Trustwave®

DATENBLATT

Trustwave Proactive Threat Hunting

ERKENNEN SIE AKTIVE BEDROHUNGEN UND OFFENE ANGRIFFSVEKTOREN IN IHRER UMGEBUNG.

Vorteile

- **Reduziert** die Verweildauer von Angreifern
- Erkennung und **Bekämpfung** von Bedrohungen in Ihrer Umgebung
- **Maximiert die Sichtbarkeit** offener Angriffsvektoren in Ihrer Umgebung
- **Gewinnen** Sie Sicherheit und einen Partner
- **Reduzieren** Sie das Risiko für Ihr Unternehmen und Ihre Kunden

Einen Angreifer am Perimeter zu blocken, ist nicht immer erfolgreich. Bedrohungen werden weiterhin an vorbeugenden Sicherheitskontrollen vorbeigelangen. Trustwave Proactive Threat Hunting hilft Ihnen, Ihre Sicherheitsmaßnahmen zu stärken. Dazu werden versteckte Angreifer innerhalb Ihrer Umgebung identifiziert und offene Angriffsvektoren, die zu einem Sicherheitsvorfall führen können, erkannt.

Wir arbeiten anders

Beim Threat Hunting steht der Mensch im Mittelpunkt. Automatisiertes Threat Hunting hat seinen Mehrwert, erfordert jedoch ein Indicator of Compromise (IOC) sowie und Taktiken, Techniken und Prozeduren (TTPs) in ein Sicherheitstool integriert werden müssen, um nach Anhaltspunkten für Cyberangriffe zu suchen.

Im Gegensatz zu anderen Threat Hunting Services, die ausschließlich automatisierte, indikatorbasierte Erkennungsmethoden verwenden, wird Trustwave Proactive Threat Hunting von Menschen durchgeführt mit einem kreativen Fokus auf Hinweise und Hypothesen. Unsere Herangehensweise an das Threat Hunting kombiniert von Menschen durchgeführte und automatisierte Prozesse mit Ihren bestehenden Sicherheitstools sowie unseren speziell entwickelten Threat Hunting-Maß-nahmen, damit Sie Cyberkriminellen immer einen Schritt voraus sind.

Wie wir vorgehen

„By definition, hunting cannot be fully automated and while many tools may make skilled threat hunters more effective, they will not wholly replace them or turn security operations center (SOC) analysts into hunters in their own right"[1]
– Gartner

Threat Hunting beginnt an einem von zwei Punkten: einer Tatsache bzw. einem Befund oder einer Hypothese. Tatsache bzw. Befund kann die Ausgabe eines automatisierten Tools oder Systems sein, das versucht, einen Befund zu erstellen. Viele in der Branche setzen die Ausgabe eines solchen Systems mit „automatisiertem Threat Hunting" gleich. Trustwave beginnt ab diesem Punkt mit seinem Threat Hunting.

Trustwave Proactive Threat Hunting setzt auf ein Team aus erfahrenen Trustwave SpiderLabs Threat Huntern, eine unternehmenseigene Threat Hunting Plattform sowie Best Practices-Empfehlungen, um Sie bei der Bekämpfung von Bedrohungen in Ihrer Umgebung zu unterstützen. Unser Ziel ist die Identifizierung von Cyberkriminellen mit Insiderwissen, nicht gepatchten Schwachstellen, Netzwerk- oder Software-Fehlkonfigurationen sowie fortschrittlichen andauernden Bedrohungen in Ihrer Sicherheitsumgebung.

Eine Elitetruppe von Threat Huntern – Trustwave SpiderLabs®

Künstliche Intelligenz allein kann menschliche Expertise und Erfahrung nicht ersetzen. Das Trustwave SpiderLabs Threat Hunter-Team besteht aus Experten mit Fachkenntnis in verschiedenen Branchen und defensiven Mindsets, die aus verschiedenen beruflichen Erfahrungen im Security-Bereich stammen.

- Die verschiedenen Berufserfahrungen reichen von Informationssicherheit in Unternehmen über Sicherheitsforschung bis zu staatlicher und lokaler Strafverfolgung.
- Jahrzehntelange Erfahrung in den Bereichen Incident Response, Digitale Forensik, Cyber Threat Intelligence und Malware-Analyse.
- Praktische Erfahrung durch hunderte Threat Hunts sowie Untersuchungen, bei denen die Experten auf Cyberkriminelle gestoßen sind und ihre kreativen Denkfähigkeiten geschult haben.

Speziell entwickelte Threat Hunting-Maßnahmen

Wenn Sie mit Trustwave SpiderLabs ein Proactive Threat Hunting durchführen, nutzen unsere Hunting-Experten unsere unternehmenseigene Threat Hunting-Plattform und kombinieren sie mit Ihrer bestehenden Sicherheitstechnologie sowie der Trustwave SpiderLabs Cyber Threat Intelligence, um Bedrohungen und Schwachstellen in Ihrer Netzwerkinfrastruktur aufzudecken.

- Die Trustwave Threat Hunting-Plattform umfasst fünf Elemente: Agent Hunter, Intel Hunter, Scribe, Dweller und Artifact Collector
- Durch den Einsatz branchenführender Sicherheitstools extrahieren wir die besten Maßnahmen für das Threat Hunting, um die Time-to-Value zu beschleunigen.
- Die Verknüpfung mit diversen Threat Hunting-Sicherheitstools bietet zusätzliche Einblicke, die den Kontext des Threat Hunting verbessern sowie die durchschnittliche Zeit bis zur Erkennung und bis zur Reaktion verkürzen.
- Kombinieren Sie Ihre Daten mit einer umfassenden Threat Intelligence-Sammlung aus der Trustwave SpiderLabs-Forschung, einem großen Datenbestand aus anonymisierten Kundendaten sowie Partner und Open Source Intelligence.

Handlungsempfehlungen und Best-Practice-Ratschläge zur Wiederherstellung

Trustwave ist überzeugt, dass zu einem guten Threat Hunting mehr gehört als nur aktive Angreifer zu identifizieren. Trustwave Proactive Threat Hunting-Ergebnisse reichen über Endpoints bis zu Netzwerk-Traffic und Sicherheitsgeräten. Unsere Ergebnisse informieren über Mängel in der Umgebung, veraltete Software und Netzwerk-Fehlkonfigurationen. Finden wir eine Bedrohung, unterstützen wir Sie bei den entsprechenden Gegenmaßnahmen. Wir liefern klare, nach Bedrohungslevel geordnete Aktionspunkte, um Ihren allgemeinen Sicherheitsstatus zu verbessern.

Werden aktive Angreifer erkannt, können Sie auf die Trustwave-Experten für Digital Forensics & Incident Response (DFIR) für eine Untersuchung des Sicherheitsvorfalls zurückgreifen. Außerdem bieten wir einen nahtlosen Übergang zu unseren umfassenderen Angeboten im Bereich Managed Threat Detection and Response, wie beispielsweise Managed Detection and Response Complete, das ein fortlaufendes Threat Hunting beinhaltet. Dabei erfolgt das Threat Hunting mehrmals im Jahr und konzentriert sich mit jedem Vorgang gezielter auf die Erkennung von Anomalien.

Fallstudie

Gesundheitswesen

Sachverhalt

Nach einer Geschäftsübernahme führte der Kunde Systeme, Geräte und Netzwerke zusammen.

Entdeckung

Während eines Proactive Threat Hunting fanden die Threat Hunter mehr als 100 Dateien mit unverschlüsselten Passwörtern. Einige der Dateien hießen Passwords.txt, Shared-passwords.xls, mypasswords.txt, usw. Viele dieser Passwörter stammten aus unternehmenskritischen Healthcare-Applikationen.

Bedrohung

Angreifer wissen beim ersten Eindringen nicht sofort, wo kritische Assets zu finden sind. Sind Dateien mit Passwörtern einfach aufzufinden, ist so, als ob man einem Dieb die Haustürschlüssel gibt.

Ergebnis

- Es wurde empfohlen, die Dateien zu entfernen und einen Passwortmanager einzusetzen.
- Das Risiko von Datenmissbrauch und möglichen HIPPA-Verstößen wurde minimiert.

Weitere Informationen zu diesen und anderen Trustwave-Produkten sowie -Services finden Sie unter www.trustwave.com.

[1] Gartner, Using Threat Hunting for Proactive Threat Detection, Michael Clark und Augusto Barros, 18. Mai 2020

Trustwave®

Weitere Informationen unter: www.trustwave.com

PTH_0820