SONICWALL

WORAUF ADMINISTRATOREN BEIM KAUF EINER ENDPUNKTSICHERHEITSLÖSUNG ACHTEN SOLLTEN

Eine neue Sicht auf die Herausforderungen des Endpunktschutzes

Zusammenfassung

Das Thema Endpunktsicherheit bereitet vielen Administratoren Kopfzerbrechen. Diese Lösungsübersicht befasst sich mit den häufigsten Herausforderungen, wie zum Beispiel:

- Wartung und Umsetzung der Sicherheitslösung
- verschlüsselte und ausgeklügelte Bedrohungen
- Warnmeldungen und Problembehebung

Einleitung

In einer Welt, in der Cyberkriminelle ihre Angriffe ständig weiterentwickeln, spielt die Verwaltung und Sicherheit von Endpunkten eine wichtige Rolle. Heutige Benutzer checken ständig mit ihren Endpunktgeräten in das Netzwerk ein und aus. Genau diese Endpunkte stehen im Mittelpunkt modernster und extrem raffinierter Cyberbedrohungen. Immer mehr verschlüsselte Bedrohungen gelangen ungeprüft an Endpunkte, Ransomware befindet sich auf dem Vormarsch und auch Anmeldedaten sind ständig von Diebstahl betroffen. Angesichts der kontinuierlich wachsenden Gefahr durch Ransomware und andere bösartige malwarebasierte Angriffe wird allerdings deutlich, dass Client-Sicherheitslösungen nicht nur anhand der Endpunkt-Compliance bewertet werden können.

Die Herausforderungen rund um den Endpunktschutz

Obwohl es bereits seit Jahren Produkte für die Endpunktsicherheit gibt, tun sich Administratoren immer noch in folgenden Bereichen schwer:

- Sicherheitsprodukte auf dem neuesten Stand halten
- Durchsetzung von Regeln und Compliance-Vorgaben
- Reporting
- Bedrohungen über verschlüsselte Kanäle
- Warnmeldungen und Problembehebung
- Lizenzverwaltung
- Abwehr hoch entwickelter Bedrohungen wie Ransomware

Sicherheitsprodukte auf dem neuesten Stand halten

Laut Compliance-Regeln müssen Administratoren sicherstellen, dass auf verwalteten Endpunkten die korrekte Version der Sicherheitssoftware läuft.

Netzwerkadministratoren benötigen verwaltete Endpunkte, um regelmäßig über deren Status berichten zu können und ihr Sicherheitskonzept kontinuierlich zu prüfen. Nur so können sie neue Bedrohungen effektiv abwehren.

In manchen Fällen müssen Administratoren den East-West-Traffic in ihren Rechenzentren stoppen, der oft einen Großteil des Datenverkehrs ausmacht. Geräte, die infiziert oder nicht regelkonform sind, sollten sie lokal unter Quarantäne stellen können. In solchen Situationen muss die Firewall den Zugang zum Internet und die Verbindung zum LAN blockieren, um so die Netzwerkpfade zu den von der Firewall unter Quarantäne gestellten Orten einzuschränken.

Um die Integrität der Daten sicherzustellen, müssen Administratoren zudem dafür sorgen, dass die Daten zwischen dem einheitlichen Client und der zentralisierten Verwaltungskonsole während der Übertragung nicht manipuliert werden können.

Durchsetzung von Regeln und Compliance-Vorgaben

Sind die Endpunkte nicht richtlinienkonform, müssen Administratoren verhindern können, dass die Endpunktgeräte UTM-Services nutzen, um Datenverkehr durch die Firewall zu übertragen. Auch Endbenutzer spielen eine wichtige Rolle bei der Endpunktsicherheit. Oft nutzen sie Firmenlaptops und andere Endpunkte, um ihre Aufgaben zu erledigen. Daher sollten sie umgehend informiert werden, wenn bösartige Software oder ungewöhnliches Verhalten identifiziert wird, sodass sie bei Bedarf entsprechende Maßnahmen treffen oder ein Ticket erstellen können.

Reporting

Es kann vorkommen, dass Administratoren für mehrere Firewalls zuständig sind, deren Benutzer in einem einzigen Pool konfiguriert sind. Um Client-Regeln zu verwalten, ist es wichtig, dass sie von Firewall-Administratoren oder über Sicherheitsmanagementkonsolen einen Single-Sign-on(SSO)-Zugriff erhalten. Gleichzeitig verlangt die Compliance oft, dass sich alle administrativen Rollen am Least-Privilege-Prinzip orientieren. Somit sollte das Unified-Client-Management eine ausreichende rollenbasierte Zugriffskontrolle für einen privilegierten Zugriff haben. Diese könnte sich beispielsweise auf zwei Rollen beschränken: eine mit Read-/Write-Zugriff und eine andere mit Read-only-Zugriff.

Bedrohungen über verschlüsselte Kanäle

Bedenkt man, dass heute immer mehr Webanwendungen über verschlüsselte Kanäle wie HTTPS geschützt werden und auch Malware Verschlüsselungstechnologien nutzt, um eine netzwerkbasierte Prüfung zu umgehen, ist eine Prüfung des SSL-/TLS-Verkehrs (DPI-SSL) mittels Deep Packet Inspection heute unbedingt notwendig. Möchte man allerdings Sicherheitsprobleme und eine Beeinträchtigung der Benutzererfahrung vermeiden, lässt sich das meist nur durch einen massiven Einsatz vertrauenswürdiger SSL-/TLS-Zertifikate für alle Endpunkte erreichen. Dies erfordert einen Mechanismus für die Distribution und Verwaltung von Zertifikaten sowie für die Kriterien, anhand derer der Browser diese Zertifikate als vertrauenswürdig einstuft.

Warnmeldungen und Problembehebung

Endbenutzer kennen sich mit Sicherheitsrisiken in der Regel weniger gut aus als Sicherheitsexperten. Daher ist es wichtig, dass ihre Endpunktsicherheitsplattform sie auf ein verändertes Risikoprofil hinweist – zum Beispiel wenn sie mit ihrem Laptop verreisen – und Sicherheitstipps gibt.

Beispielsweise könnte eine Warnmeldung von einem einheitlichen Client oder einer Drittanbietersoftware generiert werden. Alternativ könnten Benutzer auf eine externe Quelle wie eine Webseite umgeleitet werden.

Um Probleme bei der Einhaltung unternehmensspezifischer Regeln rasch zu beheben, kann es sowohl für Endbenutzer als auch für die IT hilfreich sein, wenn Endbenutzer Zugriff auf Informationen erhalten, die ihnen sagen, wie sie das Problem selbst beheben können. Wenn das Gerät eines Benutzers nicht regelkonform ist und unter Quarantäne gestellt wird, benötigt der User auch Unterstützung und Informationen darüber, wie er die Compliance wiederherstellen kann.

Lizenzverwaltung

Administratoren müssen sicherstellen, dass ihre Endpunktsicherheitslösungen automatisch aktualisiert und an ihre Verwaltungsschnittstelle angepasst werden, sodass eine korrekte Lizenzierung der Endpunkte gewährleistet ist. Beispielsweise sollten sämtliche Lizenzdaten für einen Kunden zentral überwacht und gespeichert werden. Beim Erwerb einer neuen Lizenz sollte die zentralisierte Unified-Client-Managementlösung einen Hinweis erhalten, um den Berechtigungsprozess für die Software zu starten.

In regelmäßigen Abständen müssen einige Administratoren Compliance-Berichte für alle implementierten Drittanbieterlizenzen ausführen, um ihre Partner zu bezahlen.

Abwehr hoch entwickelter Bedrohungen wie Ransomware

Mit traditionellen Lösungen ist es nicht immer möglich, alle administrativen Anforderungen zu lösen. Der veraltete signaturbasierte Ansatz herkömmlicher Antivirentechnologien ist angesichts der schnellen Entwicklungszyklen neuer Malware sowie der immer raffinierteren Umgehungsmethoden wirkungslos. Für den modernen Client-Schutz sind neue Strategien gefragt, die nicht nur auf hoch entwickelte Engines zur Bedrohungserkennung setzt, sondern auch einen mehrschichtigen Schutz auf Endpunkten unterstützt.

Ein großes Problem aktueller Insellösungen (bekannt als Enforced AV-Clients) besteht darin, dass sie speziell für einen bestimmten Drittanbieter entwickelt und in das Angebot dieses Drittanbieters integriert wurden. Administratoren benötigen ein offeneres Modell, das eine relativ schnelle Erweiterung mit zusätzlichen Sicherheitsmodulen erlaubt, wenn dies aus Sicht des Unternehmens oder der Industrie erforderlich ist.

Fazit

Endpunkte werden zunehmend als Angriffsvektor genutzt. Sicherheitsexperten müssen daher Maßnahmen ergreifen, um Endpunktgeräte besser zu schützen. Mit der zunehmenden Verbreitung von Trends wie Telearbeit, Mobilität und BYOD ist es außerdem extrem wichtig, sämtliche Clients unabhängig von ihrem Standort konsequent zu schützen.

Sicherheitsadministratoren müssen bei der Evaluierung von Endpunktlösungen stets die praxisrelevanten Anforderungen im Auge behalten.

Erfahren Sie mehr. Lesen Sie unsere Lösungsübersicht Maßgeschneiderte Endpunktsicherheit für Ihre Organisation oder besuchen Sie uns unter www.sonicwall.com/capture-client.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com