CYBERKRIMINALITÄT UND ADVANCED PERSISTENT THREATS. FRAGEN UND ANTWORTEN.

Sie möchten mehr zum Thema Advanced Persistent Threats erfahren? Wir haben für Sie im Folgenden häufig gestellte Fragen beantwortet.

1. Was versteht man unter Cyberkriminalität?

Grundsätzlich unterscheidet man zwischen **„opportunistischer" Cyberkriminalität**, das heißt, nicht auf ein bestimmtes Unternehmen ausgerichtete Angriffe mit dem Ziel, möglichst viele Opfer zu infizieren (z.B. mittels Ransomware, Phishing-Mails etc.), und **organisierter Cyberkriminalität**. Hier handelt es sich um gut organisierte Gruppen mit hoher Spezialisierung und enormen finanziellen Ressourcen mit dem Ziel, Unternehmen oder kritische Infrastrukturen gezielt anzugreifen (in Form von komplexen, gezielten Angriffen – APTs).

2. Was ist Ransomware?

Ransomware sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Meist dient dies dazu, Lösegeld („ransom") zu erpressen.

3. Was bedeutet Advanced Persistent Threat? (gezielter Angriff)

Advanced (fortgeschritten)
Ein APT ist eine Cyberattacke, die auf bestimmte, ausgewählte Unternehmen, Personen oder Institutionen ausgerichtet ist. Sie wird von gut ausgebildeten Angreifern mit erweiterter Technologie, strategischer Taktik und entsprechenden (finanziellen) Ressourcen durchgeführt. Herkömmliche Cyberkriminalität zielt auf unspezifische, möglichst hohe Opferanzahlen ab, während APT strukturiert und komplex verläuft.

Persistent (andauernd)
Nach erfolgreicher Infektion ist es das Ziel des Angreifers, möglichst lange unerkannt zu bleiben, um sich weiter im System und Netzwerk auszubreiten. Es werden in der Regel Hintertüren zur Fernsteuerung implementiert, Informationen gesammelt, manipuliert oder ausgeleitet.

Threat (Bedrohung)
APT stellt eine Cyber Bedrohung mit maximaler Komplexität und Schaden für ein Unternehmen dar.

4. Wer ist von APTs betroffen?

Mit über 60 Prozent sind, laut Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.), 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.

5. Wie erkennt man aktuelle Cyberattacken?

Um Cyberattacken - sowohl opportunistische als auch gezielte Angriffe - zu erkennen und erfolgreich abzuwehren, bedarf es innovativer **Sicherheitstechnologie** und Experten, die diese Technologien beherrschen.

Für herkömmliche Sicherheitssysteme wie Virenscanner und IDS-Systeme sind raffinierte Attacken, mit denen Cyberkriminelle versuchen, Zugriff auf Ihre Unternehmensdaten zu erlangen, meist nicht mehr erkennbar.

6. Was ist ein Threat Management?

Unter Threat Management versteht man die Gesamtheit der Maßnahmen und Lösungen, mit denen Unternehmen und Organisationen ihre Cyber Security managen.

- Mit unserem APT Defense Service bieten wir einen **Managed Security Service** aus einer Hand, der eine führende Breach Detection Lösung mit Incident Response as a Service vereint.
- Über unser Security Operation Center (SOC) lässt sich der Umfang an Managed Services auch auf weitere Security Lösungen von Ihnen ausweiten.
- Zusätzlich stellen wir mit unseren Professional Services eine breite Auswahl an Möglichkeiten zur Verfügung (Lösungsbausteine verschiedener Hersteller sowie Consulting Dienstleistungen) – für ein effektives Threat Management zur nachhaltigen Verbesserung Ihrer Cyber Security.

7. Wie erhalte ich einen Überblick über meine aktuelle Sicherheitslage?

- Zu Beginn beobachtet unsere Compromise Assessment Appliance Ihr Netzwerk über einen Zeitraum von vier Wochen, um den aktuellen Status zu bestimmen.
- Nach 14 Tagen erhalten Sie einen Zwischenbericht und nach Ablauf der Analysephase einen Abschlussbericht, der Ihnen einen detaillierten Überblick über die aktuelle Sicherheitslage gibt. Basierend auf diesen Erkenntnissen leiten wir ab, welche technische Lösung für Sie geeignet ist, und wo sie integriert wird.
- Nach der Implementierung weisen unsere Experten Ihre **Mitarbeiter** ein und setzen mit ihnen gemeinsam die nötigen Prozesse auf, um bei Vorfällen richtig auf einen Angriff zu reagieren.

8. Wie funktioniert der APT Defense Service?

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.

Detektion von Anomalien: Stellen die Sensoren Indikatoren fest, die auf einen Angriff oder eine Infektion hindeuten, wird der verdächtige Netzwerk-Verkehr komplett verschlüsselt in ein TÜV Rheinland-Datacenter ausgeleitet.

Qualifizierung des Sicherheitsvorfalls: In der virtuellen Umgebung von TÜV Rheinland wird das mögliche Schadpotenzial des Traffics geprüft, d.h. es wird getestet, wie sich diese Daten beim Betrachten oder Ausführen verhalten.

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.

9. Für welche Unternehmen ist der APT Defense Service geeignet?

Um Cyberangriffe zu erkennen und erfolgreich abzuwehren, bedarf es innovativer Sicherheitstechnologien und Experten, die diese Technologien beherrschen. Meist ist dies nur in Großunternehmen mit eigenem Cyber Defense Center (CDC) der Fall.

Mit dem APT Defense Service – als budgetschonenendem Managed Security Service – kann sich nun auch der Mittelstand vor Cyber-Attacken schützen.

10. Wann greift der APT Defense Service ein?

Dank des permanenten Sicherheitsmonitorings erfolgt die Erkennung von Sicherheitsvorfällen sofort und komplett automatisch. Die Informationen werden dann in Echtzeit dem **TÜV Rheinland CSIRT** zur Analyse, Bewertung sowie Ableitung von Behebungsmaßnahmen zur Verfügung gestellt. Mit dem APT Defense Service nutzt Ihr Unternehmen hochinnovative verhaltensbasierte Sensor-Technologie, die derzeit am Markt zum Schutz gegen Cyber-Angriffe verfügbar ist.

11. Welche Vorteile hat der APT Defense Service für mich als Informationssicherheitsverantwortlicher?

Planungssicherheit durch Security as a Service: Sind die Sensoren einmal installiert, fallen für Sie bis zum Zeitpunkt der Identifikation eines Sicherheitsvorfalls keine operativen Aufgaben an.

12. Welche Vorteile hat der APT Defense Service für mich als Geschäftsführer?

Schützen Sie sich und Ihre Unternehmenswerte vor Angriffen und Attacken und minimieren Sie mögliche Schäden und Kosten für eine notwendige Wiederherstellung einer guten Reputation. Durch die Zusammenarbeit mit den Experten von TÜV Rheinland entlasten und schulen Sie gleichzeitig Ihre IT-Mitarbeiter.

Ihre Frage ist nicht dabei? Kontaktieren Sie uns jetzt! Unsere Experten helfen Ihnen gerne weiter.

Kontaktieren Sie uns!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806 – 0
service@i-sec.tuv.com
www.tuv.com/apt

TÜVRheinland®
Genau. Richtig.