

Grundprinzipien der Netzwerksicherheit

Von Christopher Leidigh

**White paper /
technische
Dokumentation
Nr. 101**

APC[®]
Legendary Reliability[®]

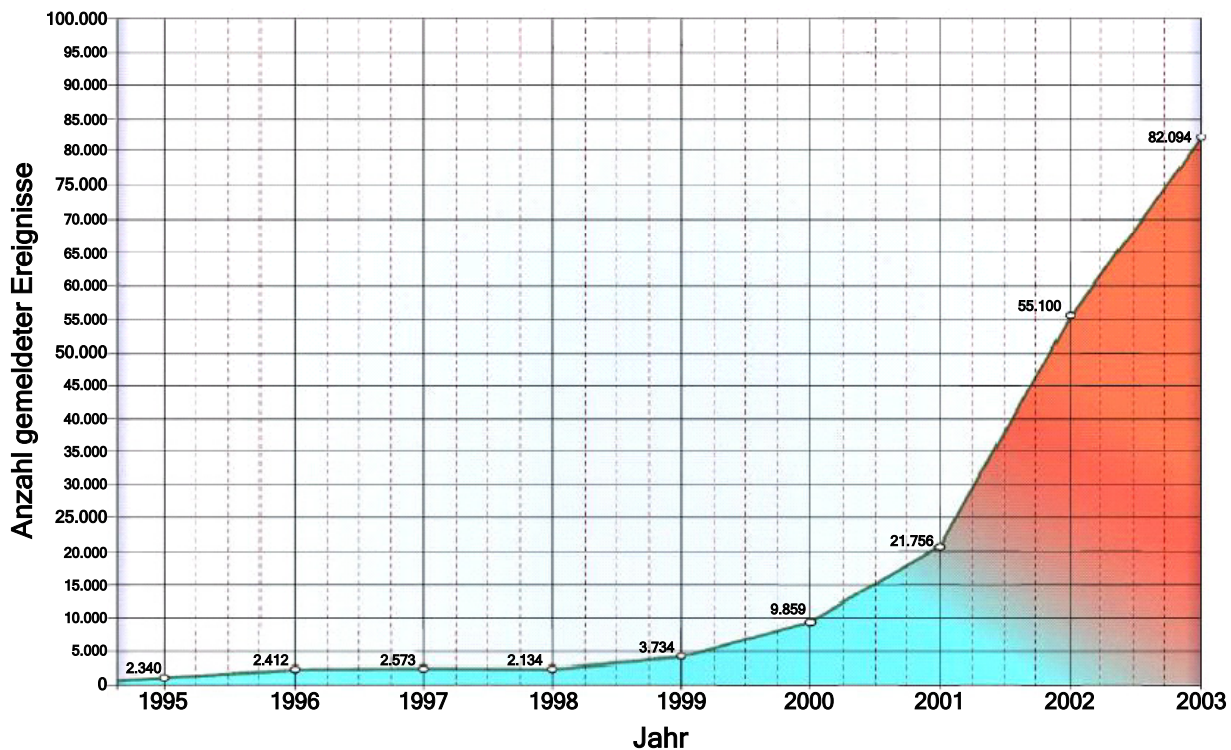
Zusammenfassung

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 Datacentern, Netzwerkadministratoren und andere Datacenterfachleute müssen die Grundlagen von Sicherheitsmaßnahmen kennen, um Netzwerke heute sicher einrichten und verwalten zu können. In diesem Papier 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.

Einführung

Die Sicherung moderner Unternehmensnetze und IT-Infrastrukturen verlangt allumfassende Maßnahmen und eine sichere Kenntnis von Sicherheitslücken und entsprechenden Schutzmaßnahmen. Mit diesen Kenntnissen lassen sich zwar nicht alle Versuche vereiteln, in Netzwerke einzudringen und Systeme anzugreifen. Netzwerktechniker sind damit jedoch in der Lage, allgemeine Probleme zu beseitigen, potenzielle Beschädigungen deutlich zu reduzieren und Sicherheitslücken schnell zu entdecken. Angesichts der stetig zunehmenden Anzahl und Komplexität der Angriffe dürfen Sicherheitsfragen sowohl in großen als auch in kleinen Unternehmen keinesfalls vernachlässigt werden. **Abbildung 1** zeigt den steilen jährlichen Anstieg von Sicherheitsereignissen, die dem CERT® Coordination Center (einem Zentrum für Internetsicherheit) gemeldet werden.

Abbildung 1 – Sicherheitsereignisse nach Jahr – CERT.ORG



© 1998-2003 Carnegie Mellon University

In diesem Papier werden Sicherheitsgrundlagen sowie einige empfohlene Vorgehensweisen für das Netzwerk, die Computerhosts und Elemente der Netzwerkinfrastruktur dargestellt. Da es für die Sicherheit kein „Allheilmittel“ gibt, muss der Leser / Umsetzer geeignete Maßnahmen selbst auswählen und abwägen.

Das menschliche Problem

Der menschliche Faktor ist in jedem Sicherheitsschema sicherlich das schwächste Glied. Die meisten Benutzer gehen mit Informationen wie Kennwörtern und Zugriffs-codes, auf denen die meisten sicheren Systeme beruhen, sehr sorglos um. In allen Sicherheitssystemen gibt es eine Reihe von Maßnahmen zur Steuerung des Zugriffs, zur Überprüfung der Identität und zur Verhinderung der Offenlegung sensibler Informationen. Zu diesen Maßnahmen gehören in der Regel verschiedene „Geheimnisse“. Wenn ein Geheimnis aufgedeckt oder gestohlen wird, können die damit geschützten Systeme gefährdet werden. Der Hinweis mag banal erscheinen, aber die meisten Systeme werden durch sehr einfache Dinge gefährdet. Es mag dumm sein, einen Zettel mit dem Systemkennwort am Bildschirm anzubringen, viele Benutzer tun dies jedoch. Kaum weniger gedankenlos ist die Tendenz, werkseitig vorgegebene Kennwörter für bestimmte Netzwerkgeräte nicht zu ändern. Ein solches Gerät könnte z. B. eine Netzwerkverwaltungsschnittstelle für eine USV sein. USV-Systeme gleichgültig welcher Kapazität werden in einem Sicherheitsschema häufig übersehen. Wenn auf solchen Geräten der vorgegebene Benutzername und das Standardkennwort erhalten bleiben, ist es eventuell nur eine Frage der Zeit, bis ein Angreifer, der lediglich den Gerätetyp und die dokumentierten Standardanmeldeinformationen kennt, Zugriff auf das Gerät erlangt. Stellen Sie sich eine Serverbank mit absolut zuverlässigen Sicherheitsprotokollen auf jedem Web- und E-Mail-Server vor, die aufgrund eines einfachen Ein-Ausschaltvorgangs einer ungeschützten USV abstürzt!

Sicherheit – das Gesamtbild

Wirksame Sicherheitsmaßnahmen in großen wie kleinen Unternehmen müssen umfassend sein. Die meisten Organisationen haben allerdings keine entsprechenden Richtlinien und Verfahren. Dafür gibt es einige gute Gründe: Sicherheit verursacht natürlich auch Kosten. Diese Kosten lassen sich nicht nur in Geld, sondern auch in Komplexität, Zeit und Effizienz messen. Um Sicherheit zu gewährleisten, ist es notwendig, Geld auszugeben, weitere Maßnahmen durchzuführen und zu warten, bis diese Maßnahmen abgeschlossen sind (eventuell müssen auch Dritte einbezogen werden).

In der Praxis sind echte Sicherheitsprogramme schwierig umzusetzen. Normalerweise muss ein Schema ausgewählt werden, das gewisse „Kosten“ verursacht und eine überschaubare Sicherheitsgarantie bietet. (Ein solches Konzept ist kaum als „umfassend“ zu bezeichnen.) Wichtig ist, zu jedem Aspekt eines Gesamtsystems sachlich begründete Entscheidungen zu treffen und mehr oder weniger Mittel bewusst und kalkuliert einzusetzen. Wenn man die weniger geschützten Bereiche kennt, können diese Bereiche wenigstens überwacht werden, um Probleme oder Sicherheitslücken zu entdecken.

Grundlagen der Sicherheit

Kenntnis des Netzwerks

Es ist nicht möglich, etwas zu schützen, wenn man nicht genau weiß, WAS geschützt werden soll. Organisationen jeder Größe müssen ihre Ressourcen und Systeme dokumentieren. Allen Elementen muss ein relativer Wert zugewiesen werden, aus dem die Bedeutung der Elemente für die Organisation hervorgeht. Die gilt z. B. für Server, Workstations, Speichersysteme, Router, Switches, Hubs, Netzwerk- und Telekommunikationsverbindungen und weitere Netzwerkelemente wie Drucker, USV-Systeme und HVAC (Heating, Ventilation and Airconditioning)-Systeme. Wichtig ist zudem die Dokumentierung des Gerätestandorts sowie Hinweise auf Abhängigkeiten. Die meisten Computer sind z. B. auf eine Notstromversorgung (USV) angewiesen, die wiederum Teil des Netzwerks sein kann, wenn sie verwaltet wird. Klimageräte wie HVAC-Geräte und Luftreiniger gehören eventuell ebenfalls hierzu.

Kenntnis unterschiedlicher Bedrohungen

Im nächsten Schritt werden, wie in **Tabelle 1** dargestellt, die potenziellen „Bedrohungen“ all dieser Elemente ermittelt. Die Bedrohungen können sowohl aus internen als auch aus externen Quellen stammen. Es kann sich um menschliches Versagen, automatische Ereignisse oder nicht beabsichtigte natürliche Ereignisse handeln. Letztere könnten eigentlich eher unter die Kategorie Bedrohung der Systemintegrität als unter Sicherheitsbedrohung subsumiert werden, jedoch kann ein Problem ein anderes nach sich ziehen. Ein Beispiel dafür ist ein Stromausfall infolge eines Einbrecheralarms. Der Stromausfall könnte willentlich oder durch ein natürliches Ereignis wie einen Blitzschlag herbeigeführt worden sein. In beiden Fällen ist die Sicherheit beeinträchtigt.

Tabelle 1 – Überblick über verschiedene Bedrohungen und deren Konsequenzen

Bedrohung	Intern \ Extern	Konsequenzen der Bedrohung
E-Mail mit Virus	Externe Herkunft, interne Verwendung	Kann System infizieren, auf dem die E-Mail gelesen wird, und sich danach in der ganzen Organisation ausbreiten.
Netzwerkvirus	Extern	Kann über ungeschützte Anschlüsse eindringen und das gesamte Netzwerk gefährden.
Webbasierter Virus	Interner Aufruf einer externen Website im Browser	Kann Systemsicherheit während des Browsens gefährden und danach andere interne Systeme beeinträchtigen.
Webserverangriff	Außerhalb von Webservern	Wenn die Sicherheit des Webserver beeinträchtigt ist, können Hacker Zugriff auf andere interne Systeme des Netzwerks erlangen.

Bedrohung	Intern \ Extern	Konsequenzen der Bedrohung
Dienstverweigerungsangriff	Extern	Externe Dienste wie Web, E-Mail und FTP können unter Umständen nicht mehr verwendet werden. Wird ein Router angegriffen, kann das gesamte Netzwerk ausfallen.
Angriff durch Netzwerkbenutzer (interner Mitarbeiter)	Generell intern	Herkömmliche Firewalls an der Netzwerkgrenze sind bei solchen Angriffen wirkungslos. Interne Segmentierungsfirewalls können Schaden eindämmen.

Physische Sicherheit, interner Schutz

Die meisten Experten würden zustimmen, dass Sicherheit stets mit der physischen Sicherheit beginnt. Die Steuerung des physischen Zugriffs auf Rechner und Netzwerkknotenpunkte ist vermutlich wichtiger als alle anderen Sicherheitsaspekte. Durch jede Art physischen Zugriffs auf einen internen Standort wird dieser einem größeren Risiko ausgesetzt. Wenn der physische Zugriff möglich ist, können in der Regel auch sichere Daten, Kennwörter, Zertifikate und alle anderen Daten abgerufen werden. Glücklicherweise gibt es alle möglichen Arten von Zugriffssteuerungsgeräten und sicheren Schränken, mit denen sich dieses Problem lösen lässt. Weitere Informationen über die physische Sicherheit von Datacentern und Netzwerkräumen finden Sie im APC White paper Nr. 82, „Physische Sicherheit in betriebskritischen Gebäuden“.

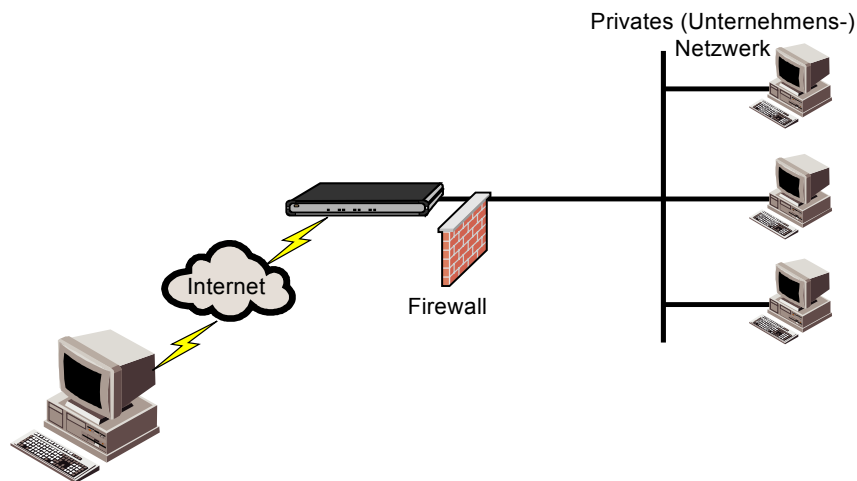
Partitionieren des Netzwerks und Schützen der Netzwerkgrenzen durch Firewalls

Neben der grundlegenden physischen Sicherheit eines Standorts ist die Kontrolle des digitalen Zugriffs auf das Netzwerk der Organisation und aus dem Netzwerk heraus der nächste wichtige Aspekt. In den meisten Fällen müssen dazu die Verbindungen mit der externen Welt, also im Regelfall mit dem Internet überwacht werden. Fast jedes mittlere und große Unternehmen verfügt über einen Internetauftritt, mit dem das Netzwerk der Organisation verbunden ist. Auch kleinere Unternehmen und private Anwender besitzen in zunehmendem Maß eine permanente Internetanbindung. Die Abtrennung des externen Internets und des internen Intranets ist ein entscheidendes Element des Sicherheitskonzepts. Gelegentlich wird die interne Seite als „vertrauenswürdig“ und das externe Internet als „nicht vertrauenswürdig“ bezeichnet. Das ist zwar grundsätzlich richtig, allerdings noch nicht genau genug, wie im Folgenden zu zeigen sein wird.

Eine Firewall ist eine überwachte Barriere, mit welcher der Netzwerkverkehr in das Intranet UND aus dem Intranet einer Organisation gesteuert wird. Firewalls sind im Wesentlichen anwendungsspezifische Router. Es kann sich dabei um spezielle eingebundene Systeme, z. B. Internetgeräte, oder um Softwareprogramme handeln, die auf einer allgemeinen Serverplattform ausgeführt werden. Normalerweise haben diese Systeme zwei Netzwerkschnittstellen, eine für das externe Netzwerk – das Internet – und eine für das interne Intranet. Mit einer Firewall lässt sich genau kontrollieren, welche Daten von einer Seite zur anderen übertragen werden dürfen. Firewalls können sehr einfach oder sehr komplex sein. Wie bei den meisten Sicherheitsaspekten richtet sich die Festlegung des zu verwendenden Firewalltyps nach Faktoren wie Datenverkehrsvolumen, schutzbedürftige Dienste und die Komplexität der erforderlichen Regeln. Je größer die Anzahl der Dienste, die die Firewall passieren müssen, desto komplexer werden die Anforderungen. Die Unterscheidung zwischen legitimem und illegitimem Datenverkehr ist bei Firewalls nicht ganz einfach.

Wovor schützen Firewalls, und welchen Schutz bieten sie nicht? Für Firewalls gilt, was auch für viele andere Dinge gilt: Wenn sie richtig konfiguriert sind, können sie ein sinnvoller Schutz vor externen Bedrohungen einschließlich bestimmter Dienstverweigerungsangriffe sein. Sind sie fehlerhaft konfiguriert, stellen sie in einer Organisation unter Umständen größere Sicherheitslücken dar. Der grundlegendste Schutz, den eine Firewall bietet, ist die Blockierung von Netzwerkverkehr zu bestimmten Zielen. Dies gilt sowohl für IP-Adressen als auch für spezielle Netzwerkdienstanschlüsse. Soll für eine Site der externe Zugriff auf einen Webserver möglich sein, kann der gesamte Datenverkehr auf Anschluss 80 beschränkt werden (den standardmäßigen HTTP-Anschluss). In der Regel wird diese Einschränkung nur auf Datenverkehr nicht vertrauenswürdiger Herkunft angewandt. Datenverkehr vertrauenswürdiger Herkunft wird nicht eingeschränkt. Der gesamte übrige Datenverkehr wie E-Mails, FTP, SNMP usw. wird von der Firewall nicht ins Intranet durchgelassen. Ein Beispiel für eine einfache Firewall sehen Sie in **Abbildung 2**.

Abbildung 2 – Einfache Firewall für ein Netzwerk

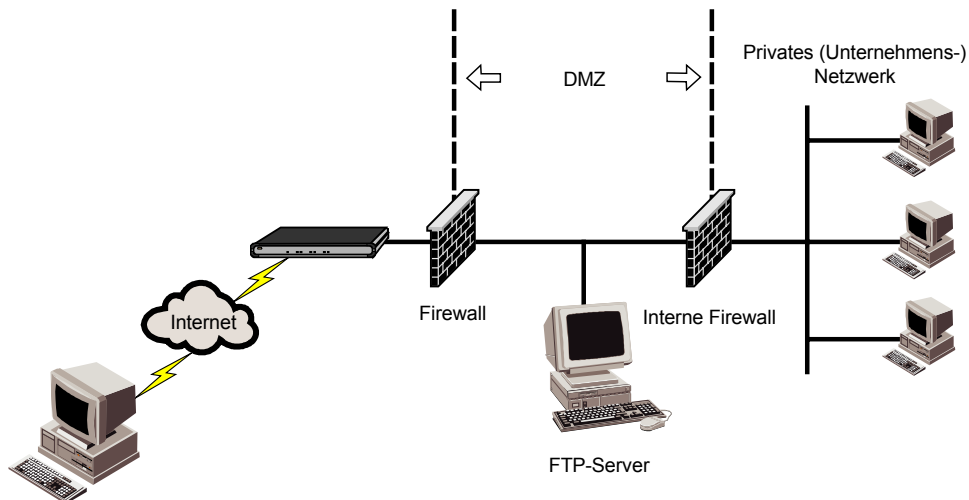


Noch einfacher sind Firewalls, die häufig von Benutzern in Heimbüros oder kleinen Unternehmen mit Kabel- oder DSL-Routern verwendet werden. Diese Firewalls sind normalerweise so eingerichtet, dass der GESAMTE externe Zugriff eingeschränkt ist und nur Dienste des internen Systems zugelassen sind. Ein aufmerksamer Leser hat vielleicht bemerkt, dass eine Firewall in keinem dieser Fälle tatsächlich den gesamten Verkehr von außen abblockt. Wäre das wirklich der Fall, wie wäre es dann möglich, im Web zu surfen und Websites aufzurufen? Was die Firewall tatsächlich bewirkt, ist die Einschränkung von Verbindungsanforderungen, die von außen kommen. Im ersten Fall werden alle Verbindungsanforderungen aus dem internen Netz sowie die gesamte folgende Datenübertragung über diese Verbindung an das externe Netz weitergeleitet. Von außen wird nur eine Verbindungsanforderung für den Webserver zugelassen, um Daten zu vervollständigen und weiterzugeben, alle übrigen Anforderungen werden abgeblockt. Im zweiten Fall ist die Vorgehensweise rigoroser, da Verbindungen nur von innen nach außen aufgebaut werden können.

Bei komplexeren Firewallregeln werden so genannte „statusbehaftete Prüfverfahren“ eingesetzt. Dabei wird die einfache Anschlussblockierung um die Prüfung von Verhaltensweisen und Sequenzen im Datenverkehr erweitert, um Angriffe mit vorgetäuschter Identität und Dienstverweigerungsangriffe zu erkennen. Je komplexer die Regeln, desto größer ist die erforderliche Rechenleistung der Firewall.

Ein Problem für die meisten Organisationen ist es, legitime Zugriffe auf „öffentliche“ Dienste wie Web, FTP und E-Mail zuzulassen und gleichzeitig die Integrität des Intranets zu sichern. In der Regel wird dazu eine so genannte demilitarisierte Zone (DMZ) erstellt; dieser aus dem kalten Krieg stammende Euphemismus wurde auf Netzwerke angewandt. In dieser Architektur gibt es zwei Firewalls: eine zwischen dem externen Netzwerk und der DMZ sowie eine weitere zwischen der DMZ und dem internen Netzwerk. Alle öffentlichen Server befinden sich in der DMZ. Bei einer solchen Konfiguration können Firewallregeln festgelegt werden, die den öffentlichen Zugriff auf die öffentlichen Server gestatten, während die innere Firewall alle eingehenden Verbindungen beschränkt. Durch die DMZ sind die öffentlichen Server dennoch besser geschützt, als wenn sie sich außerhalb einer Site mit einfacher Firewall befänden. **Abbildung 3** zeigt die Verwendung einer DMZ.

Abbildung 3 – Doppelte Firewalls mit DMZ



Durch die Verwendung interner Firewalls an verschiedenen Intranetgrenzen lassen sich außerdem Schädigungen durch interne Bedrohungen und Objekte wie Würmer eindämmen, denen es gelang, die äußeren Firewalls zu überwinden. Interne Firewalls können auch im Bereitschaftsmodus ausgeführt werden. Der normale Datenverkehr wird auf diese Weise nicht blockiert, bei Auftreten eines Problems werden jedoch strenge Regeln aktiviert.

Workstation-Firewalls

Es gibt einen wichtigen Faktor für die Netzwerksicherheit, der den meisten Benutzern erst jetzt bewusst wird: die Tatsache, dass ALLE Knoten oder Workstations in einem Netzwerk potenzielle Sicherheitslücken darstellen. In der Vergangenheit wurden hauptsächlich Firewalls und Server beachtet. Mit dem Aufkommen

des Webs und dem Entstehen immer neuer Klassen von Knoten wie z. B. Internetgeräten sind beim Schutz des Netzwerks einige zusätzliche Aspekte zu beachten. Zahlreiche Wurmprogramme erobern Computer und benutzen sie, sowohl um sich selbst zu verbreiten als auch um gelegentlich Systeme zu schädigen. Viele dieser Würmer könnten gestoppt oder stark behindert werden, wenn die internen Systeme der Organisationen besser gesichert wären. Firewalls für Workstations können sämtliche Zugriffe auf einzelne Hosts und aus einzelnen Hosts heraus blockieren, die nicht der normalen Funktion der einzelnen Hosts entsprechen. Zusätzlich können Firewallregeln auf der INTERNEN Seite, die verdächtige ausgehende Verbindungen aus der Organisation blockieren, verhindern, dass sich die Würmer wieder aus einer Organisation heraus verbreiten. Die interne und externe Replikation auf beiden Seiten kann reduziert werden. Grundsätzlich sollten alle Systeme in der Lage sein, alle Anschlüsse zu blockieren, die nicht benötigt werden.

Grundlegende Sicherheit für Netzwerkhosts

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 Liebingsmannschaft 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.

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.

Tabelle 2 – Überblick über die wichtigsten Authentifizierungsprotokolle

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

Protokoll	Funktionen	Verwendung in Protokollen
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. Paradoxe Weise 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.

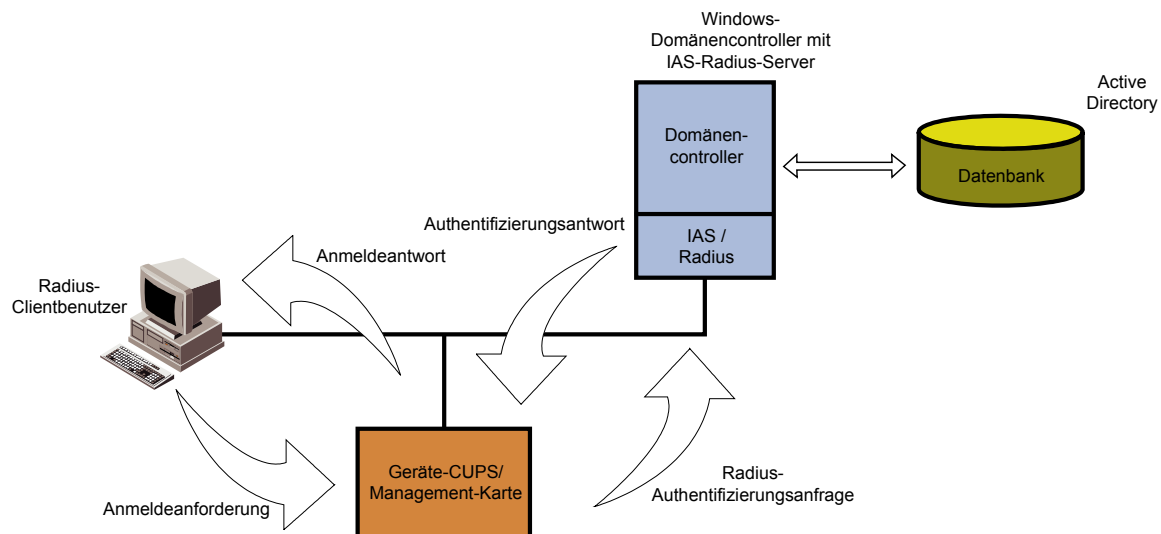
Zentrale Authentifizierungsmethoden

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 überschreiten 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 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.

Tabelle 3 – Überblick über die wichtigsten kryptographischen Algorithmen

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

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 Client- und 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 Authentifizierung 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 Netzwerkanschlüsse 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.

Über den Autor:

Christopher Leidigh ist Director of Communications and Technology Research bei APC in Rhode Island, USA. Er hat 18 Jahre Erfahrung im Programmieren und Entwerfen von Computer- und Mikroprozessorsystemen. Zurzeit befasst er sich vor allem mit der Erforschung und Entwicklung von Kommunikationssystemen, IP-Netzwerken, Sicherheit und eingebundenen Systemen. Seit zehn Jahren leitet er bei APC die Produktlinie für eingebundene Netzwerke und Verwaltung. An der Brown University hat er einen Bachelor-Abschluss in bioelektrischer Verfahrenstechnik gemacht. Er hält regelmäßig Vorträge auf den Embedded Systems Conferences in den USA und im Ausland sowie als Mitglied des Beirats. Seine Veröffentlichungen erscheinen in Journal of Physiology, Communications Systems Design, Embedded Systems Programming und EE Times.