stratego IT

Threat-Management und Anomaly Detection

oder einfach auf deutsch:

Risiko- und Bedrohungsmanagement und Erkennen von „Auffälligkeiten“ / Sicherheitsanomalien

Herausforderung / Risiko:

Die zunehmende Risiko- und Bedrohungslage für globale IT-Infrastrukturen zeigt deutlich, dass herkömmliche Methoden und Tools im Bereich der IT-Sicherheit (Firewalls, SPAM-, Content- und Virenfilter) nicht mehr ausreichen, um eine verlässliche Netzwerksicherheit zu gewährleisten.

Lösung:

Früherkennungs-System für IT-Sicherheitsanomalien - **„Anomaly-Detection-System“ und Threat-Management-Prozess**

Projektablauf:

1. **Einführungsworkshop**
   Überprüfung der unternehmensspezifischen Umgebung und der Voraussetzung

2. **Umsetzungsworkshops und Konzeption**
   Erstellung eines Konzept zur Einführung eines Threat-Managements und Anomaly-Detection-Systems in Ihrer Organisation.
   In kleineren Workshops werden weitere Verantwortliche in das Projekt integriert (z.B. Datenschutz und Mitbestimmung) und die notwendigen Grundlagen für eine Analyse gelegt.

3. **Technische Implementierung**
   Wir installieren in Ihrem Netzwerk die im Workshop festgelegten Werkzeuge zur Erkennung von Schwachstellen (Vulnerability-Scanner) oder zur aktiven Netzwerküberwachung (Anomaly-Detektoren, Logfile-Scanner, etc.). Die Systeme werden über einen längeren Zeitraum im Rahmen der Pilotphase betrieben und sammeln entsprechende Daten für eine spätere Auswertung.

4. **Auswertung und Diskussion der Ergebnisse**
   Die Daten aus der Pilotphase werden vorgestellt, aufbereitet und bewertet. In einem Workshop werden weitere Maßnahmen und Schritte für einen möglichen Rollout erörtert

Ihre Vorteile:

- Herstellerunabhängig
- Experten-Know-how
- Beratung und Ausführung auf Basis von anerkannten und empfohlenen Standards

Serviceportfolio:

- Informationssicherheits-Management System (ISMS)
- Externer Datenschutzbeauftragter
- Datenschutz Management System (DSMS)
- Konformitätsprüfungen
- Schulungen und Coachings
- Interne und externe Audits
- Penetrationstests
- Schwachstellenmanagement
- Netzwerk-Sicherheit (Anomaly Detection)
- Digitale Forensik
- Absicherung von HomeOffice Umgebung

Ihre Ansprechpartner:

Alexander Freitag
Fon: +49 (0)7046 38 79 88 - 5
alexander.freitag@stratego-it.com

Alexander Hedrich
Fon: +49 (0)7046 38 79 88 - 0
alexander.hedrich@stratego-it.com

stratego IT management GmbH
Hofäckerstraße 32
74374 Zaberfeld

stratego IT

5. **Auswertung und Diskussion der Ergebnisse**
   Die Daten aus der Pilotphase werden vorgestellt, aufbereitet und bewertet. In einem Workshop werden weitere Maßnahmen und Schritte für einen möglichen Rollout erörtert

6. **Rollout- und Integrationskonzept**
   Wir helfen Ihnen bei der Konzeption eines weiterführenden Threat-Management-Prozesses und definieren ein mögliches Setup. Dazu werden bestehende Schnittstellen zu existierenden Prozessen (Change- und Incident-Management) definiert und die Verantwortlichkeiten für das Auswerten, Erkennen und Behandeln von Sicherheitsvorfällen und Anomalien beschrieben.

7. **Integration in Ihre Betriebsumgebung**
   Im letzten Schritt werden die im Integrationskonzept definierten, weiteren Sensoren in das zentrale Anomaly-Detection-System integriert.

   Die Konzeption ist wesentlich für eine sinnvolle Früherkennung auf einer breiten Fläche. Dazu werden beispielsweise Logdaten aus kritischen Systemen (SAP, Exchange) und anderen Sicherheitstools (Firewall, Virenscanner) an das Repository angedockt, um eine sensiblere und genauere Auswertung im Verdachtsfalle zu ermöglichen. Die Auswerteroutinen werden in Ihre vorhandenen IT-Prozesse integriert, um verantwortliche Administratoren schnellstmöglich informieren zu können.

8. **Unterstützung beim Betrieb des Systems**
   Die nachhaltige Überwachung und Alarmierung durch dieses System ermöglicht Ihnen eine Früherkennung von Gefahren im Netzwerk und die Abwehr von Risiken. Ein wesentlicher Aspekt ist das frühzeitige Erkennen dieser Art von Ereignissen.

   Wir bieten Ihnen an, Sie bei der Überwachung und Auswertung des Anomaly-Detection-Systems zu unterstützen.
   Unsere IT-Forensiker werden nach Absprache oder bei Verdacht mit Ihnen gemeinsam nach möglichen Regelverstößen oder Angriffsmustern suchen und mögliche Maßnahmen zur Problemlösung vorschlagen. Damit haben Sie ein zusätzliches „menschliches“ Expertenwissen zur Verfügung und können Ihr eigenes IT-Personal entlasten.

Für weitere Details stehen wir Ihnen gerne zur Verfügung

Ihre Vorteile:

- Herstellerunabhängig
- Experten-Know-how
- Beratung und Ausführung auf Basis von anerkannten und empfohlenen Standards

Serviceportfolio:

- Informationssicherheits-Management System (ISMS)
- Externer Datenschutzbeauftragter
- Datenschutz Management System (DSMS)
- Konformitätsprüfungen
- Schulungen und Coachings
- Interne und externe Audits
- Penetrationstests
- Schwachstellenmanagement
- Netzwerk-Sicherheit (Anomaly Detection)
- Digitale Forensik
- Absicherung von HomeOffice Umgebung

Ihre Ansprechpartner:

Alexander Freitag
Fon: +49 (0)7046 38 79 88 - 5
alexander.freitag@stratego-it.com

Alexander Hedrich
Fon: +49 (0)7046 38 79 88 - 0
alexander.hedrich@stratego-it.com

stratego IT management GmbH
Hofäckerstraße 32
74374 Zaberfeld

stratego IT

Wir, die stratego IT Management GmbH, haben es uns zur Aufgabe gemacht, Sie dabei zu unterstützen, dass die IT zum echten Mehrwert für ihr Unternehmen wird.

Informations-Sicherheits-Management-System (ISMS):

Unsere Kernkompetenz liegt in der Schaffung und Überprüfung Ihrer **Informationssicherheit** mit Fokus auf die ISO 27001 sowie deren abgewandelte Formen. Wir helfen Ihnen, dass IT-Sicherheit in Ihrem Unternehmen gesetzeskonform und alltagstauglich ist. Von uns bekommen Sie praxisnahe Methoden von hochkompetenten Mitarbeitern für den Unternehmensalltag. Mit einer Konformitätsprüfung /Audit hinsichtlich z.B. der ISO 27001:2015, ISO 9001 etc. erfahren Sie genau auf Ihr Unternehmen ausgerichtet, ob und falls ja welche Maßnahmen in Ihrem Unternehmen implementiert und umgesetzt werden müssen. Nach dieser Analyse der gegebenen Bedingungen unterstützen wir Sie auch gerne bei der Implementierung eines effektiven ISMS, um die geforderte Zertifizierungsreife zu erhalten.

Datenschutzmanagementsystem (DSMS)

Unsere hochkompetenten Datenschützer sind im Bereich der EU-Datenschutzgrundverordnung „EU-DSGVO“ auf dem neuesten Stand. Auch hier ermöglich wie die Schaffung und Überprüfung der Datenschutzkonformität
Wir helfen Ihnen, dass der Datenschutz in Ihrem Unternehmen gesetzeskonform und alltagstauglich ist. Weiterhin erhalten Sie wie beim ISMS praxisnahe Methoden von zertifizierten und kompetenten Mitarbeitern für den Unternehmensalltag.
Mit einer Konformitätsprüfung /Audit hinsichtlich des Datenschutzes erfahren Sie genau auf Ihr Unternehmen ausgerichtet, ob und falls ja welche Maßnahmen in Ihrem Unternehmen implementiert und umgesetzt werden müssen. Nach dieser Analyse der gegebenen Bedingungen unterstützen wir Sie auch gerne als externer Datenschützer bei der Implementierung eines effektiven DSMS. Dadurch erhalten die Sicherheit, das ihr Unternehmen gesetzeskonform arbeiten kann und somit verringert sich das Risiko sowie den erhalt eines Bußgeldes.

stratego IT management GmbH
Hofäckerstraße 32
74374 Zaberfeld

Tel.	07046 – 38 79 88 - 0
Fax	07046 – 38 79 88 - 9
E-Mail	info@stratego-it.com
Internet	www.stratego-it.com