prego.SECaaS

Der modulare Cybersecurity-Ansatz

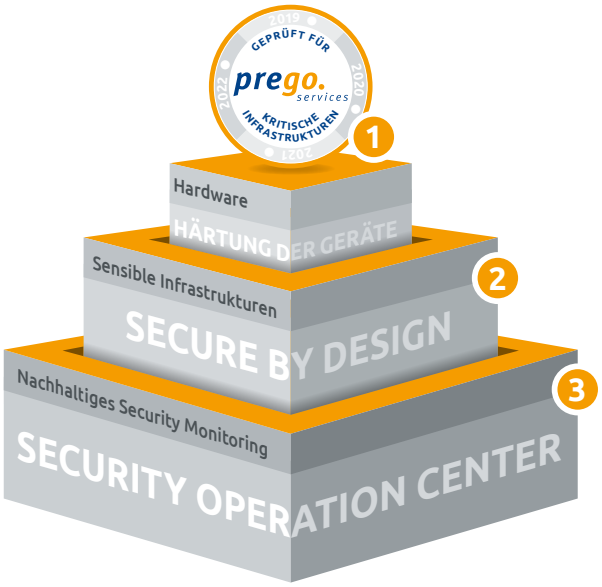
Nachhaltige Sicherung sensibler Infrastrukturen in der Energiebranche

Die Bedrohungslage wird immer komplexer

Nach wie vor ist die Bedrohungslage im Bereich Cybersecurity sehr hoch. Neue moderne Angriffsmethoden stellen die Systeme dabei immer wieder vor neue Herausforderungen.
Wir selbst haben in unserem Security Operations Center vermehrte Angriffe auf unsere Systeme registriert; die allgemeinen Prognosen gehen von einer stetigen Zunahme aus. Hinzu kommt die immer größere Angriffsfläche in den Infrastrukturen durch die zunehmende Digitalisierung der eingesetzten Geräte. Darüber hinaus schaffen die divergierenden Anforderungen an Flexibilität und Mobilität ganz neue Bedrohungsszenarien, auf die die Akteure der Energiewirtschaft reagieren müssen.

Inhouse-Ressourcen nicht ausreichend

Viele Energieversorgungsunternehmen haben lediglich den Standard Security Schutz (Firewall, Virenscanner und Verschlüsselung) im Einsatz. Die Sicherheitsanforderungen zum Schutz kritischer Infrastrukturen werden jedoch immer komplexer. Aus Erfahrung wissen wir, dass die installierten Firewalls hier sehr schnell an ihre Grenzen geraten. Deshalb haben wir ein modulares System geschaffen, das Sie ganz gezielt zuschalten können, um Ihre Cybersicherheit zu optimieren. Wir gehen hierbei von drei unterschiedlichen Ebenen aus, die vernetzt zu betrachten sind.



Modulsystem schafft Cybersicherheit

Dreistufiger skalierbarer Qualifizierungsprozess zum nachhaltigen Schutz Ihrer Infrastruktur

- **Stufe 1 – Hardware**
  - Prüfung und Härtung der IP-basierten Geräte in Ihrem System
- **Stufe 2 – Sensible Infrastrukturen**
  - Sicherung des Netzwerks durch bspw. Segmentierung der Infrastruktur in Zonen und DMZ
  - Beraten, planen, bauen, betreiben von Secure by Design-Infrastrukturen
- **Stufe 3 – Nachhaltiges Security Monitoring**
  Monitoring/Betreuung und kontinuierliche Anpassung an die Bedrohungslage mit:
  - Security Information & Event Management (SIEM)
  - Malware-Erkennung
  - Sicherheitsbetrachtung, Forensik, Penetrationstests

prego. services

Der modulare Cybersecurity-Ansatz

Nachhaltige Sicherung sensibler Infrastrukturen in der Energiebranche

Stufe 1
Härtung der Geräte

Sicherheitsbewertung vorhandener und Integration neuer Hardware im Rahmen der Absicherung Ihrer kritischen Netzwerke
Unser Qualifizierungsprozess ist praxiserprobt und entspricht dem gewünschten ISMS-Sicherheitsniveau für Energieunternehmen. Eine von uns geprüfte Hardware erhält ein prego Prüfzertifikat und kann unter Berücksichtigung des zuvor erarbeiteten Sicherheitskonzepts in Ihrem Netzwerk verwendet werden.

Der Qualifizierungsprozess umfasst folgende Aspekte:

- Prüfung der Schutzziele, Vertraulichkeit, Integrität und Verfügbarkeit bei der zu untersuchenden Hardware
- Hardware-Penetrationstest, um Sicherheitslücken und Schwachstellen zu erkennen
- Prüfung der Compliance von Sicherheitsanforderungen der Hardware
- Überprüfung der Monitoring-Eigenschaften der neuen Hardware, um Cyberangriffe frühzeitig zu erkennen und schnellstmöglich zu reagieren
- Integration der Hardware in die Sicherheitsprozesse, z. B. Patchmanagement zur Vorbeugung von Sicherheitslücken

Die neuen Herausforderungen für die Digitalisierung sind vielschichtig. Deshalb ist es wichtig, jedes IP-Gerät im Netzwerk zu prüfen, um Schwachstellen zu erkennen und zu analysieren.

prego. services

Der modulare Cybersecurity-Ansatz

Nachhaltige Sicherung sensibler Infrastrukturen in der Energiebranche

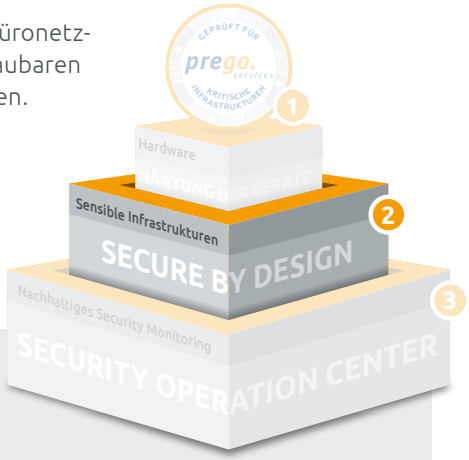
Stufe 2
Secure by Design

Secure by Design ist unsere Kernphilosophie, die wir gemeinsam mit unseren Kunden angehen und aktiv umsetzen. Dabei sind das Gesamtsystem und die Einzelkomponenten für optimale Sicherheit konzipiert und aufgebaut. So werden von vornherein Sicherheitslücken ausgeschlossen. Weiterhin betrachten wir die Systemlandschaften aus Redundanzgesichtspunkten, um sicherheitsrelevante Funktionen nachhaltig zu gewährleisten. Durch die Bündelung von Schutzmaßnahmen zu integrierten Ebenenkonzepten schaffen wir gestaffelte Sicherheitslösungen für nachhaltigen Cyberschutz.

Definition der zu prüfenden Systemlandschaft
Vor dem Qualifizierungsprozess ist zu prüfen, für welches Netz die Untersuchung durchgeführt werden soll:

- **Prozessnetzwerke**
  Bei Prozessnetzwerken wird oftmals ein höheres Schutzniveau gefordert als bei einem Büronetzwerk. Der Grund dafür ist, dass Prozessnetzwerke bisher als Inselnetzwerke mit überschaubaren Kommunikationsbeziehungen und scharfen Grenzen zur Außenwelt implementiert wurden. Durch die Digitalisierung wird die Infrastruktur angreifbarer, offener für die Außenwelt und die Geräte sind in der Regel auch länger im Einsatz.

- **Büronetzwerke**
  Büronetzwerke hingegen sind vielschichtiger in ihrer Infrastruktur, haben Unmengen an Kommunikationsbeziehungen und eine größere Angriffsfläche für Cyberkriminalität.



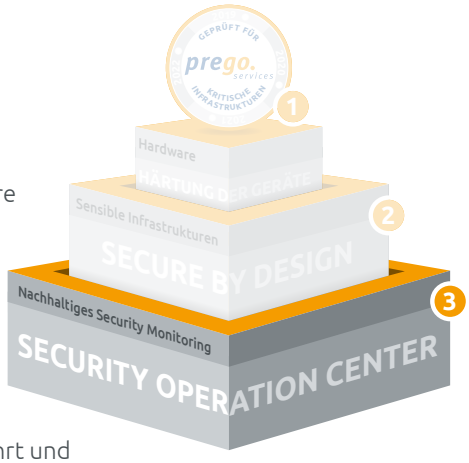
Unser Experten-Team berät, plant, baut und betreibt nachhaltige Systemarchitekturen für unsere Kunden und schafft so maßgeschneiderte, sichere Systemlandschaften für alle relevanten Anwendungen – dokumentiert, geprüft und sicher.

prego. services

Der modulare Cybersecurity-Ansatz

Nachhaltige Sicherung sensibler Infrastrukturen in der Energiebranche

Stufe 3
Security Operation Center (SOC)



Als fortlaufende Sicherheitseinrichtung Ihrer Systemlandschaften bieten wir Ihnen unsere SOC-Dienstleistungen an. Damit erhalten Sie ein umfassendes Monitoring, das sich kontinuierlich an die Bedrohungslage anpasst und Ihnen eine nachhaltige Sicherung Ihrer IT-Infrastrukturen ermöglicht. Diese Services können Sie wie folgt untergliedern und zu Ihrem eigenen Security-Konzept hinzubuchen:

- **Security Information & Event Management SIEM**
  Gezielte Analyse und Bewertung von Sicherheitsmeldungen und Schwachstellen. Dabei wird aufgrund von Use Cases eine ständige Prüfung auf Cyberangriffe durchgeführt und ggf. im Ernstfall alarmiert. Darüber hinaus erfolgt eine Analyse der Log-Daten, die gemeinsam mit der Erarbeitung von USE-Cases die Grundlage für die Erstellung eines Playbooks zur Abwehr von Angriffen bildet.

- **Anomalie- und Malware-Erkennung**
  Hier liegt der Fokus auf der Erkennung von Malware-Infektionen und deren Ausbreitung im Netz. Hierbei analysieren wir den Netzwerkverkehr und erkennen frühzeitig Anomalien in den Systemen. Die Verwundbarkeit und Schwachstellen des Internet, Darknet-Zugriffe oder menschliche Anwenderfehler bieten ein wachsendes Risikopotential. Nur durch die permanente Überwachung, Prüfung des digitalen Fußabdrucks und einer laufenden Bewertung der jeweiligen Risikoanalyse durch geschulte Experten im laufendem Betrieb kann den Gefahren entgegengewirkt werden.

- **Security-Expertenberatung**
  Wann immer Sie Fragen haben, Sicherheitsfälle oder Unsicherheiten auftreten, können Sie sich an unser Security-Team wenden. Diese ausgewiesenen Experten sind neben ihrer Expertise vor allem in die nationalen und internationalen Cybersecurity-Expertennetzwerke eingebunden und so hinsichtlich der aktuellen Bedrohungen immer up to date.
  Sie unterstützen Sie gerne bei einem Notfall oder auch bei der Forensik.

Haben Sie Fragen zu unserem modularen Cybersecurity-Ansatz?

Wir helfen Ihnen gerne weiter.

Kontakt

prego services GmbH
Neugrabenweg 4 · 66123 Saarbrücken
Franz-Zang-Straße 2 · 67059 Ludwigshafen
0681 95943-1265
vertrieb@prego-services.de
www.prego-services.de
info@prego-services.de

prego. services

Stand: 03/2021 v2