DEKRA CyberSafeAlert

IT Security Monitoring für den Mittelstand

DEKRA

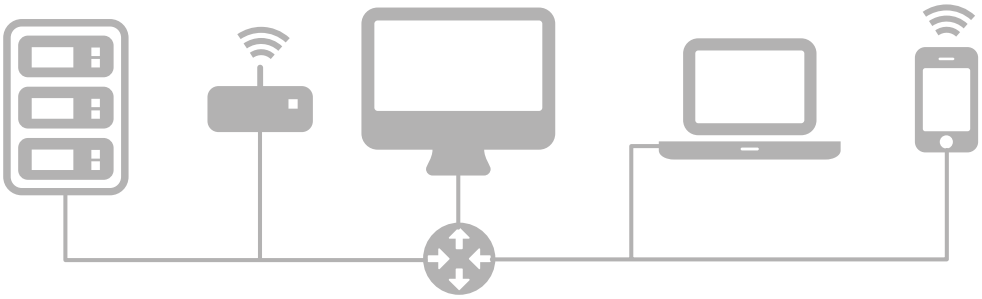
Cyber SafeAlert – detektiert kontinuierlich IT-Risiken.

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.



Selbsteinschätzung per Fragebogen

Netzwerkstrom-Analyse

interne und externe Schwachstellenanalyse

Log-Daten-Analyse

Optional: Erweiterte Bedrohungserkennung

Datenkorrelation

Threat Intelligence

Cyber SafeAlert Cockpit

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 Risikoanalyse werden Rahmenfaktoren Ihrer IT-Sicherheit mit einbezogen.

Wie groß ist aktuell die Gefahr, dass Ihr Unternehmen Schäden durch einen Cyberangriff erleiden könnte? Cyber SafeAlert ermöglicht Ihnen den Überblick über die Fakten, die Ihrem aktuellen IT-Risiko zugrunde liegen. Dazu gehören nicht nur die Erkenntnisse, die aus der automatisierten Risikoanalyse mit Hilfe unserer Werkzeuge gezogen werden. Auch Rahmenfaktoren, die Ihre IT-Sicherheit bestimmen, sind entscheidend. Organisatorische Details innerhalb und außerhalb Ihres Unternehmens werden regelmäßig im Rahmen einer einfachen und verständlichen Selbsteinschätzung abgefragt und in die Risikoanalyse einbezogen.

Netzwerkstromanalyse

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

Daten werden ständig aus dem Internet empfangen und an das Internet gesendet. Das betrifft nicht nur die von Ihnen bewusst gesendeten und empfangenen Daten. Auch Angreifer nutzen diesen Austausch. Cyber SafeAlert erkennt verdächtige Muster und Anomalien wie z.B. Malware, Command and Control Server, Bots, Spyware, Drive-by sources, DDoS Ziele und Quellen.

Signaturbasierte Erkennung erfolgt aufgrund von vorgegebenen Mustern. Angreifer nutzen aber vermehrt Wege in Ihr Netzwerk, die vorher noch nicht bekannt sind. Die verhaltensbasierte Erkennung ist genau auf diesen Bereich spezialisiert.

Wählen Sie aus den verschiedenen Paketgrößen, die jeweils eine maximal zu analysierende Datenmenge enthalten.

Externe und interne Schwachstellenanalyse

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

Externe und interne Schwachstellen-Scans (in der Fachsprache Vulnerability Management and Assessment genannt) bieten Ihnen den Überblick über aktuell bestehende Schwachstellen in Ihrem Netzwerk nach Risiko-Grad (hoch, mittel und gering) kategorisiert. Das Resultat sehen Sie in Ihrem Cyber SafeAlert Cockpit: Eine klare Prioritätenliste für die Abarbeitung und aufbereitete Informationen zur Erfüllung von Compliance Anforderungen. Aufwendige Spezial-Schulungen sind nicht notwendig.

Neben den schnellen und effizienten authentifizierten oder nicht-authentifizierten Schwachstellen-Scans werden durch Compliance- und Passwort-Checks Konfigurationsprobleme in Bezug auf Anwendungen und Passwörter- sowie User-Policies erkannt. Standard- oder fehlende Passwörter werden festgestellt, veraltete Versionen bei installierter Software und Services werden bei Windowssystemen mit Registry und dll-Checks aufgedeckt.

Die Anzahl der Geräte, die für die Scans entscheidend sind, variiert je nach dem von Ihnen gewählten Paket. Je nach Wahl führt das Paket entweder eine oder beide Arten der Scans durch.

Logdaten-Analyse

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

Logs aus verschiedenen Quellen in einem Netzwerk (Server, Clients, Netzwerkgeräte, Firewalls, Anwendungen, etc.) geben entscheidende Hinweise auf sicherheitsrelevante Ereignisse. Die Herausforderung besteht darin, sicherheitsrelevante Informationen aus Millionen von Ereignissen herauszufiltern. In der Fachsprache nennt man dieses IT-Risikoerkennungsmodul Security Information and Event Management (SIEM).

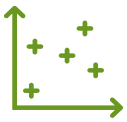
Zahlreiche gängige Log Formate werden unterstützt. Legen Sie aus einer Liste an standardisierten Log-Quellen fest, welche daraus für Ihr Unternehmen relevant sind. Die unterschiedlichen Paket-Varianten enthalten je eine maximale Anzahl an Log-Quellen.

Informationen und Ereignisse aus diesen Logdateien werden aggregiert. Durch eine moderne Correlation Engine mit kontinuierlich erweiterten und maßgeschneiderten Regeln und Policies werden potenzielle Risiken identifiziert.

Optional: Erweiterte Bedrohungserkennung (Email / Web)

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

Neuartige bzw. getarnte Malware, Advanced Persistent Threats (APTs) und Trojaner gelangen durch Web Downloads und/oder E-Mail-Anhänge in Unternehmen, da sie durch signatur-basierende Systeme allein nicht erkannt werden. Hinzu kommt das Risiko von Insider-Threats, wodurch gezielt wichtige Informationen unberechtigt erlangt werden. DEKRA Cyber SafeAlert setzt mehrere Systeme zur signatur- und verhaltensbasierten Analyse von Netzwerkverkehr und Sandbox-Technologien der neuesten Generation mit vollständiger Systememulation zur Analyse aller eingehenden E-Mail-Anhänge sowie Web-Downloads ein und wertet die Erkenntnisse zentral aus. Die Aktualität dieses Moduls wird durch kontinuierliche Updates sichergestellt.



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.

Eine einzelne Information innerhalb einer Datenmasse weist oftmals noch nicht auf ihre Sicherheitsrelevanz hin. Erst durch die Kombination von Informationen entstehen die wertvollen Puzzlestücke, die notwendig sind, um einem Angreifer auf die Spur zu kommen. Eine Korrelation von Logs mit Schwachstellen, IDS-Daten oder SIEM Erkenntnissen lässt einen Gesamtüberblick über sicherheitsrelevante Daten zu.

Korrelation und Cross-Korrelation basieren auf Regeln, Policies und selbstlernenden Algorithmen: Regeln werden vordefiniert und kontinuierlich erweitert, um Muster zu erkennen. Policies werden verwendet, um festzustellen, ob spezifische Aktionen zur richtigen Zeit und am richtigen Ort stattfinden. Selbstlernende Algorithmen umfassen die Lernfähigkeit der Correlation Engine, zwischen normalem und abnormalem Vorkommen zu unterscheiden und Verhaltensveränderungen bei Applikationen, Servern und in anderen Netzwerkbereichen erkennen zu können. Eine Verwendung außerhalb der Geschäftszeiten, eine übermäßige Verwendung von Anwendungen oder anderen IT-Services sowie Muster im Netzwerkverkehr über die Zeit und im Vergleich zu vergangenen Perioden (unter Berücksichtigung von täglichen, wöchentlichen, monatlichen und saisonalen Schwankungen) sind Beispiele für die Erkennung von Anomalien.

Threat Intelligence

Bringt die aktuellen sicherheitsrelevanten Informationen zusammen.

Threat Intelligence Informationen werden aus zahlreichen Quellen zusammengeführt. Mit ihnen wird schädliches Verhalten schneller erkannt – seien es zum Beispiel Verbindungen von oder zu verdächtigen IPs aus der internen IT-Infrastruktur.

Zu diesen Informationen gehören neben den IP Adressen mit schlechter Reputation auch ebensolche URLs, für Phishing verwendete E-Mail-Adressen und für Schadsoftware verwendete Dateinamen, Dateipfade oder User Agents.

Die von Cyber SafeAlert umfassend gesammelten und verarbeiteten sicherheitsrelevanten Daten, gepaart mit den umfangreichen Threat Intelligence Informationen aus verschiedenen Quellen, ermöglichen eine unvergleichliche Schnelligkeit bei Detection & Response.

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.

Das Cockpit zeigt Ihren individuellen Überblick über die sicherheitsrelevanten Informationen, welche die automatisierte Erkennung geliefert hat. Die Ergebnisse werden mit den festgestellten, klassifizierten und priorisierten Sicherheitsproblemen dargestellt.

Die Übersicht über die vorhandenen Geräte bietet die Möglichkeit auszuwählen, welche Geräte in die Überprüfung mit einbezogen werden sollen.

Sie wissen, was in welcher Reihenfolge erledigt werden sollte und halten bereits die Informationen in den Händen, die Sie für die nächsten Schritte der Behebung oder Risikominimierung benötigen. Ersparen Sie sich ein langes Suchen auf den Webseiten von einzelnen Herstellern. Cyber SafeAlert liefert die wichtigsten Informationen gleich mit.

Expertenunterstützung auf Wunsch –

Wie wir Sie als IT-Partner im weiteren Vorgehen unterschützen können.

Je nachdem, wieviel Kapazität Ihnen in Ihrem Unternehmen für die IT-Sicherheit zur Verfügung steht, kann es sinnvoll sein, einen IT-Partner in die Aufgaben rund um das kontinuierliche IT Security Monitoring mit einzubeziehen.

Wir können Sie zum Beispiel in den folgenden Bereichen unterstützen

> Tiefere Expertenanalyse der automatisiert erlangten Ergebnisse
> Unterstützung bei der Behebung von Risiken und / oder Schwachstellen
> Hilfe in dringenden Notfällen / akuten Angriffsfällen
> Ansprechpartner für weitergehende Fragen oder beim Handling der Risikoerkennungswerkzeuge
> Beratung bei Fragen rund um Ihre laufende IT-Sicherheit
> Durchführung von IT-Sicherheits- und Mitarbeiterschulungen
> Unterstützung beim Setup des Systems
> Erweiterter Remote-Support

Cyber SafeAlert – Leistungspakete im Überblick.

Ihre Unternehmensgröße*	1 - 49 Mitarbeiter	50 - 99 Mitarbeiter	100 - 249 Mitarbeiter	250 - 500 Mitarbeiter
Cyber SafeAlert Silber	NIDS (50 MBit) VAS Extern (2 IPs)	NIDS (100 MBit) VAS Extern (5 IPs)	NIDS (150 MBit) VAS Extern (10 IPs)	NIDS (200 MBit) VAS Extern (25 IPs)
Cyber SafeAlert Gold	NIDS (100 MBit) VAS Extern (2 IPs) VAS Intern (50 IPs) Risikofragebogen	NIDS (200 MBit) VAS Extern (5 IPs) VAS Intern (100 IPs) Risikofragebogen	NIDS (300 MBit) VAS Extern (10 IPs) VAS Intern (250 IPs) Risikofragebogen	NIDS (500 MBit) VAS Extern (25 IPs) VAS Intern (500 IPs) Risikofragebogen
Cyber SafeAlert Platin	NIDS (100 MBit) VAS Extern (2 IPs) VAS Intern (50 IPs) SIEM (5 Logquellen) Risikofragebogen	NIDS (200 MBit) VAS Extern (5 IPs) VAS Intern (100 IPs) SIEM (10 Logquellen) Risikofragebogen	NIDS (300 MBit) VAS Extern (10 IPs) VAS Intern (250 IPs) SIEM (25 Logquellen) Risikofragebogen	NIDS (500 MBit) VAS Extern (25 IPs) VAS Intern (500 IPs) SIEM (50 Logquellen) Risikofragebogen

Für das Modul „SIEM" gelten folgende Fair-Use Regeln:

- SIEM 1-49 (5 Log-Quellen):
  - Event pro Sekunde (EPS) Durchschnitt binnen 24 Stunden: 50
  - Events pro Sekunde (EPS-PEAK) binnen 24 Stunden: 200
- SIEM 50-99 (10 Log-Quellen):
  - Event pro Sekunde (EPS) Durchschnitt binnen 24 Stunden: 100
  - Events pro Sekunde (EPS-PEAK) binnen 24 Stunden: 400
- SIEM 100-249 (25 Log-Quellen):
  - Event pro Sekunde (EPS) Durchschnitt binnen 24 Stunden: 250
  - Events pro Sekunde (EPS-PEAK) binnen 24 Stunden: 1000
- SIEM 250-500 (50 Log-Quellen):
  - Event pro Sekunde (EPS) Durchschnitt binnen 24 Stunden: 500
  - Events pro Sekunde (EPS-PEAK) binnen 24 Stunden: 2000

Werden diese angeführten Fair-Use Werte (wobei die Überschreitung entweder von EPS oder EPS-PEAK ausreicht) bei einem Kunden in zwei aufeinander folgenden Monaten überschritten, so kann (1) der Endkunde dazu aufgefordert werden, entweder in das nächst größere Leistungspaket zu wechseln, oder (2) die DEKRA Cyber SafeAlert Gesamtlösung von DEKRA so konfiguriert werden, dass die über die Fair-Use Werte hinausgehenden Datenmengen vor Übertragung in das Cyber SafeAlert-Cockpit (und damit vor einer Risikoanalyse) gelöscht und damit nicht verarbeiten werden.

Wenn kein nächst größeres Leistungspaket verfügbar ist (bei „Paket für Unternehmen mit 250 bis 500 Mitarbeitern"), stehen optional Erweiterungspakete für SIEM zur Verfügung, die zusätzlich gebucht werden können.

* Je nach ausgewähltem Leistungspaket und Ihrer Unternehmensgröße gehört die Bereitstellung einer passenden SafeAlert-Hardware zum Lieferumfang (Alert-ONE / Alert-TWO). Optional ist als erweiterte Funktion die Advanced Threat Detection Mail only / Mail und Web verfügbar. Die Unternehmensgröße erlaubt einen ungefähren Schluss auf die Anzahl der IT-Geräte in Ihrem Unternehmen/die Anzahl der IT-Geräte, die von der Risikoerkennung erfasst werden sollen. Die Anzahl der IT-Geräte ist die Basis für die Preiskalkulation.

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

Änderungen vorbehalten. März 2019