OPEN SKIES

Genau meine Lösung.

Security Operations Center (SOC)

Richtig aufgestellt im Kampf gegen Cyber-Attacken!

Effizientes Erkennen, Bewerten und Beheben systembasierter IT-Risiken

Die Cyber-Bedrohung steigt von Jahr zu Jahr und wird immer komplexer. Laut Bitkom-Studie haben die Schäden aufgrund von Cyber-Angriffen von 2017 bis 2019 nochmals um 27 % zugenommen, d. h. 2019 waren 70 % aller deutschen Unternehmen betroffen. Fast täglich berichten auch die Medien von neuen Herausforderungen und gezielten Attacken auf Unternehmen. Vor allem die zunehmende Digitalisierung in der Arbeitswelt und im wirtschaftlichen Umfeld schafft immer größere Angriffsflächen für Hackerattacken, die für Schäden in Millionenhöhe sorgen. Cyber-Kriminalität wird dadurch immer mehr zum größten Unternehmensrisiko!

Der Lagebericht des BSI 2019 zur IT-Sicherheit in Deutschland bestätigt die Bedrohungslage:

- Täglich bis zu 110.000 Bot-Infektionen deutscher Systeme
- 11,5 Mio. Meldungen zu Schadprogramm-Infektionen
- 40 Mio. Schaden erlitt ein einzelnes Unternehmen durch einen Ransomware-Angriff
- 114 Mio. neue Schadprogramm-Varianten
- Starke Zunahme von Identitätsdiebstählen im Netz

Schwierige Ausgangslage

Während die Angriffe immer ausgefeilter und vielfältiger werden, verlassen sich die meisten Unternehmen auf einen Basisschutz aus Firewall, Virenscanner und Datenverschlüsselung. Ein fataler Irrtum, **denn die reine Abwehr ohne professionelle Datenanalyse reicht nicht mehr aus**, um Cyber-Angriffe abzuwehren. Bitkom und BSI empfehlen deshalb eine Datenanalyse als weiterreichende Maßnahme zum Schutz der kritischen Systeme.

Verteidigung gegen Cyber War

Der Schutz der IT-Systeme durch technische Mittel wie:

Virenscanner | Datenverschlüsselung | Firewalls

reicht alleine nicht mehr aus!

Empfohlen wird von Bitkom, BSI, ...

Datenanalyse

prego. services

Security Operations Center (SOC)

Richtig aufgestellt im Kampf gegen Cyber-Attacken!

Effizientes Erkennen, Bewerten und Beheben systembasierter IT-Risiken

Schwachpunkte der EVUs

Schlechtes Monitoring und Logging
Zum Beispiel: Angriffe werden vom Admin nicht registriert, da kein zentrales Sicherheits-monitoring stattfindet.

Fehlende Netzwerkverkehrsanalyse
Zum Beispiel: Der Schadcode möchte „nach Hause telefonieren" und Kontakt mit dem Hacker aufnehmen – auf Grund der fehlenden Netzwerkanalyse werden Command- und Control-Zugriffe nicht erkannt und die Kommunikation nicht verhindert.

Das SOC als zentrale, operative Einheit im Kampf gegen Cyber-Angriffe

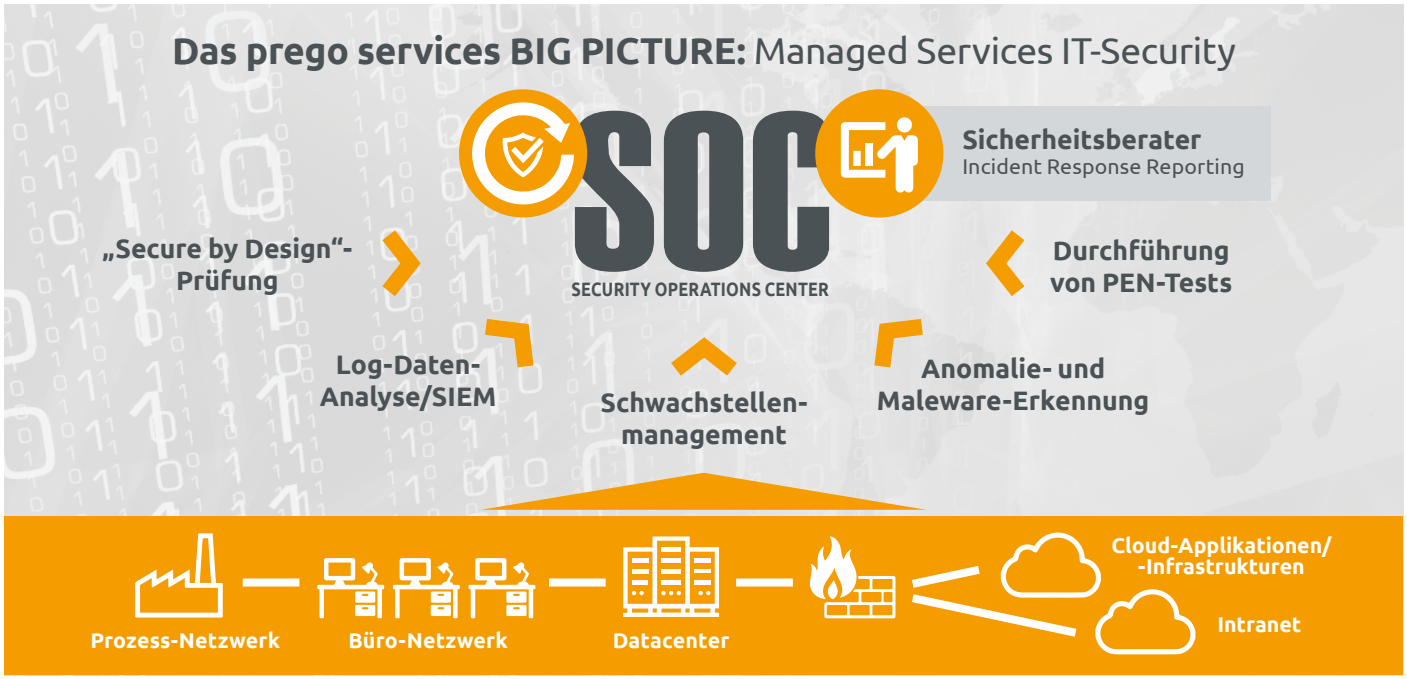
Cybersecurity ist ein hoch relevantes Thema, mit dem sich prego services als erfahrener IT-Spezialist für kritische Systeme im Energiemarkt schon lange intensive beschäftigt. Dabei konzentrieren wir uns derzeit auf die sich stetig verändernden Angriffstechniken von Hackern und übernehmen für unsere Kunden die **Verteidigung im Cybersecurity-Umfeld**. Aktuelle Geschehnisse und Angriffe zeigen, wie schnell Unternehmen lahmgelegt werden können und welche enormen wirtschaftlichen Schäden entstehen können.

Geheimwaffe SOC

Mit dem Security Operations Center (SOC) bietet prego services die perfekte Lösung, um die sich ständig ändernde Bedrohungslage besser zu überblicken und rechtzeitig darauf reagieren zu können:

- ☑ Das SOC analysiert die Daten
- ☑ Das System erkennt Angriffe auf Basis von Security USE Cases oder Traffic-Verhaltensanalysen und alarmiert, informiert und reagiert umgehend
- ☑ Egal ob stationäre Datensysteme oder Cloud-Plattformen – das SOC ist ein umhüllendes System und kann an alle vorhandenen IT-Infrastrukturen angeschlossen werden.

Das prego services BIG PICTURE: Managed Services IT-Security



Wir arbeiten mit den BSI-Initiativen zusammen

Teilnehmer UP KRITIS

Allianz für Cyber-Sicherheit

prego. services

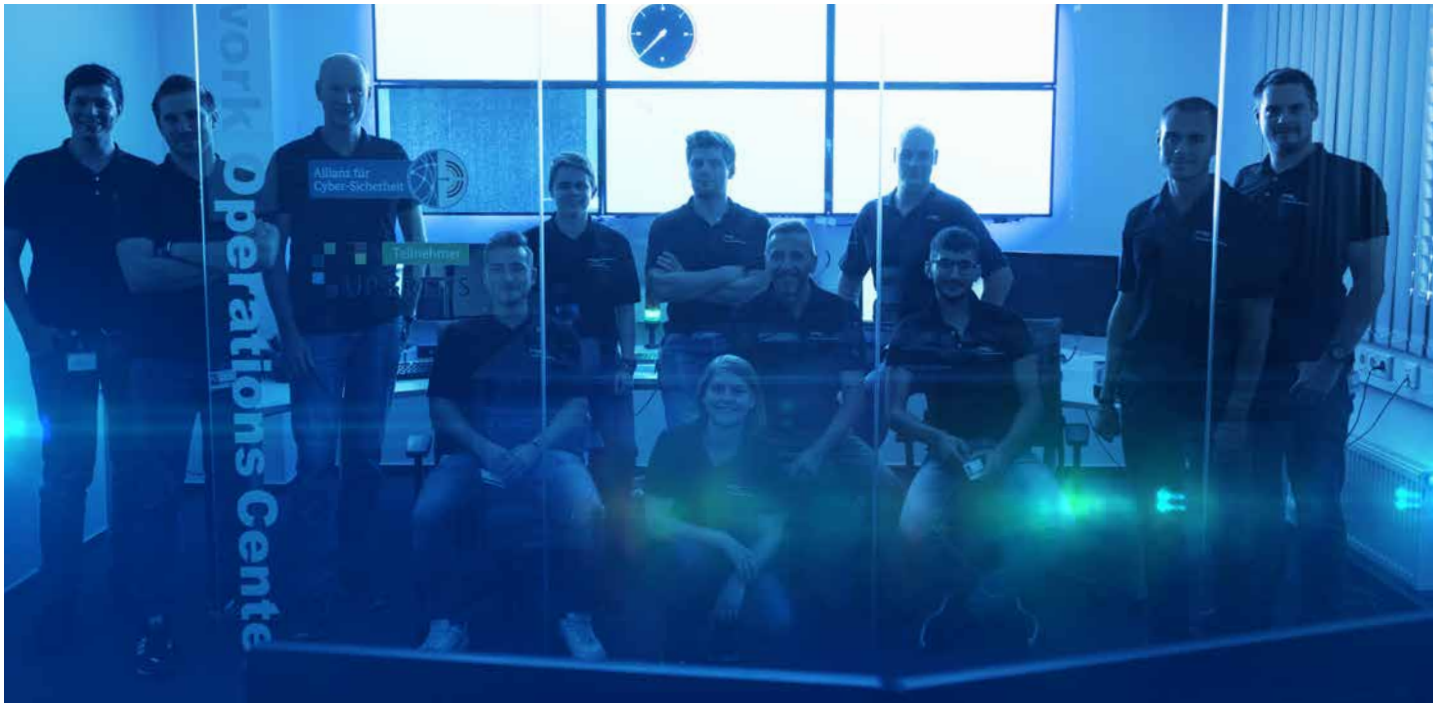
Security Operations Center (SOC)

Richtig aufgestellt im Kampf gegen Cyber-Attacken!

Effizientes Erkennen, Bewerten und Beheben systembasierter IT-Risiken

Fakten und Kennzahlen

- Alle Serviceprozesse aus deutschen Standorten (Saarbrücken, Ludwigshafen)
- ITIL-basierende Service-Prozesse
- Eigene, physikalisch besonders gesicherte Arbeitsbereiche
- ISO-27001-Zertifizierung
- Teilnehmer KRITIS und Allianz für Cyber-Sicherheit, Teilnahme BSI Übungszentrum Netzverteidigung



Das prego services Security Operations Center ist eine der Lösungen innerhalb unseres Open-Skies-Ansatzes für den Mittelstand, der Unternehmen einen einfachen und sicheren Zugang zur Cloud-Strategie ermöglicht. Unser Ansatz umfasst vernetzte IT-Infrastrukturen, modulare Cybersecurity-Lösungen, IT as a Service und maßgeschneiderte Cloudstrategien.
Lernen Sie die nachhaltigen Vorzüge von Open Skies kennen und sprechen Sie uns an!

Haben Sie Fragen zu unserem Security Operations Center?
Wir helfen Ihnen gerne weiter.

Kontakt

Heinz Pecis · Key Account Manager
Tel.: 0681 95943-1270 · Fax: 0681 95943-1212
Mobil: 0151 46711219
E-Mail: heinz.pecis@prego-services.de

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

prego. services