Grundprinzipien der Netzwerksicherheit - Teil 3: Zugriffsprotokolle und Vorgehensweisen

Sicherheitsvorfälle nehmen jedes Jahr mit alarmierender Geschwindigkeit zu. Je komplexer die Bedrohungen, desto komplexer werden auch die Sicherheitsmaßnahmen zum Schutz von Netzwerken. Die Mitarbeiter in Datencentern, Netzwerkadministratoren und andere Datencenterfachleute müssen die Grundlagen von Sicherheitsmaßnahmen kennen, um Netzwerke heute sicher einrichten und verwalten zu können. In dieser Fachartikelreihe werden die Grundlagen sicherer Netzwerksysteme sowie Firewalls, Netzwerktopologie und sichere Protokolle behandelt. Darüber hinaus werden empfohlene Vorgehensweisen erläutert, die den Lesern eine Einführung in die schwierigeren Aspekte der Sicherung von Netzwerken geben.

Sichere Zugriffsprotokolle

Es gibt eine Vielzahl von Protokollen wie SSH und SSL, die verschiedene kryptographische Verfahren verwenden, um Sicherheit durch Authentifizierungs- und Verschlüsselungsmethoden zu gewährleisten. Der Grad der Sicherheit hängt von vielen Dingen ab, beispielsweise von den verwendeten kryptographischen Methoden, vom Zugriff auf die übertragenen Daten, von der Länge der Algorithmusschlüssel, von Server- und Clientimplementierungen und vor allem von menschlichen Faktoren. Das genialste Verschlüsselungsschema wird wertlos, wenn die Anmeldeinformationen eines Benutzers, beispielsweise ein Kennwort oder ein Zertifikat, Dritten bekannt werden. Oben wurde bereits das klassische Beispiel aufgeführt, nämlich der an den Bildschirm geheftete Notizzettel mit dem Kennwort.

Das SSH-Protokoll

Das Client-Server-Protokoll Secure Shell (SSH) wurde Mitte der 90er Jahre entwickelt, um ein sicheres Verfahren für den Remotezugriff auf Computerkonsolen oder Shells über ungeschützte oder nicht sichere Netzwerke bereitzustellen. Das Protokoll ermöglicht die Verwendung „sicherer“ Methoden, da Benutzer und Server authentifiziert werden und der gesamte Datenverkehr zwischen Client und Server verschlüsselt wird. Es gibt zwei Protokollversionen, Version 1 und 2, die sich hinsichtlich der kryptographischen Mechanismen geringfügig unterscheiden. Version 2 ist darüber hinaus überlegen, da es in der Lage ist, vor bestimmten Arten von „Angriffen“ zu schützen. (Ein Versuch „unbeteiligter“ Dritter, ausgetauschte Daten abzufangen, zu fälschen oder auf andere Weise zu ändern, gilt als Angriff.)

SSH wird auf Computerkonsolen schon seit Jahren als sicheres Zugriffsprotokoll verwendet, während es auf Geräten der sekundären Infrastruktur wie USV- und HVAC-Geräten üblicherweise seltener verwendet wird. Da Netzwerke und die Netzwerkinfrastruktur, die diese unterstützt, für die Geschäftsprozesse von Unternehmen jedoch immer mehr an Bedeutung gewinnen, wird die Verwendung einer solchen sicheren Zugriffsmethode für alle Geräte immer mehr zur Regel.

Das SSL / TLS-Protokoll

Während SSH das normale sichere Protokoll für den Konsolenzugriff über eine Befehlszeile ist, wurden die Protokolle Secure Socket Layer (SSL) und später auch Transport Layer Security (TLS) zum Standardverfahren für die Sicherung des Webverkehrs und anderer Protokolle wie SMTP (E-Mail). TLS ist die jüngste Version von SSL. Die Bezeichnung SSL wird allgemein immer noch gleichbedeutend mit TLS verwendet. SSL und SSH unterscheiden sich vor allem im Hinblick auf die in die beiden Protokolle integrierten Clientund Server-Authentifizierungsverfahren. TLS wurde zudem als IETF-Norm (Internet Engineering Task Force) akzeptiert, während SSH niemals zu einer voll anerkannten IETF-

Norm wurde, obwohl es als Entwurfsnorm sehr weite Verbreitung fand. SSL ist das sichere Protokoll, das HTTP-Webverkehr schützt, und wird auch als HTTPS für „http secure“ bezeichnet. Sowohl Netscape als auch Internet Explorer unterstützen SSL und TLS. Wenn diese Protokolle verwendet werden, erfolgt eine formelle Authentifizierungs des Servers gegenüber dem Client in Form eines Serverzertifikats. Zertifikate werden im Folgenden beschrieben. Der Client kann auch mit Zertifikaten authentifiziert werden, obwohl normalerweise Benutzernamen und Kennwörter verwendet werden. Da sämtliche SSL-Sitzungen verschlüsselt sind, sind die Authentifizierungsinformationen und alle Daten auf Websites sicher. SSL wird stets auf Websites verwendet, die für Bankgeschäfte und andere kommerzielle Zwecke gesichert sein müssen, da die Clients üblicherweise über das öffentliche Internet auf diese Websites zugreifen.

Da sich die webbasierte Verwaltung von Netzwerkgeräten (eingebundene Webserver) als Methode für die grundlegende Konfiguration und den Benutzerzugriff durchgesetzt hat, wird der Schutz dieser Verwaltungsmethode sehr wichtig. Unternehmen, welche die gesamte Netzwerkverwaltung sicher abwickeln, aber dennoch die Vorteile graphischer Benutzeroberflächen wie HTTP nutzen möchten, sollten SSL-basierte Systeme verwenden. Wie bereits oben erwähnt, kann SSL auch Datenübertragungen schützen, die nicht mit HTTP arbeiten. Wenn Geräteclients ohne HTTP verwendet werden, sollte auf diesen Systemen auch SSL für die Zugriffsprotokolle eingesetzt werden, um Sicherheit zu gewährleisten. SSL bietet in all diesen Fällen außerdem den Vorteil, dass Standardprotokolle mit den üblichen Authentifizierungs- und Verschlüsselungsschemata verwendet werden können.

Empfohlene Vorgehensweisen für die Netzwerksicherheit
Durch ausgeklügelte Sicherheitsrichtlinien lässt sich die Sicherheit eines Netzwerks deutlich erhöhen. Richtlinien können sowohl kompliziert und schwerfällig als auch einfach und unkompliziert sein; häufig erweisen sich einfache Konzepte als besonders hilfreich. Betrachten Sie die Kombination eines zentral verwalteten Systems für die Virenschutzaktualisierung und einen Hostscanner, mit dem neue oder veraltete Systeme entdeckt werden. Ein solches System enthielte zwar Setupfunktionen und böte Möglichkeiten zur zentralen Verwaltung und Softwarebereitstellung, diese Fähigkeiten sind im Allgemeinen jedoch bereits in modernen Betriebssystemen enthalten. Generell lassen sich offensichtliche Lücken in der Systemsicherheit mit Richtlinien und im Idealfall mit Tools für deren automatische Erzwingung schließen, sodass komplexere Fragen in den Mittelpunkt rücken können. Die folgenden Aspekte gehören normalerweise zu den Richtlinien für die Netzwerksicherheit eines Unternehmens:

- Firewalls an allen Übergängen vom öffentlichen in das private Netzwerk
- Versionsgesteuerte und zentral bereitgestellte Firewallregeln
- Auslagerung externer Ressourcen in Netzwerke, die durch zwei Firewalls und DMZ geschützt sind
- Auf allen Netzwerkhosts werden nicht benötigte Netzwerkanschlusse sowie nicht benötigte Dienste deaktiviert.
- Alle Netzwerkhosts verfügen über eine zentral verwaltete Virenschutzsoftware.
- Sicherheitsupdates für alle Netzwerkhosts werden zentral verwaltet.
- Sichere zentrale Authentifizierung wie RADIUS, Windows / Kerberos / Active Directory
- Zentrale Benutzerverwaltung mit Kennwortrichtlinie (Änderung alle drei Monate und Verwendung „sicherer Kennwörter“)
- Vorausschauendes Durchsuchen des Netzwerks nach neuen Hosts und veralteten Systemen
- Überwachung des Netzwerks auf verdächtige Verhaltensweisen
- Mechanismen zum Reagieren auf Ereignisse (Richtlinien, manuell, automatisch usw.)

In der obigen Liste sind die wichtigsten Elemente angegeben, die in einer Richtlinie enthalten sein müssen. Möglicherweise können Richtlinien noch andere einflussreiche Elemente

enthalten. Beim Festlegen von Typ und Reichweite einer Richtlinie kommt es natürlich stets darauf an, Faktoren wie Unternehmensgröße, Risikoanalyse, Kosten und Auswirkungen auf das Geschäft gegeneinander abzuwägen. Ein guter Ausgangspunkt ist in der Regel, wie oben erwähnt, eine Systemanalyse, an die sich eine Unternehmensanalyse anschließen sollte. Auch wenn es auf den ersten Blick nicht sinnvoll zu sein scheint, sollten doch auch sehr kleine Unternehmen Sicherheitsrichtlinien festlegen, da alle Netzwerke unabhängig von ihrer Größe Ziel von Angriffen sein können.

Ergebnisse

Angesichts der zunehmenden Anzahl von Netzwerkbedrohungen durch Würmer, Viren und intelligente Hacker können Sicherheitsmaßnahmen auch in „privaten“ Netzwerken nicht mehr lediglich als Option betrachtet werden. Die Sicherung sämtlicher Geräte, einschließlich der Geräte für die physische Infrastruktur wie USV- und HVAC-Systeme, ist für die Aufrechterhaltung des Betriebs und den reibungslosen Zugriff auf Dienste von entscheidender Bedeutung. Die Bereitstellung und Aufrechterhaltung der Sicherheit im gesamten Unternehmen bedeutet im Regelfall einen erhöhten Verwaltungsaufwand. Bisher war dies das größte Hindernis für umfassende Implementierungen von Sicherheitsmaßnahmen. Heute kann der zeitliche Aufwand für die Reparatur eines Netzwerks, das von nur einem Wurm oder Virus angegriffen wurde, ohne weiteres größer sein als die im voraus aufgewandte Zeit für eine bessere Sicherung eines Unternehmens. Glücklicherweise gibt es in Systemen und Softwareprogrammen zahlreiche Optionen zur Erhöhung der Netzwerksicherheit, die zugleich den Aufwand für die Verwaltung solcher Systeme senken. Selbst durch einfache Maßnahmen wie regelmäßige Softwareaktualisierungen, das Deaktivieren aller Geräte und die Verwendung von Verfahren für die zentrale Authentifizierung und einen sicheren Zugriff können Risiken deutlich reduziert werden. Durch die Einrichtung entsprechender Sicherheitsrichtlinien und häufige Netzwerkprüfungen lässt sich der Schutz des Netzwerks insgesamt weiter verbessern.