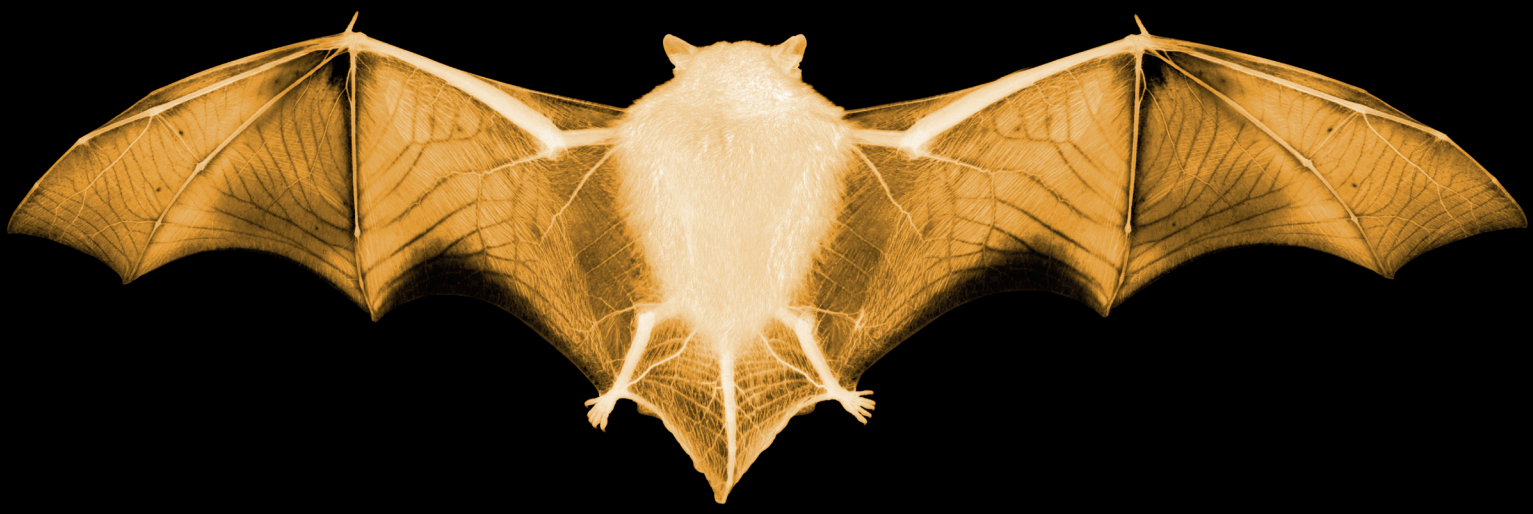
iT-CUBE SYSTEMS

Security Health Check

Palo Alto Networks



„Dem trüben Blick hilft keine Brille“

Der Spruch **„man kann nicht sichern, was man nicht sieht“** ist in den gewachsenen IT-Umgebungen von heute relevanter denn je. Wenn Sie folgende Fragen ohne zu zögern beantworten können, brauchen Sie nicht weiterzulesen:

Wie viele Applikationen sind in Ihrem Netz aktiv und wer nutzt diese in seiner Kommunikation?

Warum sollte die Antwort auf diese Frage für Ihre Organisation so wichtig sein? Moderne Angriffe zielen primär auf Applikationen. Wer keine Kontrolle über den Umgang mit Applikationen hat, kann dem Datenklau nichts entgegensetzen. Das bedeutet aber auch, dass Sie ein genaues Bild benötigen, welche Arten der Kommunikation für Ihre IT-Landschaft relevant sind.

Check und Vorsorge statt Notoperation

Der Arzt Ihres Vertrauens rät grundsätzlich zur Vorsorge und schlägt einen Gesundheitstest vor. Obgleich es in der IT-Sicherheit angesagter Trend ist, auf kontinuierliches Monitoring und „Incident Response“ zu setzen, bleiben Präventivmaßnahmen ein wichtiges Element in jeder Sicherheitsarchitektur. Wenn es um die Erkennung von Anwendungen, Angriffen, Malware und Bots geht, liefert Palo Alto Networks mit der Next Generation Firewall Technologie die passenden Werkzeuge sowohl für einen Security Health Check als auch eine Plattformlösung für Perimeterschutz und Endpoint Security.

Die drei wichtigsten Elemente unseres Security Health Checks konzentrieren sich auf die Transparenz von Anwendungen, Benutzern und Inhalten (App-ID, User-ID und Content-ID). Mithilfe ausgereifter Identifikationstechnologien können wir exakt bestimmen, was in ihrem Netzwerk geschieht. So können sie fundierte Richtlinienentscheidungen treffen und den Gesundheitszustand Ihrer IT nachhaltig optimieren.

paloalto NETWORKS®

Wenn's tatsächlich brennt: WildFire™

Ergänzt wird der Health Check um Palo Alto WildFire™, dem Modul zur Erkennung von **Advanced Persistent Threats (APT)**. Hochentwickelte Cyberangriffe nutzen getarnte und hochprofessionelle Methoden, um traditionelle Sicherheitsmaßnahmen zu umgehen. WildFire identifiziert unbekannte Malware, Zero-Day-Attacken und APTs, indem verdächtige Dateien und E-Mail-Anhänge direkt in einer skalierbaren, cloud-basierten, virtuellen Sandbox-Umgebung ausgeführt werden. Signaturen und IoCs werden automatisiert erstellt und innerhalb von 5 Minuten in die Security Plattform von Palo Alto Networks geladen. WildFire™ kann während des Health Checks auch feststellen, ob Ihre Systemlandschaft durch APT-Angriffe bereits kompromittiert wurde.

Unsere Vorsorge-Leistungen

- **Planung & Durchführung:**
  Bevor wir starten, stimmen wir gemeinsam mit Ihnen alle erforderlichen Schritte im Detail ab. Danach installieren und konfigurieren wir die passenden Appliances in Ihrer Umgebung und überwachen die Durchführung des Checks. Nach zwei bis drei Wochen starten wir gemeinsam mit Ihnen die Analyse und bauen anschließend die installierten Komponenten wieder ab.

- **Analyse & Auswertung:**
  Die Informationen zu Anwendungen, Verkehrswerten, Bedrohungen und Angriffen werden hinsichtlich ihrer Kritikalität bewertet und übersichtlich aufbereitet. In einem Abschlussworkshop diskutieren unsere Experten mit Ihnen die Ergebnisse und übergeben einen aufschlussreichen Report mit allen Analysen samt Bewertung.

- **Beratung & Unterstützung:**
  Der Health-Check ist oft nur der erste Schritt. Wenn Sie möchten, unterstützen wir Sie gerne bei der Entwicklung eines Sicherheitskonzepts und der praktischen Umsetzung in Planung und Implementierung.

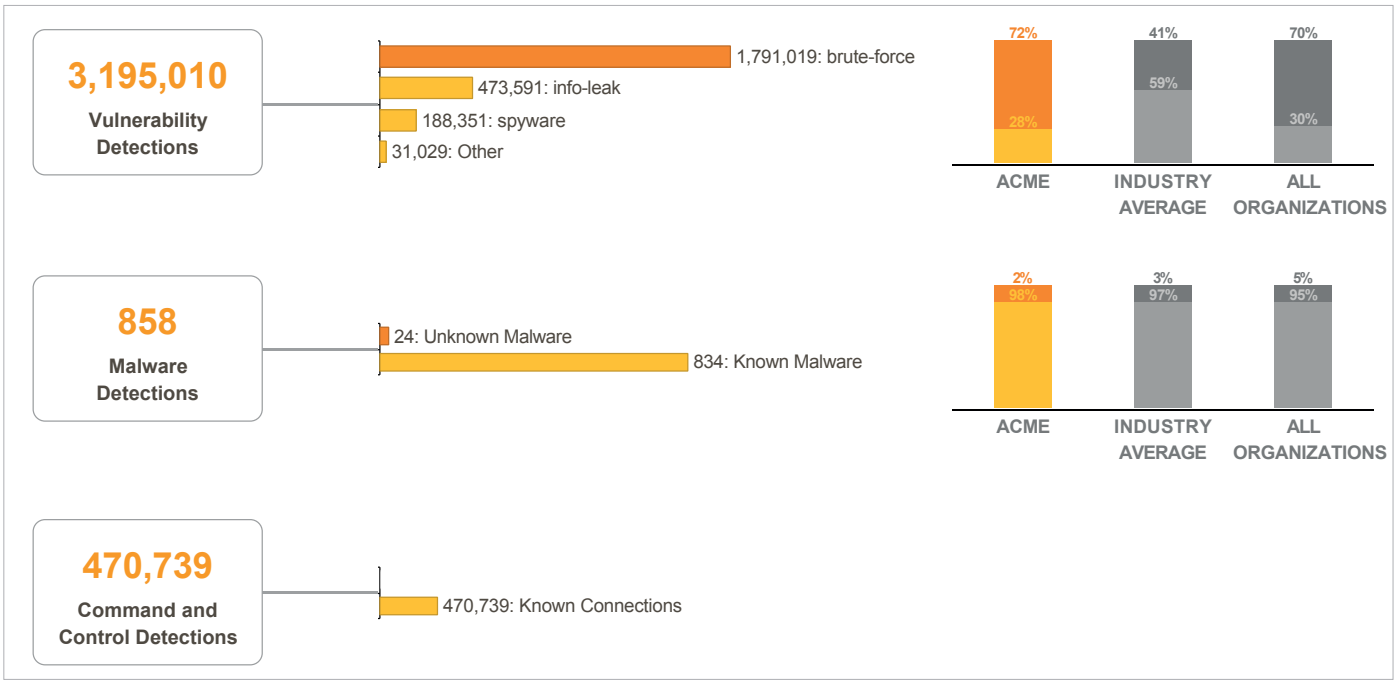


Abbildung 1: Auszug aus dem SLR Example-Report

Unsere Services und Experten stehen zu Ihrer Verfügung!

iT-CUBE SYSTEMS AG
Paul-Gerhardt-Allee 24
81245 München, Germany
T: +49 89 2000 148 00
F: +49 89 2000 148 29
info@it-cube.de
www.it-cube.de