Trustwave®

Blended Threats-Modul und Secure Email Gateway

AUSSCHALTEN VON GEZIELTEN ANGRIFFEN

Überblick

Kriminelle, die gezielte Angriffe auf Basis von E-Mails mit komplexen Bedrohungen organisieren, verwenden Social-Engineering-Methoden, um E-Mail-Nachrichten zu erstellen, die von vertrauenswürdigen Absendern zu stammen scheinen, jedoch einen Link zu einer Website mit bösartigem Code enthalten. Sie nutzen dann verschiedene Tools, um verstärkt Zugang auf Informationen und Systeme zu erhalten.

Das Trustwave Blended Threats-Modul in Verbindung mit dem Trustwave Secure Email Gateway (SEG-Produkte) bietet eine leistungsfähige Lösung, die vor gezielten Angriffen und komplexen Bedrohungen schützt. Mithilfe von Verhaltensanalysen und Inhaltsprüfungen in Echtzeit sperrt das Trustwave Blended Threats-Modul alle Websites, die verdächtigen oder bösartigen Code enthalten. Da dieser Dienst ohne Signaturen auskommt, ist er hinsichtlich der Erfassung und Neutralisierung neuer Gefahren immer auf dem neuesten Stand.

So funktioniert es

Trustwave SEG-Produkte (On-Premise)

Mit Trustwave SEG kann konfiguriert werden, welche URLs wann umgeschrieben werden müssen. Administratoren können zahlreiche Regelkriterien verwenden, um sicherzustellen, dass ihre Richtlinie die Anforderungen exakt erfüllt. Für noch mehr Flexibilität und Kontrolle bei der Aufstellung von Regeln für das Umschreiben von URLs können URLs einer Positivliste (Whitelist) hinzugefügt werden. Alle URLs, die umgeschrieben wurden, werden dann über das cloudbasierte Trustwave Blended Threats-Modul umgeleitet.

Trustwave Blended Threats-Modul (cloudbasierter Dienst)

Das Trustwave Blended Threats-Modul bietet kompromisslose Sicherheit ohne Mehraufwand für die Verwaltung. Durch diesen cloudbasierten Dienst wird der Schutz auf alle Empfänger ausgedehnt, an die ein von Trustwave SEG-Produkten umgeschrieber Link weitergeleitet wurde.

Das Trustwave Blended Threats-Modul analysiert täglich Millionen von URLs und bietet somit Schutz vor gezielten Angriffen und komplexen Bedrohungen. Diese Daten fließen dann in die Forschung des Trustwave Labors ein.

Das Trustwave Blended Threats-Modul verwendet dieselbe Technologie wie das Trustwave SWG, um die wahre Absicht einer Website zu analysieren. Anstatt sich auf reputations- oder signaturbasierten Schutz zu verlassen, teilt das Modul eine Website in ihre einzelne Komponenten (HTML, Java, Flash, ActiveX usw.) auf und unterzieht jeden Teil einer speziell dafür vorgesehenen Analysemethode. Alle verborgenen oder ausgeblendeten Informationen werden dekodiert und ebenfalls einer eingehenden Analyse unterzogen. In einer zusätzlichen tiefgreifenden Codeanalyse wird ein Verhaltensprofil bestimmt, das jegliche potenzielle bösartige Kombination der einzelnen Funktionen aufdeckt. Dadurch werden unbekannte und dynamische Bedrohungen identifiziert und entschärft.

Wird auf einer Website bösartiger Code gehostet, informiert das Trustwave Blended Threats-Modul den Benutzer darüber, dass der Zugriff verweigert wurde. Da die URL von den Trustwave SEG-Produkten bereits umgeschrieben wurde, wird der Schutz auch all denjenigen gewährt, an die die Nachricht anschließend weitergeleitet wurde, einschließlich Benutzern, die versuchen, über ein Mobilgerät oder Webmail auf die kompromittierte Website zuzugreifen.

Seg-Produkte – Ablauf

1. Die Trustwave SEG-Produkte empfangen die zu scannende E-Mail und entscheiden, ob eine URL im Nachrichtentext analysiert werden muss. Die URL wird umgeschrieben und mit einem eindeutigen Kundenreferenzvorsatz und einem Link zum Trustwave Blended Threats-Modul versehen.
2. Wenn ein Benutzer auf den Link klickt, wird die Anfrage zur Analyse durch das Trustwave Blended Threats-Modul geleitet.
3. Das Trustwave Blended Threats-Modul analysiert den mit dem Link verbundenen Webinhalt und unterzieht diesen mehreren Verhaltens- und Absichtsprüfungen.
4. Wenn die Website keinen bösartigen Code enthält, wird sie an den Benutzer freigegeben. Andernfalls wird dem Benutzer eine Seite mit einem Sperrhinweis angezeigt, die darauf hinweist, dass er vor einem gezielten Angriff geschützt wurde.

Merkmal/Vorteile-Matrix

Merkmal	Vorteile
Mehrschichtige Anti-Malware-Engine mit dynamischer Codeanalyse in Echtzeit durch Trustwave SWG	Bei gezielten und opportunistischen Angriffen werden ausgereifte Techniken zur Verhinderung einer Aufdeckung, zur Ausnutzung von Schwachstellen und zur Gefährdung von Computern verwendet. Durch die Codeanalyse in Echtzeit wird das Verhalten und die Absicht eines von einer Website präsentierten Codes sofort identifiziert. Sie kommt ohne Signaturen zum Schutz vor bekannten und bisher unbekannten Angriffen aus. Diese stellen 60 % der modernen Malware dar, die von Antivirus-, Firewall-, IPS/IDS- und reputationsbasierten Lösungen übersehen wird. Da die Gefährdung der Rechner schon vorab verhindert wird, werden die mit erfolgreichen Malware-Angriffen verbundenen Kosten für beispielsweise Desktop-Reimaging, Datenverlust, Rufschädigung oder sogar Geldstrafen vermieden.
Umschreibung der URLs	Bei einer umgeschriebenen URL wird der Link bei jedem Anklicken vom Trustwave Blended Threats-Modul gescannt, auch wenn diese E-Mail im Anschluss weitergeleitet wurde. Dadurch wird sichergestellt, dass die Zielwebsite zum Zeitpunkt des Zugriffs gescannt wird und keine Lücke für einen möglichen Angriff bleibt.
Scannen der Websites direkt beim Zugriff	Bei einem gestaffelten gezielten Angriff wird der bösartige Code auf einer Website eventuell erst nach einer bestimmten Zeit oder für kurze Zeitabschnitte im Verlauf des Tages aktiviert. Aufgrund dieses „Versteckens“ und der möglichen Veränderung des bösartigen Codes ist es sehr wichtig, dass eine Website bei jedem Zugriff über einen nicht vertrauten Link und dynamische Websites gescannt wird.
Rückmeldung an Trustwave SEG-Produkte	Das Trustwave Blended Threats-Modul leitet auf regelmäßiger Basis Informationen an die Trustwave SEG-Produkte zurück, um wichtige Daten für die Berichterstellung und Analyse bereitzustellen. Diese Daten ermöglichen Administratoren die Identifizierung von Benutzern, die ein besonderes Ziel für Angriffe sind bzw. die womöglich eine zusätzliche Schulung zum Sicherheitsbewusstsein benötigen. Ferner können diese Daten dazu verwendet werden, basierend auf der Anzahl der verhinderten Angriffe die Rendite darzustellen, die durch diesen Dienst erzielt wurde.
Seite mit Sperrhinweis informiert den Benutzer über die Bedrohung	Die Benachrichtigung der Benutzer über potenzielle Bedrohungen hält diese nicht nur vom Besuchen von Websites mit bösartigem Code ab, sie erinnert sie außerdem an sichere Computing-Gewohnheiten sowie vorsichtigere Verfahrensweisen beim Browsen im Internet.
Hybride Architektur	Ein hybrider Ansatz bietet die Vorteile eines Dienstes kombiniert mit der Genauigkeit eines On-Premise-Produkts. Das Trustwave Blended Threats-Modul hilft bei der Reduzierung der Verwaltungs-Gemeinkosten und sorgt für erhöhte Sicherheit. Es lässt sich auf einfache Weise konfigurieren und verwalten und bietet laufende, von Trustwave verwaltete Sicherheitsupdates, die im Einklang mit den neuesten Forschungserkenntnissen und den vom Trustwave SpiderLabs-Team erfassten Bedrohungsinformationen gestaltet sind.

ERFAHREN SIE MEHR AUF TRUSTWAVE.COM

Trustwave®