Der Triple-A-Ansatz zur Netzwerksicherheit

Florian Malecki, International Product Marketing Director, Dell Networking Security

Zusammenfassung

Wie wissen IT-Entscheidungsträger, wann ihre Organisation ein Maß an Sicherheit erreicht hat, bei dem Schutz vor Cyberangriffen gewährleistet ist und Mitarbeiter gleichzeitig bei ihrer Arbeit unterstützt werden? In diesem Exposé werden die drei grundlegenden Faktoren erläutert, die für einen umfassenden Sicherheitsansatz erforderlich sind. Organisationen, deren Netzwerksicherheit bei allen drei Faktoren gut abschneidet, verdienen eine Triple-A-Bewertung.

Einführung

Triple-A-Bewertungen werden meist mit Chief Financial Officers (CFOs) in Verbindung gebracht, die Anleiheratings oder Kreditwürdigkeit kontrollieren. Wie kann ein CIO oder IT-Entscheidungsträger in der Welt der IT die Effizienz einer IT-Sicherheitsimplementierung bewerten?

Die IT-Sicherheit ist die größte Sorge von IT-Entscheidungsträgern, da aktuelle Sicherheitslücken wie beispielsweise Shellshock und Heartbleed Organisationen auf der ganzen Welt betreffen. Daher ergreifen IT-Entscheidungsträger Maßnahmen, um das Unternehmensnetzwerk vor Bedrohungen aller Art zu schützen.

Dennoch wird die Sicherheit durch interne und externe Faktoren gefährdet.

Wie wissen IT-Entscheidungsträger, wann sie ein Maß an Sicherheit erreicht haben, bei dem Schutz vor Cyberangriffen gewährleistet ist und Mitarbeiter gleichzeitig bei ihrer Arbeit unterstützt werden? Ein umfassender Sicherheitsansatz sollte drei Faktoren berücksichtigen:

- Er sollte **adaptiv** sein, das heißt, sich an Bedrohungen, Geschäftsanforderungen und die sich ändernde Internetnutzung im Unternehmensnetzwerk anpassen lassen.
- Er sollte **angepasst** sein, um die spezifischen Anforderungen der Organisation zu erfüllen.
- Er sollte von den Endbenutzern vollständig **angewendet** werden.

Ein Sicherheitsansatz ist jedoch nur dann effektiv, wenn ihm auch passende Sicherheitsinfrastruktur zugrunde liegt. Bei der Implementierung einer neuen Lösung für das Sicherheitsportfolio Ihres Netzwerks müssen Sie sich vergewissern, dass der Anbieter auch in der Lage ist, mit der Lösung das Wachstum Ihrer Organisation zu unterstützen. Es gilt sozusagen das Prinzip: "Mehr Sicherheit, bessere Geschäfte!"

73 % aller Organisationen weltweit haben in den vergangenen zwölf Monaten bereits eine Sicherheits-verletzung erlebt.

Diese Faktoren können zusammenfassend als Triple-A-Sicherheitsansatz bezeichnet werden. Wenn Sie dies erreichen, können Sie die Gesamtsicherheit stärken und gewährleisten, dass Ihre Organisation bei der Sicherheit mit Triple-A bewertet wird. Lesen Sie weiter, um zu erfahren, wie Sie einen Sicherheitsansatz mit Triple-A-Status erreichen und wie die IT-Sicherheit Innovationen fördern kann, statt sie zu behindern.

Adaptiv

IT-Infrastrukturen verändern sich ständig. In der Vergangenheit waren IT-Infrastrukturen statisch, die Entwicklung geht jedoch in Richtung Konvergenz. Daher müssen Sicherheitsinfrastrukturen angepasst werden, um effektiv sein zu können. Eine adaptive Sicherheitsarchitektur sollte präventiv, detektivisch, retrospektiv und prädiktiv sein. Zudem sollte ein abgerundeter Sicherheitsansatz kontextsensitiv sein.

Gartner beschreibt die sechs wichtigsten Trends, die den Bedarf nach adaptiven, kontextsensitiven Sicherheitsinfrastrukturen verstärken: zunehmende Mobilität, Auslagerung und Zusammenarbeit, Virtualisierung, Cloud Computing, Consumerization und die Industrialisierung der Hacker.[1] Doch was genau ist mit "kontextsensitiv" gemeint? Gartner definiert kontextbezogene Sicherheit als "die Nutzung ergänzender Informationen zur Verbesserung der Sicherheitsentscheidung zum Zeitpunkt der Entscheidung" und sagt voraus, dass im Jahr 2015 90 % der von Unternehmen eingesetzten Sicherheitslösungen kontextsensitiv sein werden.

Die Voraussetzung für adaptive, kontextsensitive Sicherheit besteht darin, dass alle Sicherheitsentscheidungen auf Informationen beruhen, die aus verschiedenen Quellen stammen. Dies beginnt bei der Berücksichtigung des Kontexts der Anfrage und der Zulassung und Blockierung der Aktion basierend auf den verfügbaren Informationen, z. B. verwendete Authentifizierungsmethode, Uhrzeit, usw. Durch diesen adaptiven Ansatz kann die Sicherheit verbessert werden.

Angepasst

Jede Organisation ist anders, warum sollte für die Sicherheitsimplementierung nicht das gleiche gelten? Sicherheitslösungen müssen flexibel sein, um die spezifischen Geschäftsanforderungen der Organisation zu erfüllen. Obwohl wir mehr denn je in den Schutz unserer Systeme sowie in die Einhaltung unternehmensinterner und regulatorischer Auflagen investieren, gibt es immer etwas, das durchs Raster fällt. Laut einer von Vanson Bourne im Auftrag von Dell durchgeführten Studie haben 73 % aller Organisationen weltweit in den vergangenen zwölf Monaten bereits eine Sicherheitsverletzung erlebt.[2]

Es gibt Dutzende von "erstklassigen" Lösungen für einzelne Sicherheitsaspekte, wobei für die Softwareverwaltung dieser einzelnen Lösungen jeweils ein entsprechend geschulter Experte erforderlich ist. Und diese Lösungen greifen nicht optimal ineinander. Patchwork-Lösungen, bei denen Produkte verschiedener Anbieter zum Einsatz kommen, führen unweigerlich zu gegenseitigen Schuldzuweisungen.

Es gibt monolithische Sicherheits-Frameworks, die versuchen, alle Sicherheitsaspekte in einer einzigen Lösung zu berücksichtigen, doch diese sind so unflexibel und teuer in der Verwaltung, dass Organisationen ihren laufenden Betrieb als zu kostenintensiv empfinden. Diese Lösungen sind außerdem nicht auf die Geschäftsziele der Organisationen abgestimmt, obwohl sie Unternehmen eigentlich helfen sollten, diesen Zielen näher zu kommen.

Stattdessen sollten Organisationen auf einen Sicherheitsansatz setzen, der auf Einfachheit, Effizienz und Vernetzung fußt. Mit diesen Prinzipien können die verschiedenen Aspekte der IT-Sicherheit in einer einzigen, integrierten Lösung zusammenfasst werden, mit der Einblicke in der gesamten Organisation gewonnen werden können.

So ist auch sichergestellt, dass Unternehmensbenutzer Regeln und

[1] Neil MacDonald, Peter Firstbrook: "Designing an Adaptive Security Architecture for Protection From Advanced Attacks" (Entwurf einer adaptiven Sicherheitsarchitektur zum Schutz vor hochentwickelten Angriffen), Gartner, Inc., 12. Februar 2014, https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

[2] "Protecting the organization against the unknown" (Schutz des Unternehmens vor dem Unbekannten), Vanson Bourne, Februar 2014, http://software.dell.com/documents/protecting-the-organization-against-the-unknown-whitepaper-27396.pdf

Richtlinien verwalten und die Endbenutzer diese Regeln und Richtlinien problemlos einhalten können. Eine solche Lösung gewährleistet, dass Organisationen keinen Universalansatz verfolgen müssen, sondern einen an ihre spezifischen Anforderungen und Geschäftsziele angepassten Sicherheitsansatz implementieren können.

Angewendet

Bei jedem Sicherheitsansatz muss außerdem gewährleistet werden, dass die Sicherheitsrichtlinien von den Mitarbeitern verstanden und tatsächlich angewendet werden. Die IT- und die Sicherheitsinfrastruktur sind dazu gedacht, das Unternehmenswachstum zu unterstützen, z. B. indem die IT es Mitarbeitern ermöglicht, mobil zu arbeiten, und so zur Steigerung der Produktivität beiträgt. Gleichzeitig ist es unerlässlich, dass die Mitarbeiter Sicherheitsrichtlinien einhalten und in angemessener Weise auf Daten und Geschäftsanwendungen zugreifen. Andernfalls werden die Mobilitäts- und anderen Richtlinien, die das Wachstum des Unternehmens fördern sollen, zu einem Sicherheitsrisiko, das dem Unternehmen schaden kann.

Viele glauben, dass Sicherheitstools die Mitarbeiterproduktivität und die Geschäftsprozesse beeinträchtigen. Tatsächlich verwenden Benutzer Systeme nicht, wenn sie deren Funktionsweise nicht mögen oder sie das Gefühl haben, dass sie die Produktivität beeinträchtigen. Dadurch haben diese Systeme keinen geschäftlichen Wert mehr und können erst recht nicht zur Gewährleistung der Netzwerksicherheit beitragen.

Auch Mobilität kann bedeutet Sicherheitsrisiken bedeuten: Mitarbeiter machen ihre Organisation beispielsweise meist durch BYOD angreifbar. Während BYOD einerseits die Flexibilität der Mitarbeiter erhöht, steigt dadurch andererseits auch das Potenzial für durch Benutzer verursachte Sicherheitsverletzungen. Eine Umfrage ergab sogar, dass der Verlust von Daten auf Mobilgeräten aktuell eine der größten Sorgen von Unternehmen ist: 71 % der befragten britischen Unternehmen nannten die "zunehmende Nutzung von Mobilgeräten" als größte Gefahr für die IT-Sicherheit in den nächsten fünf Jahren.[3] Dieses Ergebnis erklärt zum Teil, warum einige britische Unternehmen zögern, ihren Mitarbeitern den Zugriff auf Unternehmensnetzwerke über private Geräte zu erlauben. 24 % der befragten britischen Unternehmen gaben an, dass weniger als ein Zehntel der Mitarbeiter private Geräte nutzen, also weniger als die weltweit durchschnittlichen 13 %. Daher ist es umso wichtiger, Mitarbeiter umfassend zu Sicherheitsangriffen und Schutzmöglichkeiten zu schulen.

Mit Mitarbeiterschulungen und Leitfäden zu Cybersicherheit können Sie dafür sorgen, dass Sicherheitsrichtlinien vollständig angewendet werden – dadurch sollte auch die IT-Abteilung einen starken Rückgang der von Mitarbeiteraktivitäten ausgehenden Sicherheitsrisiken feststellen können.

Triple-A

Wenn Sie bei Ihrer unternehmensweiten Sicherheitsrichtlinie bei allen drei As ein Häkchen setzen können, ist Ihre Sicherheit sehr hoch. Es genügt jedoch nicht, diese Überprüfung nur einmal durchzuführen. Zum Schutz vor Bedrohungen sollten Sie diese kurze Checkliste regelmäßig überprüfen, um sicherzustellen, dass maximale Sicherheit erreicht wird und aufrechterhalten bleibt. Außerdem sollten Sie sich vergewissern, dass alle eingesetzten Sicherheitslösungen es Ihrer Organisation ermöglichen, jederzeit zu wachsen, und bereits vorhandene Teile des Netzwerks nicht beeinträchtigen.

Die Triple-A-Bewertung ist insgesamt ein weitgehend anerkanntes und vertrauenswürdiges Konzept zur Beschreibung des finanziellen Zustands eines Unternehmens oder Landes. Ebenso ist der Triple-A-Sicherheitstest eine gute Möglichkeit zur Bewertung der Sicherheit von Unternehmensnetzwerken. Wenn Sie sicherstellen, dass Ihr Netzwerk mit Triple-A bewertet wird, können Sie gewährleisten, dass alle Bereiche des Unternehmensnetzwerks jederzeit geschützt sind.

Durch die Annäherung an dieses Framework wird es möglich, Lücken in der Netzwerksicherheit zu identifizieren, sodass zukünftige Angriffe vermieden werden können.

71 % der britischen Unternehmen sagen, dass die "zunehmende Nutzung von Mobilgeräten" in den nächsten fünf Jahren die größte Bedrohung für die IT-Sicherheit darstellen wird.

[3] Warwick Ashford: "Businesses ignore unknown threats despite cost, study shows" (Eine Studie zeigt, dass Unternehmen trotz der Kosten unbekannte Bedrohungen ignorieren), TechTarget/ ComputerWeekly.com, 20. Februar 2014; http://www.computerweekly.com/news/2240214754/ Businesses-ignore-unknown-threats-despite-cost-study-shows

Weitere Informationen

Über Dell Software

Dell Software unterstützt Kunden dabei, ihr Potenzial durch den Einsatz von Technologie voll auszuschöpfen – mit skalierbaren, erschwinglichen und benutzerfreundlichen Lösungen, die die IT vereinfachen und Risiken minimieren. Das Portfolio von Dell Software deckt Kundenanforderungen in fünf Schlüsselbereichen ab: Rechenzentrums- und Cloud-Verwaltung, Informationsverwaltung, Verwaltung mobiler Mitarbeiter sowie Sicherheit und Datensicherung. In Kombination mit Hardware und Services von Dell versetzen unsere Softwareprodukte Kunden in die Lage, effizienter und produktiver zu arbeiten und schnellere Geschäftsergebnisse zu erzielen. www.dellsoftware.com

Bei Fragen zur möglichen Nutzung dieses Dokuments wenden Sie sich bitte an:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Informationen zu unseren regionalen und internationalen Büros finden Sie auf unserer Webseite.