VECTRA
SECURITY THAT THINKS

E-BOOK

So umgehen Cyber-Angreifer die Signaturerkennung

AUTOMATISCHE BEDROHUNGSVERWALTUNG

OPERATIVE EFFIZIENZ

CLOUD-NATIVES

UNTERNEHMEN

Gefährdung durch die Cyber-Sicherheitslücke

Zwischen dem Zeitpunkt, an dem ein Angreifer das Eindringungsschutzsystem umgeht, und dem Zeitpunkt, an dem das Unternehmen den Diebstahl oder die Zerstörung wichtiger Assets feststellt und mit der Behebung beginnt, besteht eine enorme Lücke.

Den Angreifern bringt diese Cyber-Sicherheitslücke einen gewaltigen Vorteil. Sie können mit komplexen und intelligenten Angriffsmethoden problemlos Signaturen, Reputationslisten und andere präventive Sicherheitsmaßnahmen umgehen.

Der herkömmliche und verbreitete Ansatz zur Bedrohungserkennung ist reaktiv und verschafft den Cyber-Kriminellen den Vorteil des ersten Schrittes.

Signaturen, Reputations- und Blockierungslisten erkennen Bedrohungen nur dann, wenn sie bereits bekannt sind, d. h. wenn es bereits ein Opfer gab. Niemand möchte dieses erste Opfer sein.

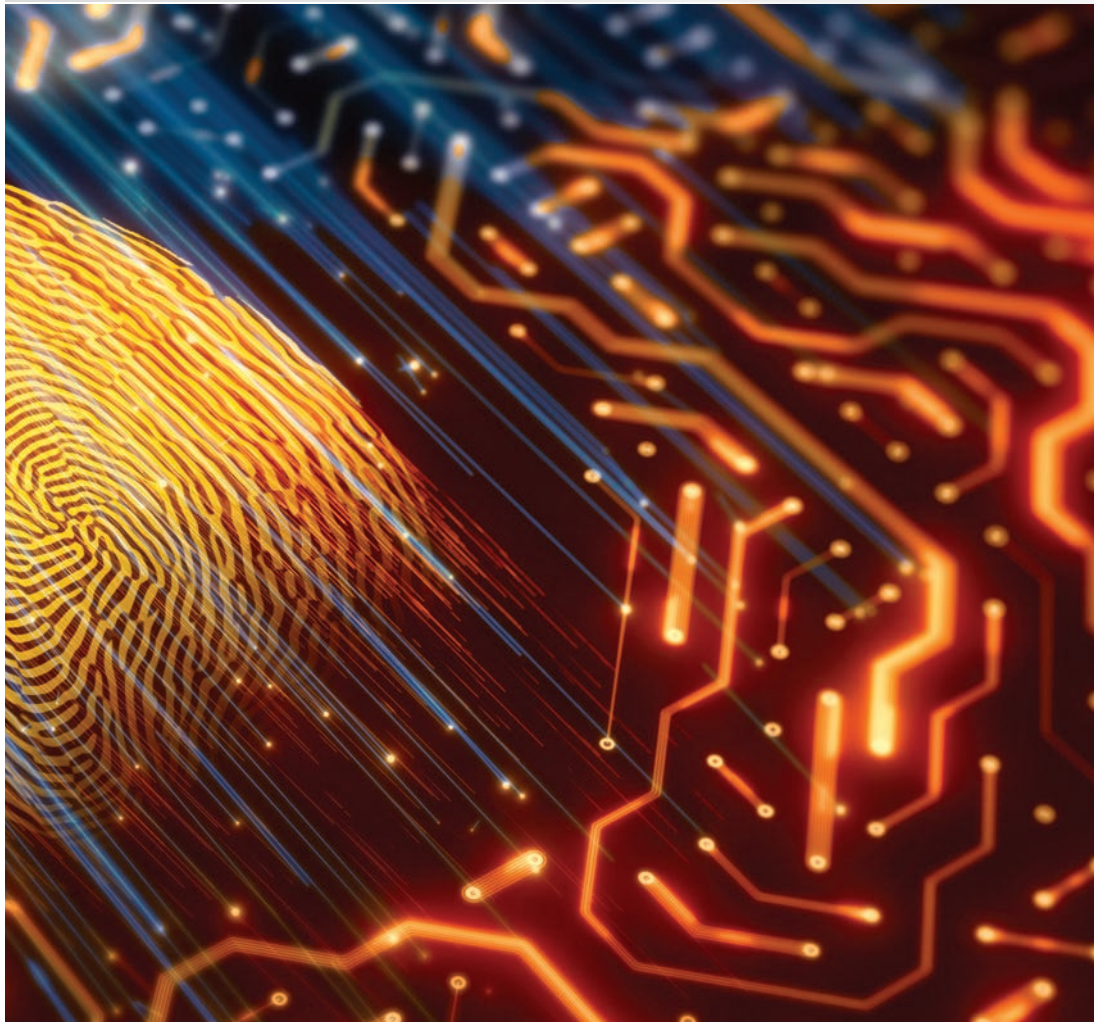
Die Erkennung von Bedrohungen hängt meist von wichtigen Sicherheitsanwendungen ab, die auf Endgeräten und Gateways installiert werden. Neue Bedrohungen werden in virtuellen Sandboxes erkannt und automatisch neue Signaturen generiert. Dieser Prozess erfordert Zeit – während dessen sich Malware auf Endgeräten festsetzen kann und Netzwerke gefährdet.

Der Ansatz mit der Erstellung neuer Signaturen hat sich in der Vergangenheit bewährt und bildet die Grundlage für alle Schutzlösungen – von Virenschutz über Firewalls der nächsten Generation bis zu Systemen zur Vermeidung und Erkennung von Eindringungsversuchen (IPS bzw. IDS). Bei diesem Ansatz bleiben die Verteidiger allerdings stets einige Schritte hinter den Angreifern. Gleichzeitig kann er ein falsches Gefühl der Sicherheit vermitteln.

Während Signaturen bekannte Bedrohungen wie Trojaner, Rootkits und anderen Schadcode stoppen können, droht die größte Gefahr durch noch nicht erfasste Bedrohungen. Wir wissen nicht, ob sie existieren und was sie können, und wir haben keine Signaturen, um sie zu erkennen.

70–90 %

Etwa 70 bis 90 Prozent der Malware-Varianten haben Eigenschaften, die auf das angegriffene Unternehmen zugeschnitten sind.



Inhärente Beschränkungen

Signaturen sind nützlich, ganz besonders bei der Erkennung großmaßstäblicher Bedrohungen wie Command & Control-Kommunikationen mit Botnets, automatisierte Crawler und Schwachstellenscanner, die das Internet durchforsten.

Der alleinige Fokus auf Signaturen sorgt jedoch für mehrere blinde Flecken, die von unzähligen gefährlichen Angriffen ausgenutzt werden.

Angreifer, die nicht auf die Kontrolle vieler Systeme, sondern auf verborgene Aktivitäten aus sind, können Signaturen umgehen. Gleichzeitig gehen diese raffinierten Angreifer eher strategisch vor und gefährden Unternehmen daher erheblich.

Wenn Sie die blinden Flecken der Signaturen verstehen möchten, müssen Sie deren Schwachstellen kennen.

Signaturen reagieren zum Beispiel nicht auf Bedrohungen durch Insider, d. h. sie bieten keine Möglichkeit, böswillige Insider mit legitimen Zugriffsrechten und Tools zu erkennen und zu stoppen. Das Verhalten der Angreifer und Abweichungen von „normalen“ Aktivitäten lassen sich mit Signaturen nicht erkennen.

Laut dem Verizon Data Beach Investigation Report 2020 (Verizon-Bericht zur Untersuchung von Datenkompromittierungen) werden Malware-basierte Angriffe zunehmend durch Angriffe ersetzt, bei denen Anmeldedaten im Mittelpunkt stehen.

Individuell erstellte Malware ist ebenfalls in der Lage, Signaturen zu umgehen. Die meisten Malware-Varianten sind unternehmensspezifisch und können daher nicht von Signaturen aufgespürt werden. Etwa 70 bis 90 Prozent der Malware-Varianten haben Eigenschaften, die auf das angegriffene Unternehmen zugeschnitten sind.

Angreifer individualisieren die Malware nicht, sondern ändern bestehende Varianten nur so weit, dass sie von Signaturen nicht erfasst werden. Für Malware-Signaturen werden Hashes bekannt gefährlicher Dateien erstellt, sodass selbst kleinste Änderungen den erfolgreichen Abgleich verhindern.

Angreifer fügen einfach ein paar Bits zur Malware-Datei hinzu, sodass der Hash-Wert nicht mehr als Malware erkannt wird. Diese Änderungen erfolgen automatisch und ohne menschliche Interaktion, sodass sich täglich unzählige, scheinbar individuelle Varianten erstellen lassen.

Wichtig ist dabei zu beachten, dass sich die Bits unterscheiden, nicht aber das Verhalten. Die Änderungen, die die signaturbasierte Erkennung verhindern, sind nur oberflächlich.

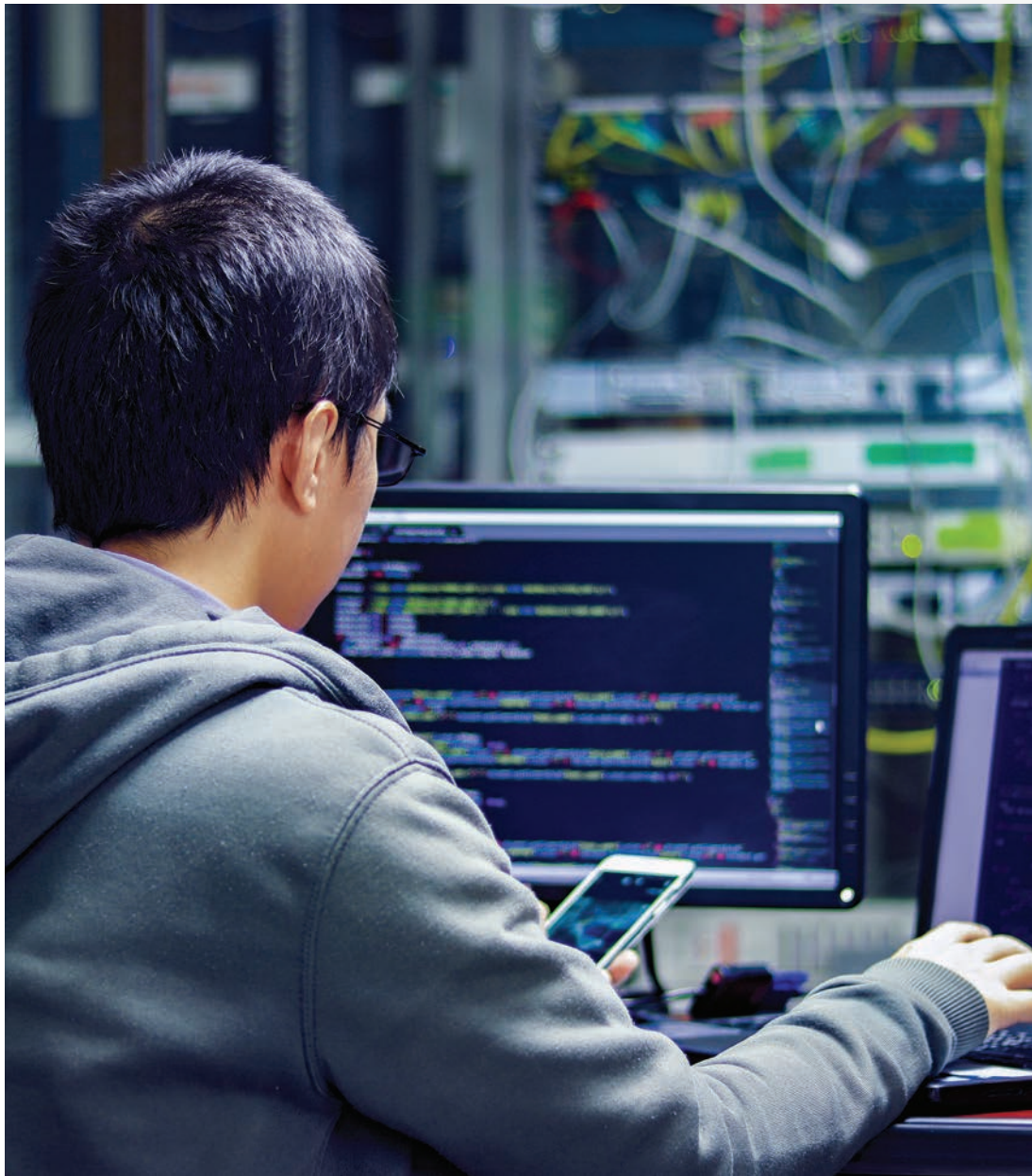
Signaturen übersehen auch Zero-Day-Angriffe, die auf Schwachstellen in Software und Betriebssystemen abzielen, zum Beispiel Heartbleed oder Duqu 2.0. Da Signaturen nur bekannte Bedrohungen stoppen, können sie diese Schwachstellen in der Praxis unmöglich abdecken.

Überwachen von Verhaltensweisen

Angreifer können Malware verändern, nach unbekannten Schwachstellen suchen und Daten von Systemen stehlen, für die sie legitime Zugriffsrechte haben, doch ihre Verhaltensweisen sind immer gleich: Sie spionieren, verbreiten sich und stehlen Daten aus dem Netzwerk ihrer Opfer.

Diese Verhaltensweisen lassen sich überwachen, wodurch Unternehmen einen Echtzeit-Einblick in aktive Bedrohungen innerhalb ihrer Netzwerke erhalten. Heute ergänzen kluge Unternehmen ihre signaturbasierten Funktionen um automatisierte Funktionen für Netzwerk-Erkennung und Response (NDR).

Diese Funktionen kombinieren Datenwissenschaft, maschinelles Lernen und Verhaltensanalysen sowie automatische Bedrohungsverwaltung zur Erkennung von böswilligem Verhalten innerhalb des Netzwerks. So werden Bedrohungen unabhängig davon erkannt, ob der Angreifer von innen oder außen angreift und ob er versucht, Signaturen zu umgehen.



Durch die Konzentration auf Verhaltensweisen und Aktionen kann NDR ohne Zuhilfenahme von Signaturen oder Reputationslisten jede Phase eines aktiven Angriffs erkennen – Command & Control, Botnet Monetization, Internal Reconnaissance, Lateral Movement und Exfiltration von Daten.

Verhaltensbasierte Bedrohungserkennung ermöglicht zudem die Identifizierung interner Reconnaissance- und Port-Scans, von Kerberos-Client-Aktivitäten und Malware-Ausbreitung innerhalb des Netzwerks. Datenwissenschaftsmodelle sind eine effektive Möglichkeit, Taktiken von Angreifern zu neutralisieren, bei denen mit Domain-Generatoren unzählige URLs für Attacken generiert werden.

Weitere Informationen erhalten Sie von unseren Servicemitarbeitern unter sales-inquiries@vectra.ai.

Cyber-Kriminelle suchen stets nach neuen Methoden, ihre Angriffskommunikation zu verbergen. Zu den effektivsten und am schnellsten wachsenden Taktiken gehört das Verbergen in einem anderen zulässigen Protokoll.

So können Angreifer zum Beispiel legitime HTTP-Kommunikation nutzen und kodierte Nachrichten in Textfeldern, Headern und anderen Parametern integrieren – und auf diese Weise kommunizieren, ohne erkannt zu werden.

Die von automatischer Bedrohungsverwaltung genutzten Erkennungsmodelle können diese verborgenen Tunnel jedoch aufdecken, indem sie Timing, Volumen und Reihenfolgen des Traffic erkennen und analysieren.

Den Netzwerkbedrohungen einen Schritt voraus bleiben

Angreifer sind flexibel und können ihre Exploits problemlos erstellen und auf unzählige Weisen verbergen. Daher sollten die nur eingeschränkt wirkungsvollen Signaturen um automatische Bedrohungsverwaltungsmodelle ergänzt werden, die kontinuierlich neues Angriffsverhalten lernen und sich an Netzwerkänderungen anpassen.

Es ist Zeit, das Hamsterrad der Signaturerstellung zu verlassen und sich einen Vorsprung vor den Angreifern zu verschaffen, indem Sie Angriffsverhaltensweisen und Aktionen erkennen und analysieren sowie Bedrohungen beseitigen, bevor Schaden entsteht.

E-Mail: info_dach@vectra.ai vectra.ai/de