Cyber SafeAlert – detektiert kontinuierlich IT-Risiken

DEKRA

DEKRA Cyber SafeAlert.
IT Security Monitoring für den Mittelstand

Mit vielseitigen Chancen und Herausforderungen digitalisieren sich Geschäftsprozesse und Produktionsabläufe im Mittelstand. Dabei gilt es stets, die Zeichen der Zeit zu erkennen, innovativ zu handeln und gleichzeitig potentielle Risiken im Blick zu behalten sowie Informationssicherheit und Rechtskonformität zu gewährleisten. Werte, die zunehmend an Bedeutung gewinnen.

Etablierte Sicherheitsvorkehrungen, wie Firewalls und Antivirussoftware, erkennen feste Muster. Heutzutage gilt es, Unregelmäßigkeiten zu identifizieren, sie zu strukturieren und zu priorisieren um sich gezielt vor ihnen schützen zu können.

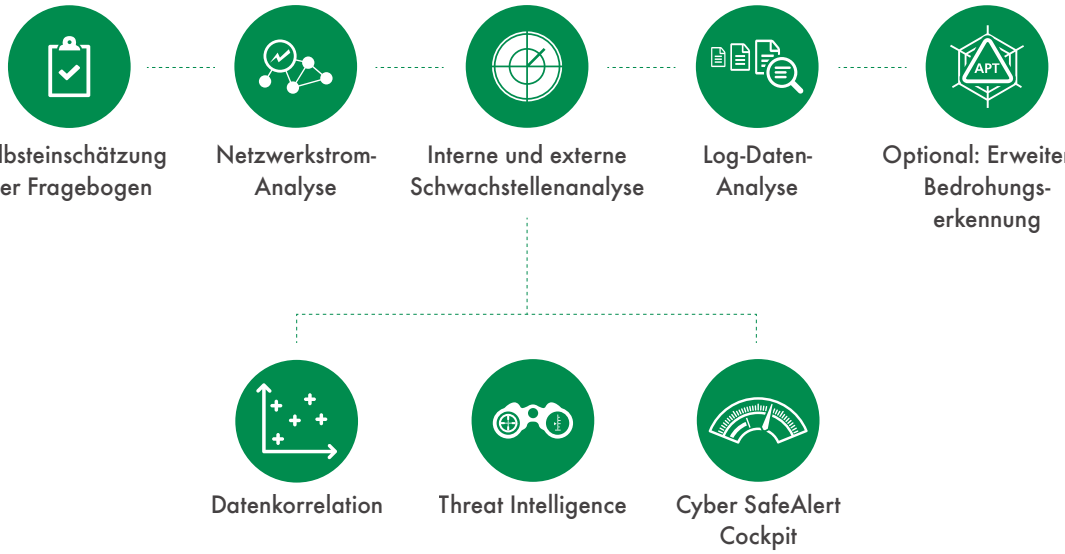
Kleinen und mittelständischen Unternehmen bietet DEKRA Cyber SafeAlert, ein technisches IT-Monitoring-System, entwickelt von den Experten in Europas größtem Kompetenzzentrum für IT-Sicherheit.

Es detektiert kontinuierlich IT-Risiken und meldet zeitnah Auffälligkeiten, Sicherheitslücken und Angriffe. Im Cockpit sind priorisierte Ergebnisse und Handlungsempfehlungen strukturiert für Sie in Ihrer Landessprache in verständlicher Form aufbereitet. Nach Bedarf ziehen Sie IT-Experten hinzu.

Mit Ihnen gemeinsam führen wir eine Schwachstellen- und Risikoanalyse durch. Anschließend wird die Cyber SafeAlert Box installiert, die in Ihr Firmennetzwerk eingebunden ist. Diese Hardware-Box registriert nun kontinuierlich Daten, die auf Sicherheitsrisiken hindeuten können. Aus dem Cockpit lassen sich unautorisierte Zugriffe und Schwachstellen ablesen und letztendlich Schutzmaßnahmen ableiten. So behalten Sie immer alles im Blick und Ihre Daten und Informationen in Sicherheit.

Vorteile auf einen Blick:

- Kontinuierliches, zentral gesteuertes, voll automatisiertes IT Security Monitoring
- Cockpit mit Behebungsanleitungen für Sicherheitsprobleme in Landessprache
- Verschiedene Leistungspakete für individuelle Budgetvorgaben



Selbsteinschätzung per Fragebogen.

Neben Erkenntnissen aus der automatisierten Risiko-analyse werden Rahmenfaktoren Ihrer IT-Sicherheit mit einbezogen.

Netzwerkstromanalyse.

Signatur- und verhaltensbasierte Analyse von gefährlicher Malware und anderen Risiken im Netzwerkverkehr.

Externe und interne Schwachstellenanalyse.

Kontinuierliche externe und interne Scans erkennen bestehende Schwachstellen in Ihrer IT und berichten sie, sodass Sie sie strukturiert beheben können.

Logdaten-Analyse.

Logs sind eine wichtige Quelle, um sicherheitsrelevanten Ereignissen auf die Spur zu kommen. Deshalb werden sie gesammelt, analysiert, korreliert und resultieren ge-gebenenfalls in Alarmierungen.

Optional: Erweiterte Bedrohungserkennung (Email/Web)

Analyse von Web-Downloads und/oder E-Mail-Anhängen.

Datenkorrelation

Sicherheitsrelevante Daten werden mit Hilfe einer umfassenden Korrelation aus der großen Datenmasse extrahiert. Korreliert werden Daten dabei sowohl innerhalb eines Risikoerkennungs-moduls als auch übergreifend über mehrere Module hinweg.

Threat Intelligence

Bringt die aktuellen sicherheitsrelevanten Informationen zusammen.

Cyber SafeAlert Cockpit

Alle gewonnenen Erkenntnisse werden zentral, verständlich und übersichtlich im Cyber SafeAlert Cockpit präsentiert. Sie sind priorisiert und mit Behebungshinweisen versehen. So wissen Sie, was wann zu tun ist.

DEKRA Assurance Services GmbH

Weltweit führt DEKRA Assurance Services Audits und Assessments entlang der Lieferkette durch. Damit können Unternehmen den Grundstein für eine erfolgreiche, nachhaltige Zukunft ihres Betriebs legen.

Neben maßgeschneiderten Assessments für die Bereiche Daten-schutz, Qualität, Gesundheit und Umwelt, Gefahrstoffmanagement und Produktlebenszyklus bietet DEKRA Assurance Services Beratungsleistungen zum Chemikalienrecht und Gefahrstoff-management.

DEKRA Assurance Services GmbH
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-3333
assurance-services.de@dekra.com

www.dekra.de

05/2020