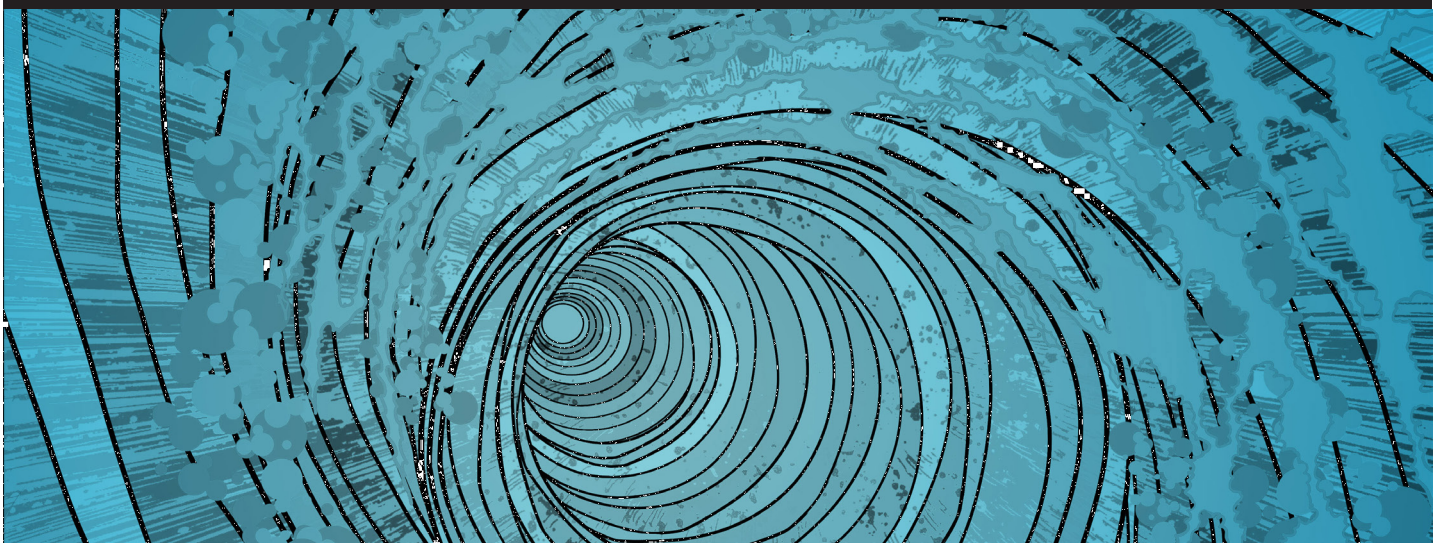
# 10 FUNKTIONEN, DIE IHRE LÖSUNG FÜR CYBERSICHERHEIT ERFÜLLEN MUSS



Cybersicherheit erfordert verschiedene Erkennungs- und Präventionsfähigkeiten, um Risiken zu steuern und Angriffe abzuwehren. Mit der Zunahme der Cyberkriminalität sind auch immer ausgeklügeltere Tools und Techniken zum Schutz Ihrer Organisation erforderlich. Es reicht jedoch nicht, mit individuellen Produkten einzelne Probleme lösen zu wollen. Eine ganzheitliche Cybersicherheitslösung, die sich dynamisch an die sich ändernde Bedrohungslandschaft anpassen kann, ist extrem wichtig.

**Erzwingen Sie die zulässigen Interaktionen zwischen Ihren Daten und den Benutzern.**

Ihr Netzwerk ähnelt einer virtuellen Autobahn, die Ihre Benutzer mit wichtigen Daten verbindet. Da mit der zunehmenden Vernetzung von Organisationen auch die Anzahl der Zugangswege zu diesen Datenspeichern steigt, erhöht sich das Angriffsrisiko ebenfalls rasant. Um die enorme Anzahl von Angriffen auf Ihr Netzwerk zu reduzieren, müssen Sie die Angriffsoberfläche durch granulares Identifizieren genehmigter Interaktionen zwischen Benutzern und Daten effektiv verkleinern. Legen Sie fest, welche Daten genau geschützt werden sollen – was sie enthalten, wo sie gespeichert sind und wie bzw. von wem sie verwendet werden dürfen.

**Stellen Sie die kontinuierliche Identifizierung von Bedrohungen bei allen Apps, Ports, Benutzern und Geräten sicher.**

Eine vollständige Bedrohungsidentifizierung für alle Anwendungen, Benutzer und Geräte innerhalb und außerhalb des Unternehmensnetzwerks sowie an sämtlichen Netzwerkspeicherorten ist für eine effektive Cybersicherheitsstrategie ausschlaggebend. Wichtig ist, dass Sie Ihr Unternehmen, Ihr Netzwerk und Ihre Benutzer kennen – Ihr Team und Ihre Tools können Ihre Organisation nur vor dem schützen, was sie sehen. Wählen Sie daher eine Cybersicherheitslösung, die Ihnen durchgängige Transparenz bietet.

**Schützen Sie Daten in mehreren Phasen des Angriffslebenszyklus.**

3

Bedrohungen bestehen jeweils aus mehreren Phasen, die zusammen den Angriffsverlauf bilden. Damit ein Angreifer sein Ziel erreicht, müssen alle Phasen erfolgreich abgeschlossen werden. Lösungen, die nur auf eine Phase fokussiert sind, können insbesondere bei neuen oder unbekannten Angriffstechniken scheitern. Eine effektive Präventionsstrategie beinhaltet Technologien, die Angriffe in den unterschiedlichen Phasen erkennen und abwehren. Diese müssen bekannte Bedrohungskomponenten einfach blockieren und bei evasivem Verhalten eingreifen können, um zu verhindern, dass Angreifer ihr Ziel erreichen.

**Überlisten Sie APTs, die speziell zur Umgehung von Sicherheitstools entwickelt wurden.**

4

Advanced Persistent Threats (fortgeschrittene, andauernde Bedrohungen, APTs) werden so entwickelt, dass sie die sicherheitsrelevanten Verteidigungsmaßnahmen umgehen können. Es ist äußerst einfach, eine Nutzlast in mehrere Segmente zu fragmentieren, einen Datei-Hash auf schadhafte Weise zu ändern oder einen E-Mail-Header zu fälschen. Ihre nächste Cybersicherheitslösung muss intelligente Signaturen verwenden, die tief in jedem Paket versteckte Bedrohungen, Dateien und Weblinks durchgängig in unterschiedlichsten Protokollen und Dateitypen erkennen, egal, um welchen Exploit oder Hash es sich handelt. Nur so lässt sich der Schutz erhöhen.

**Erleichtern Sie die Übersetzung neuer Informationen in Schutzmechanismen.**

5

Bei 60 Prozent aller Angriffe dauert es nur wenige Minuten, bis sie Schaden anrichten. Daher ist eine schnelle Übersetzung der Daten in umsetzbare Informationen und erzwingbare Schutzmechanismen unabdinglich. Erwägen Sie den Einsatz einer eigenständig lernenden Lösung, um diesen Prozess zu automatisieren und innerhalb weniger Minuten auszuführen. Je relevanter die nutzbaren Daten sind, desto aktueller sind Ihre Sicherheitsmaßnahmen und desto eher können Sie Ihre Daten schützen und die Prävention in Ihre Cybersicherheitsstrategie einbinden.

**Bleiben Sie bei den Schutzmechanismen gegenüber neuen Angriffsformen auf dem aktuellen Stand.**

6

Bedrohungen ändern sich ständig, da Angreifer ihre Methoden weiterentwickeln, um immer unbemerkter vorgehen zu können. Schutzmechanismen für Ihr Netzwerk, die morgens noch effektiv sind, können am Nachmittag bereits veraltet sein. Während ein engagiertes Team zur Erforschung von Bedrohungen wichtig ist, benötigen Sie dennoch auch automatisierte Schutzmechanismen, um mit der Einführung neuer Bedrohungen durch die Angreifer Schritt halten zu können. Daten neuer Angriffe auf Ihre Organisation und auf der ganzen Welt müssen schnell in umsetzbare Informationen und entsprechende Schutzmaßnahmen kompiliert werden, sobald Angreifer diese Bedrohungen einsetzen.

**Ermöglichen Sie eine schnelle und präzise Schadensbegrenzung.**

7

Obgleich eine Prävention vorzuziehen ist, spielen die Schadensbegrenzung und -behebung weiterhin eine wichtige Rolle in der Cybersicherheitsstrategie jeder Organisation. Zudem zählt bei einer Infektion jede Minute. Ihre nächste Cybersicherheitslösung muss Bedrohungsprotokolle aller erkannten Angriffsphasen korrelieren und hoch empfindliche Schadensindikatoren aktiv suchen und melden können. Hierzu zählt auch die Identifizierung infizierter Geräte über eine einfache IP-Adresse hinaus.

**Koordinieren Sie Aktionen für die einzelnen Sicherheitstechnologien.**

8

Sicherheitstechnologien und Sensoren im gesamten Netzwerk enthalten Funktionen zur Datenerfassung und Durchsetzung, durch deren Kombination Ihr Team die Organisation erheblich einfacher schützen kann. Ihre nächste Cybersicherheitslösung muss umsetzbare Informationen in umfassendem Maße für individuelle Technologien und Funktionen bereitstellen, Richtlinien innerhalb des gesamten Netzwerks aktualisieren und Sie bei Infektionen ungeachtet des Netzwerkspeicherorts unverzüglich benachrichtigen.

**Sorgen Sie für ein unterbrechungsfreies Unternehmen.**

9

Wenn es darum geht, die Organisation zu schützen und gleichzeitig die unzähligen Anwendungen zuzulassen, die für effiziente und rentable Unternehmensabläufe erforderlich sind, wird in der Regel zulasten der Sicherheit entschieden. Dies muss jedoch nicht sein. Die Angriffsoberfläche zu reduzieren, ist wichtig, um die Benutzerfreundlichkeit aufrechtzuerhalten. Da rechenintensive Aufgaben erforderlich sind, benötigen Sie für diese Aufgabe geeignete Hardware und Software. Diese muss beispielsweise auf Volumes mit hohem Datenverkehr und geringer Latenztoleranz, wie sie in kritischen Infrastrukturen gängig sind, Anwendungen identifizieren und Bedrohungen abwehren können.

**Benutzerfreundlichkeit.**

10

Selbst bei Verwendung eines zentralen Managementsystems stellt das Durchsuchen und Korrelieren der Daten aus einzelnen Protokollen einen enormen Aufwand dar. Durch nativ integrierte Sicherheitstechnologie, die auf einem einzelnen Gerät ausgeführt wird, können Sie sich jeden einzelnen Datenfluss ansehen. Kritische Sicherheitswarnungen lassen sich auf einfache Weise suchen, korrelieren und priorisieren. Außerdem können Sie Richtlinien basierend auf gegenwärtigen Ereignissen detailliert anpassen. Dies Art des Einblicks ermöglicht es Ihnen zudem, infizierte Geräte schnell und exakt zu lokalisieren, Angriffe abzuwehren und die Cybersicherheit Ihrer Organisation zu gewährleisten.

Laden Sie den vollständigen **Leitfaden für Käufer von Cybersicherheits-Lösungen** hier herunter.
Weitere Informationen erhalten Sie unter
**paloaltonetworks.com/cybersecurity**

**Palo Alto Networks**
4401, Great America Parkway
Santa Clara, California 95054, USA

+1-408-753-4000 Zentrale
+1-866-320-4788 Vertrieb
+1-866-898-9087 Support
www.paloaltonetworks.com