Grundprinzipien der Netzwerksicherheit - Teil 2: Sicherheitsaspekte

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.

Sperren von Anschlüssen und Minimieren aktiver Dienste

Auf vielen Netzwerkgeräten und Computerhosts werden Netzwerkdienste standardmäßig gestartet. Jeder dieser Dienste bietet Angriffsmöglichkeiten für Eindringlinge, Würmer und Trojaner. Häufig werden diese Standarddienste nicht benötigt. Wenn Sie diese Dienste ausschalten und damit bestimmte Anschlüsse sperren, wird dieses Risiko verringert. Wie bereits im Abschnitt über Firewalls erwähnt, kann auf Desktops und Servern eine einfache Firewallsoftware ausgeführt werden, die etwa die gleichen Funktionen wie eine Netzwerkfirewall erfüllt und den Zugriff auf nicht benötigte IP-Anschlüsse auf dem Host blockiert oder den Zugriff von bestimmten Hosts aus einschränkt. Diese Vorgehensweise ist für den internen Schutz wichtig, wenn die äußeren Verteidigungslinien verletzt wurden oder andere interne Bedrohungen abgewehrt werden sollen. Es gibt viele Desktop-Firewall-Softwarepakete, die sich sehr gut zum Schutz von Hosts eignen; Microsoft z. B. hat in Windows XP Service Pack 2 ebenfalls eine einfache Firewall integriert.

Verwaltung von Benutzernamen und Kennwörtern

Wie in der Einführung erwähnt, ist die Verwaltung von Benutzernamen und Kennwörtern in den meisten Unternehmensnetzwerken mangelhaft. Mithilfe ausgeklügelter, zentraler Authentifizierungssysteme (die später erörtert werden) lassen sich diese Probleme verringern. Es gibt jedoch auch grundlegende Richtlinien, die enorm hilfreich sein können, wenn sie beachtet werden. Bei Benutzernamen und Kennwörtern müssen die vier folgenden Grundregeln eingehalten werden:

1. Verwenden Sie keine naheliegenden Kennwörter wie den Namen des Ehegatten, die Lieblingsmannschaft usw.
2. Verwenden Sie längere Kennwörter mit Zahlen oder Symbolen.
3. Ändern Sie Kennwörter regelmäßig.
4. Verwenden Sie auf Netzwerkgeräten NIEMALS die Standardanmeldeinformationen.

Nur wenn auf den Computern oder Geräten Richtlinien aktiv sind, die die oben genannten Regeln durchsetzen, müssen diese Regeln nicht selbst erzwungen werden. Die Durchführung der vierten Regel kann mithilfe von Netzwerksonden überprüft werden, die versuchen, Geräte mit Standardanmeldeinformationen zu erkennen.

Zugriffssteuerungslisten

Für viele Arten von Geräten oder Hosts können Zugriffssteuerungslisten konfiguriert werden. In diesen Listen werden Hostnamen oder IP-Adressen angegeben, von denen aus auf das fragliche Gerät zugegriffen werden darf. Typischerweise wird z. B. der Zugriff auf Netzwerkgeräte aus dem Netzwerk einer Organisation heraus beschränkt. Dabei wird jede Art von Zugriff abgewehrt, durch den eine externe Firewall eventuell verletzt würde. Solche Zugriffssteuerungslisten dienen als wichtige letzte Verteidigungslinie und können auf manchen Geräten dank unterschiedlicher Regeln für verschiedene Zugriffsprotokolle sehr leistungsfähig sein.

Quelle: www.voltimum.de

Sichern des Zugriffs auf Geräte und Systeme
Da davon auszugehen ist, dass Datennetze nicht immer vor Eindringversuchen oder dem „Erschnüffeln“ von Daten geschützt sind, wurden Protokolle entwickelt, die die Sicherheit angeschlossener Netzwerkgeräte erhöhen. Im Allgemeinen gibt es zwei gesonderte Aspekte, die zu beachten sind: Authentifizierung und Geheimhaltung (Verschlüsselung). Bei gesicherten Systemen und Kommunikationswegen werden diese beiden Anforderungen durch verschiedene Schemata und Protokolle umgesetzt. Im Folgenden werden zunächst die Grundlagen der Authentifizierung und anschließend die der Verschlüsselung erläutert.

Benutzerauthentifizierung für Netzwerkgeräte
Die Authentifizierung ist erforderlich, wenn der Zugriff auf Netzwerkelemente gesteuert werden soll, insbesondere auf Geräte der Netzwerkinfrastruktur. Die Authentifizierung hat zwei Teilaspekte, die allgemeine Zugriffsauthentifizierung und die funktionale Autorisierung. Bei der allgemeinen Zugriffsauthentifizierung wird kontrolliert, ob ein bestimmter Benutzer ÜBERHAUPT ein Zugriffsrecht für das fragliche Element besitzt. Dies geschieht in der Regel über ein „Benutzerkonto“. Bei der Autorisierung geht es um einzelne „Benutzerrechte“. Über welche Möglichkeiten verfügt ein Benutzer beispielsweise, nachdem er authentifiziert wurde? Kann er das Gerät konfigurieren oder nur Daten anzeigen? Tabelle 2 gibt einen Überblick über die wichtigsten Authentifizierungsprotokolle, deren Eigenschaften und deren entsprechende Anwendungszwecke.

Protokoll	Funktionen	Verwendung in Protokollen
Benutzername / Kennwort	Klartext, gespeichertes Token	Telnet, HTTP
CHAP (Challenge Handshake Authentication Protocol)	Verwendet Zerstückelung von Kennwörtern und zeitlich variierende Daten, um eine direkte Kennwortübertragung zu vermeiden.	MS-CHAP, PPP, APC HTTP, Radius
RADIUS	CHAP oder direkte Kennwörter, Autorisierungs- und Kontoführungsverfahren	Back-End für Telnet, SSH, SSL, Front-End für Microsoft IAS Server. Typische zentrale Authentifizierungsmethode für Netzwerkgeräte
TACACS+	Authentifizierung, Autorisierung, Kontoführung, volle Verschlüsselungsunterstützung	Cisco-Protokoll, zentrale Authentifizierung, RAS (Remote Access Service)
Kerberos	Dienstauthentifizierung und -autorisierung, volle Verschlüsselung	Kerberos-Anwendungen wie Telnet, Microsoft Domänenauthentifizierungsdienst integriert in Active Directory

Die Einschränkung des Zugriffs auf Geräte ist einer der wichtigsten Aspekte bei der Sicherung von Netzwerken. Da Infrastrukturgeräte sowohl die Netzwerk- und damit auch die Datenverarbeitungsgeräte unterstützen, kann eine Gefährdung dieser Geräte potenziell zum Ausfall eines ganzen Netzwerks und dessen Ressourcen führen. Paradoxerweise geben sich viele IT-Abteilungen große Mühe, Server zu schützen, Firewalls einzurichten und Zugriffsmechanismen zu sichern, vernachlässigen jedoch nahezu völlig Sicherheitsmaßnahmen für einfache Geräte.

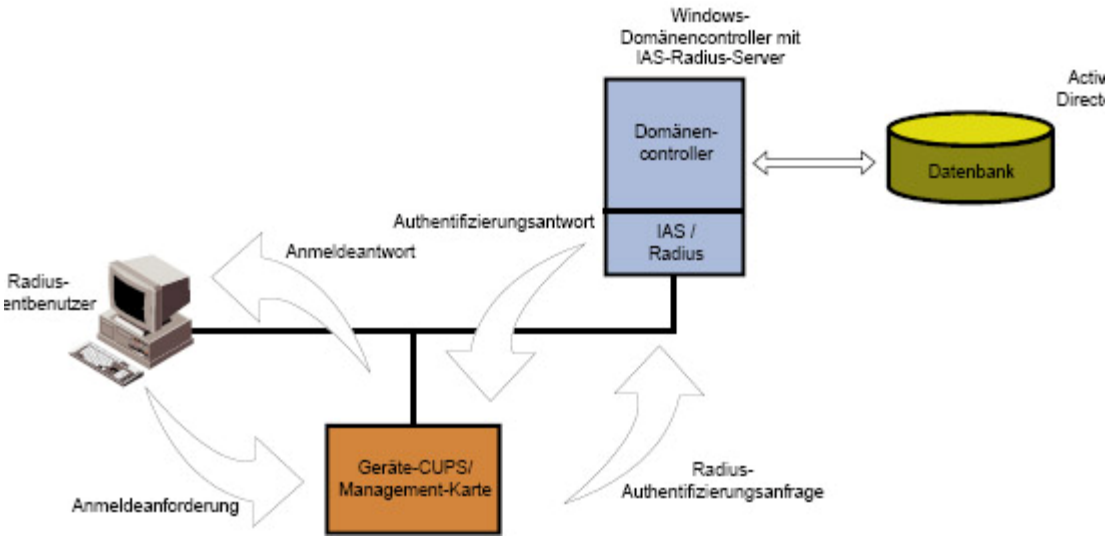
Alle Geräte sollten mindestens eine Benutzernamen- und Kennwortauthentifizierung mit

nichttrivialen Zeichen haben (10 Zeichen, alphanumerische Zeichen, Zahlen und Symbole gemischt). Die Anzahl der Benutzer sowie deren Autorisierungstyp sollte eingeschränkt werden. Bei Verwendung unsicherer Remotezugriffsmethoden (Benutzernamen und Kennwörter werden als Klartext über das Netzwerk übertragen) sollte vorsichtig vorgegangen werden. Kennwörter sollten zudem häufiger geändert werden, etwa alle drei Monate und bei Ausscheiden von Mitarbeitern, wenn Gruppenkennwörter verwendet werden.

Zentrale Authentifizierungsmethoden

Geeignete Authentifizierungsmethoden sind eine Mindestanforderung; wenn a) die Gerätebenutzer zahlreich sind oder b) das Netzwerk viele Geräte enthält, sind zentrale Authentifizierungsmethoden jedoch noch besser. Üblicherweise wurden Probleme im Fall a) durch eine zentrale Authentifizierung gelöst; die gängigste Methode war der Remotenetzwerkzugriff. Bei Remotezugriffssystemen wie DFÜ-RAS konnten die Benutzer in den RAS-Netzwerkeinheiten selbst allerdings einfach nicht verwaltet werden. Potenziell konnte jeder Netzwerkbenutzer versuchen, einen der vorhandenen RAS-Zugriffspunkte zu verwenden. Das Ablegen aller Benutzerinformationen in allen RAS-Einheiten und das anschließende Aktualisieren dieser Informationen würde die Fähigkeiten von RAS-Einheiten in jedem großen Unternehmen überschrei-ten und wäre eine administrative Katastrophe. Bei zentralen Authentifizierungssystemen wie RADIUS und Kerberos lässt sich dieses Problem mithilfe zentraler Benutzerkonteninformationen lösen, auf die die RAS-Einheiten oder andere Arten von Geräten sicher zugreifen können. Die zentralen Schemata ermöglichen das Speichern von Informationen an einer statt an vielen Stellen. Die Benutzer müssen nicht mehr auf vielen Geräten verwaltet werden, sondern es kann ein Benutzerverwaltungsstandort verwendet werden. Änderungen von Benutzerinformationen, etwa die Eingabe eines neuen Kennworts, sind einfach. Wenn ein Benutzer das Unternehmen verlässt, wird durch das Löschen des Benutzerkontos mithilfe der zentralen Authentifizierung der Zugriff auf sämtliche Geräte blockiert. Ein typisches Problem bei der dezentralen Authentifizierung in größeren Netzwerken ist es, alle Stellen zu erfassen, an denen Konten zu löschen sind. Zentrale Authentifizierungssysteme wie RADIUS lassen sich in der Regel nahtlos in andere Benutzerkontenverwaltungs-schemata wie Microsoft Active Directory oder LDAP-Verzeichnisse integrieren. Zwar sind diese beiden Verzeichnissysteme selbst keine Authentifizierungssysteme, sie fungieren jedoch als zentrale Kontenspeicher. Die meisten RADIUS-Server können über das normale RADIUS-Protokoll mit RAS- oder anderen Netzwerkgeräten kommunizieren und anschließend gesichert auf die in den Verzeichnissen gespeicherten Konteninformationen zugreifen. Dies entspricht genau der Funktionsweise des IAS-Servers von Microsoft, der auf diese Weise RADIUS und Active Directory verknüpft. Ein solcher Ansatz bedeutet nicht nur, dass den Benutzern von RAS und Geräten die zentrale Authentifizierung zur Verfügung steht, sondern auch, dass die Konteninformationen mit den Microsoft-Domänenkonten vereinigt werden. Abbildung 4 zeigt einen Windows-Domänencontroller, der sowohl als Active Directory-Server als auch als RADIUS-Server für Netzwerkelemente fungiert, die in einer Active Directory-Domäne authentifiziert werden müssen.

***Abbildung 4** – Windows-Domänencontroller*



Sichern von Netzwerkdaten durch Verschlüsselung und Authentifizierung In manchen Fällen muss die Offenlegung von Informationen verhindert werden, die zwischen Netzwerkelementen, Computern oder Systemen ausgetauscht werden. Es ist gewiss nicht wünschenswert, dass ein Benutzer Zugriff auf ein Bankkonto erhält, das ihm nicht gehört, oder dass er vertrauliche Informationen abfangen kann, die über ein Netzwerk übertragen werden. Wenn die Offenlegung von Daten über ein Netzwerk vermieden werden soll, müssen Verschlüsselungsmethoden verwendet werden, welche die übertragenen Daten für einen Benutzer unlesbar machen, der die Daten bei der Übertragung im Netzwerk auf irgendeine Weise erfasst. Es gibt zahlreiche Methoden zum „Verschlüsseln“ von Daten, und einige der wichtigsten Methoden werden hier beschrieben. Bei Netzwerkgeräten wie USV-Systemen müssen üblicherweise nicht Daten wie USV-Spannungen und Stromleistenströme geschützt werden; problematisch ist vielmehr die Steuerung des Zugriffs auf diese Elemente.

Die Geheimhaltung von Authentifizierungsinformationen wie Benutzernamen und Kennwörtern ist in allen Systemen, in denen der Zugriff über ungeschützte Netzwerke wie z. B. das Internet erfolgt, von entscheidender Bedeutung. Selbst innerhalb des privaten Netzwerks einer Organisation ist der Schutz von Anmeldeinformationen eine empfohlene Vorgehensweise. Nach und nach beginnen immer mehr Organisationen, Richtlinien zu implementieren, nach denen der GESAMTE Verwaltungsverkehr verschlüsselt wird, nicht nur die Authentifizierungsinformationen. In beiden Fällen müssen bestimmte kryptographische Verfahren verwendet werden.

Die Daten werden in der Regel verschlüsselt, indem Klartextdaten (die Eingabe) unter Verwendung eines bestimmten Verschlüsselungsalgorithmus mit einem geheimen Schlüssel kombiniert wird (z. B. 3DES, AES usw.). Das Ergebnis (die Ausgabe) ist verschlüsselter Text. Nur wenn ein Benutzer (oder ein Computer) über den geheimen Schlüssel verfügt, kann der verschlüsselte Text in Klartext umgewandelt werden. Dieses Verfahren ist Hauptbestandteil aller sicheren Protokolle (Beschreibung weiter unten). Ein weiteres Element kryptographischer Systeme ist der „Hash“ (die Zerstückelung). Bei Zerstückelungsmethoden wird auf Grundlage von Klartexteingaben und eventuell Schlüsseleingaben eine große Zahl berechnet, eine sogenannte Hashzahl. Diese Zahl hat unabhängig von der Größe der Eingabe eine feste Länge (feste Anzahl von Bits). Während Verschlüsselungsmethoden umkehrbar sind, da der Klartext mithilfe des Schlüssels wiederhergestellt werden kann, ist dies bei Zerstückelung nicht möglich. Es ist mathematisch nicht möglich, aus Hashdaten den Klartext wiederherzustellen. Zerstückelungen werden in verschiedenen Protokollsystemen als spezielle IDs verwendet, da die Daten einer gespeicherten Datei zur Erkennung von Datenänderungen ähnlich wie bei einer CRC (Cyclic Redundancy Check, zyklische Redundanzprüfung) überprüft werden. Die Zerstückelung wird als

Quelle: www.voltimum.de

Datenauthentifizierungsmethode (nicht identisch mit Benutzerauthentifizierung) verwendet. Benutzer, die Daten bei der Übertragung über das Netzwerk unentdeckt zu ändern versuchen, ändern die Zerstückelungswerte und bewirken damit, dass sie entdeckt und erkannt werden. Tabelle 3 gibt einen Überblick über kryptographische Algorithmen und deren Verwendung.

Algorithmus	**Primäre Verwendung**	**Algorithmus Primäre Verwendung Verwendung in Protokollen**
DES	Verschlüsselung	SSH, SNMPv3, SSL / TLS
3DES	Verschlüsselung	SSH, SNMPv3, SSL / TLS
RC4	Verschlüsselung	SSL / TLS
Blowfish	Verschlüsselung	SSH
AES	Verschlüsselung	SSH, SSL / TLS
MD5	Zerstückelung, Nachrichtenauthentifizierungscodes	SSH, SNMPv3, SSL / TLS
SHA	Zerstückelung, Nachrichtenauthentifizierungscodes	SSH, SNMPv3, SSL / TLS