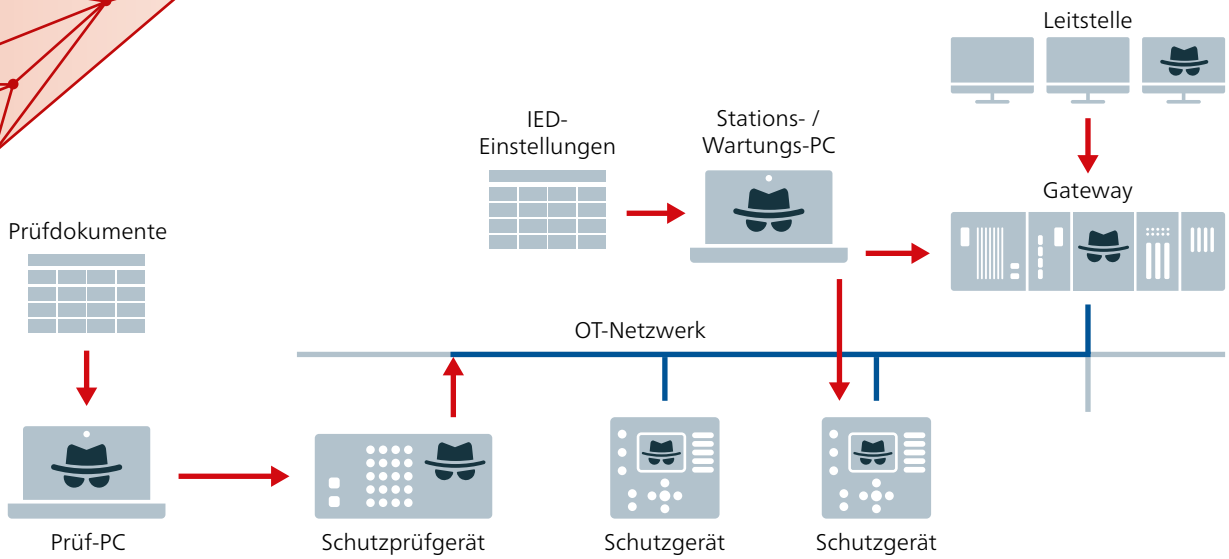
# CMC 500

## DAS ERSTE CYBER-GEHÄRTETE SCHUTZRELAISPRÜFGERÄT DER WELT




Bei unzureichendem Schutz bieten sich Angreifer:innen mehrere Möglichkeiten, um sich Zugriff auf den Stationsbus kritischer Intrastrukturen zu verschaffen.

Wer Schaltanlagen wirksam vor Cyberbedrohungen schützen möchte, muss einen ganzheitlichen Zugang wählen. Der Einsatz von cyber-sicheren Schutzrelaisprüfgeräten ist dabei ein essentieller Faktor, der in keinem Sicherheitskonzept fehlen darf. Erfahren Sie, warum das so ist und welche umfangreichen Maßnahmen wir gesetzt haben, um einen neuen Maßstab beim Thema Cybersicherheit in der Schutzprüfung zu etablieren.

Es gibt bereits genügend reale Fälle, die zeigen, dass Cyberangriffe auf kritische Infrastruktur nicht nur in Romanen vorkommen. Beim wohl bekanntesten Vorfall in der Ukraine 2016 nutzten Angreifer dafür beispielsweise die Verbindung zur Leitstelle aus. Solche Angriffe zeigen, dass der Schutz von kritischer Infrastruktur unerlässlich ist und inzwischen auch durch verschiedene gesetzliche Vorgaben gefordert wird. In der EU setzt beispielsweise die NIS2-Richtlinie (Network and Information Security) den Rahmen für Maßnahmen zur Verbesserung der Cybersicherheit in diesem Bereich.

Die Grundlage für die Härtung der Anlagen stellt dabei eine umfassende Bedrohungsanalyse dar, die möglichst alle Angriffsvektoren und Schwachstellen zu erfassen versucht. Denn wie eine Studie des Ponemon Institute gezeigt hat, wurden bei 100 % der untersuchten Angriffe bekannte Schwachstellen ausgenutzt. Alle Schwachstellen zu eliminieren stellt für Energieversorger jedoch eine echte Herausforderung dar, da es etliche Angriffsvektoren gibt (siehe Bild oben), wie beispielswiese:

- die Verbindung zur Leitstelle und Fernwartungszugänge,
- Stations- und Wartungscomputer,
- die Firmware und Einstellungsdateien der Schutzgeräte selbst
- als auch Prüfgeräte die in den Anlagen zum Einsatz kommen.

Während das Bewusstsein hinsichtlich Cybergefahren mittlerweile vorhanden ist, wird bei näherer Betrachtung allerdings klar, dass es zum Teil an spezifischen Lösungen mangelt.

Bei der Schutzprüfung stellen sowohl das Schutzprüfgerät als auch der Prüflaptop Angriffsvektoren dar, die ausgenutzt werden könnten. Ein sicheres Prüfgerät bietet dabei den Vorteil, dass sich beide Angriffspfade

*»Um bei einem Produkt von ›Cybersecurity-by-Design‹ sprechen zu können, braucht es mehr als nur Maßnahmen auf Hard- und Softwareebene.* ***Die Analyse möglicher Angriffsvektoren muss auf Unternehmensebene starten und alle involvierten Prozesse umfassen.«***

adressieren lassen. Bisher gab es allerdings schlicht kein cybersicheres Schutzprüfgerät auf dem Markt – mit unserem neuen CMC 500 steht jetzt eine Lösung zur Verfügung.

### Angriffsvektor Prüfgerät

Mit dem CMC 500 haben wir uns diesem Thema angenommen und das erste cyber-gehärtete Schutzrelaisprüfgerät der Welt entwickelt. Aber welche Maßnahmen sind dafür notwendig? Was verstehen wir unter cyber-sicher? Analog zur Bedrohungsanalyse bei kritischer Infrastruktur war der erste Schritt die Identifikation möglicher Angriffsvektoren bei Prüfgeräten, um diese anschließend Schritt für Schritt zu adressieren. Die jahrelange Erfahrung die wir mit StationGuard, unserem auf den Energiesektor maßgeschneiderten Intrusion Detection System (IDS), in diesem Bereich gesammelt haben, war dafür äußerst hilfreich. Um ein höchstmögliches Maß an Cybersicherheit zu erreichen, war für uns klar, dass wir auch bei der Entwicklung des CMC 500 einem holistischen Ansatz folgen. Dafür haben wir Maßnahmen auf Unternehmens-, Prozess-, Produktions-, Software- und natürlich auch der Hardwareebene gesetzt. Im Zusammenspiel werden diese dem Schlagwort „Cybersecurity-by-Design" mehr als gerecht.

### Sichere Prüfhardware

Auf Hardwareebene setzt das CMC 500 auf ein ISO/IEC-11889-konformes Trusted Platform Module (TPM 2.0). Dieser Kryptoprozessor stellt die Voraussetzung für mehrere Sicherheitsmaßnahmen dar, da auf ihm diverse Schlüssel und Zertifikate sicher gespeichert werden können. Dadurch lässt sich einerseits eine zuverlässige Verschlüsselung der Kommunikation gewährleisten und andererseits wird die eindeutige Identifikation des Prüfgeräts möglich – wie bei einem Fingerabdruck. Angriffe wie Machine-in-the-middle-Attacken können so unterbunden werden. Ebenso lassen sich während des Bootvorgangs, mittels „Secure Boot" und „Measured Boot", Checks durchführen, die die Authentizität der Firmware überprüfen und den Start des Geräts verhindern, wenn diese fehlschlagen. Auf einer weiteren Ebene kann zusätzlich die gesamte Kommunikation durch das Setzen eines Passworts geschützt werden.

### Sichere Prüfsoftware

Eine gehärtete Hardware kann ihren Zweck allerdings nicht ohne die entsprechende Prüfsoftware erfüllen. Deshalb erfolgt auch deren Entwicklung nach klaren Regeln. Unser Secure-Software-Development-Life-Cycle(SSDLC)-Prozess, der mit der Entwicklung von StationGuard eingeführt wurde, sorgt für eine hohe Qualität und Sicherheit des Codes. Zudem definiert er den Umgang mit potenziellen Schwachstellen und deren Veröffentlichung. Transparenz stellt dabei einen wesentlichen Eckpfeiler dar, um die Cybersicherheit unserer Produkte zu gewährleisten.

Mehr Informationen zum Umgang mit Schwachstellen finden Sie auf omicronenergy.com/product-security.

### Sichere Produktion und Reparatur

Auch bei der Produktion und Reparaturen setzen wir nicht nur auf ausgewählte Zulieferer und vertrauenswürdige Partner, sondern nehmen die entscheidenden Schritte selbst in die

Hand. So sind nur einige wenige autorisierte Mitarbeiter:innen befugt, die Zertifikate und Schlüssel auf dem CMC 500 einzurichten. Dabei ist der Prozess so aufgesetzt, dass er ohne Unterbrechung abläuft, um jegliche Manipulation währenddessen zu unterbinden. Zusätzliche intern entwickelte Softwaredienste sorgen mithilfe eines Hardware Security Module (HSM) dafür, dass keine Schlüssel entwendet werden können. Jeder Versuch, physisch auf die Schlüssel im HSM zuzugreifen, führt dabei zu deren Zerstörung. Der gesicherte Serverraum, in dem sich die Module befinden, komplettiert die umfassenden Sicherheitsmaßnahmen in diesem Bereich.

### Sichere Prozesse im ganzen Unternehmen

Egal ob bei der Entwicklung der Hardware, der Software, in der Produktion oder der Reparatur, bei all diesen Prozessen stehen Menschen im Mittelpunkt. Deren Sensibilisierung in Bezug auf Daten- und IT-Sicherheit ist einer der wichtigsten Faktoren, um Cyberkriminellen das Leben schwer zu machen. Daher sind unsere Mitarbeiter:innen nicht nur entsprechend geschult, sondern müssen ihr Wissen und ihre Fähigkeiten im Rahmen von internen Phishing-Simulationen aber auch während ISO/IEC 27001 Audits regelmäßig unter Beweis stellen.

### Cybersicherheit neu definiert

Um bei einem Produkt von „Cybersecurity-by-Design" sprechen zu können, braucht es mehr als nur Maßnahmen auf Hard- und Softwareebene. Die Analyse möglicher Angriffsvektoren muss auf Unternehmensebene starten und alle involvierten Prozesse umfassen. Beim CMC 500 sind wir genau diesen Weg gegangen und begleiten auch den gesamten Produktlebenszyklus mit entsprechenden Maßnahmen, wie beispielsweise dem Management von Schwachstellen. Für den Angriffsvektor Prüfgerät steht damit eine Lösung zur Verfügung, die ihresgleichen sucht: das CMC 500 als erstes cyber-gehärtetes Schutzrelaisprüfgerät auf dem Markt.

Hier erfahren Sie mehr über das neue CMC 500!

omicron.energy/new-cmc

***»Der Kryptoprozessor stellt die Voraussetzung für mehrere Sicherheitsmaßnahmen dar,** da auf ihm diverse Schlüssel und Zertifikate sicher gespeichert werden können.«*