APT Defense Service – Schutz vor gezielten Angriffen.

Managed Security Service zur Abwehr von Hacker-Angriffen

Mit über 60 Prozent waren mittelständische Unternehmen am stärksten von IT-Spionage- oder Sabotageakten betroffen. Die meisten Organisationen sind bereits kompromittiert, ohne dies auch nur zu ahnen. Im Erkennen und der zielgerichteten Behandlung von Sicherheitsvorfällen sind Unternehmen oft überfordert, sowohl technologisch als auch in Bezug auf das erforderliche spezielle Know-how.

Unsere Lösung – der APT Defense Service:
Das Prinzip ist so praxisorientiert wie wirkungsvoll: umfassendes Know-how kombiniert mit Top-Technologie. Budgetschonend als Security as a Service.

Maßgeschneiderter Schutz gegen Cyber-Attacken

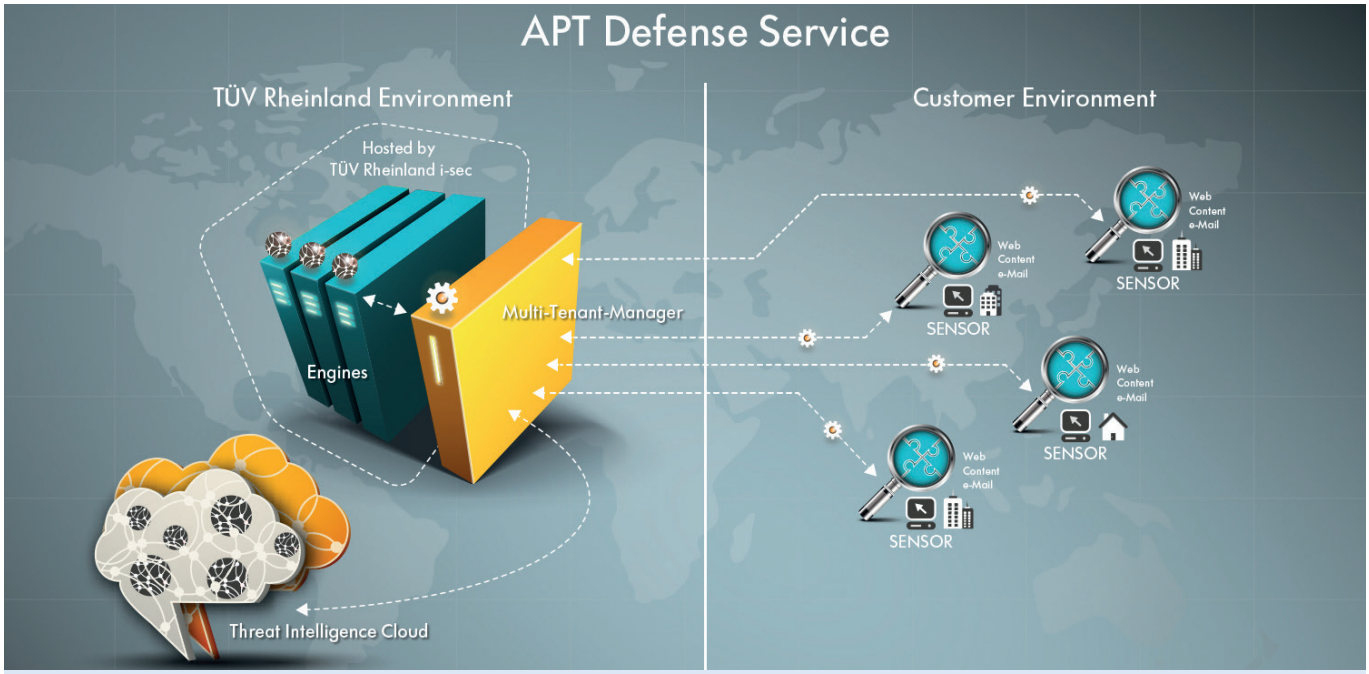
Für herkömmliche Sicherheitssysteme sind sie oft nicht mehr erkennbar: gezielte Attacken, mit denen Cyberkriminelle versuchen, Zugriff auf Unternehmensdaten zu erlangen. Um gezielte komplexe Angriffe, kurz APT (Advanced Persistent Threats) zu erkennen und erfolgreich abzuwehren, bedarf es innovativer Sicherheitstechnologie und Experten, die diese Technologien beherrschen.

Beides ist jetzt nicht mehr nur Großunternehmen vorbehalten: Der neue APT Defense Service bietet nun auch dem Mittelstand gezielten Schutz vor Cyber-Attacken.

Bewahren Sie Ihr geistiges Eigentum nachhaltig vor Datendiebstahl, Spionage und Sabotage – mit dem APT Defense Service von TÜV Rheinland.

Ihre Vorteile

- **Best practice – zu einem attraktiven Preis:** Ihr Unternehmen nutzt hochinnovative verhaltensbasierte Sensor-Technologie, die derzeit am Markt zum Schutz gegen Cyber-Angriffe verfügbar ist.
- **Permanentes Sicherheitsmonitoring:** Die Erkennung von Sicherheitsvorfällen erfolgt komplett automatisch. Die Informationen werden in Echtzeit dem TÜV Rheinland CSIRT zur Analyse, Bewertung sowie Ableitung von Behebungsmaßnahmen zur Verfügung gestellt.
- **Entlastung und Qualifizierung Ihrer Mitarbeiter in der IT:** Durch die Zusammenarbeit mit den Experten von TÜV Rheinland entlasten – und gleichzeitig schulen – Sie Ihre IT-Mitarbeiter.
- **Maßgeschneiderte Lösungen:** Das Service Level bestimmen Sie selbst. Der APT Defense Service ist mit modularen Service Level Agreements buchbar: vom Betrieb bis zur Forensik.
- **Planungssicherheit durch Security as a Service:** Sind die Sensoren einmal installiert, fallen für das Unternehmen bis zum Zeitpunkt der Identifikation eines Sicherheitsvorfalls keine operativen Aufgaben an.



1. **Technische Voraussetzungen:**
   Die Anschaffung umfangreicher Hardware ist nicht erforderlich. In der Kunden-Netzwerkinfrastruktur platziert TÜV Rheinland lediglich kleine, kostengünstige Sensoren im Monitoring Mode (TAP). Diese Sensoren unterziehen den im Unternehmen generierten Netzwerkverkehr (Web, Mail, etc.) einer Vor-Analyse.
2. **Detektion von Anomalien:**
   Stellen die Sensoren Indikatoren fest, die auf einen Angriff oder eine Infektion hindeuten, wird der verdächtige Netzwerkverkehr komplett verschlüsselt in ein TÜV Rheinland-Datacenter ausgeleitet.
3. **Qualifizierung des Sicherheitsvorfalls:**
   In den Analyseumgebungen von TÜV Rheinland wird das mögliche Schadpotenzial des Traffics geprüft, d.h. es wird getestet, wie sich diese Daten beim Betrachten oder Ausführen verhalten.
4. **Begrenzung des Angriffs:**
   In Form eines Managed Security Service prüfen und qualifizieren die Experten von TÜV Rheinland die Ergebnisse. Im Falle einer Infektion oder eines Angriffs definieren sie gezielte Abwehrmaßnahmen und unterstützen die interne IT des Kunden bei konkreten Abwehrmaßnahmen.

Gut die Hälfte aller Unternehmen in Deutschland war in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl*.

*Umfrage Digitalverband Bitkom 2015, www.bitkom.org, für die Studie wurden Geschäftsführer und Sicherheitsverantwortliche von 1.074 Unternehmen repräsentativ befragt.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
Fax +49 221 806-2295
service@i-sec.tuv.com

TÜVRheinland®
Genau. Richtig.