



## Fortified SSH: Ein kostengünstiger Weg zum Schutz Ihres Netzwerks

### INHALT

Zwei Versionen von SSH .....	1
SSH-Funktionen .....	2
SSH-Schutzmaßnahmen .....	3
Wann bietet SSH keinen Schutz? .....	4
Fünf Fallstudien aus der Praxis .....	5
Abwägung der Kosten für SSH .....	7
Vergleich der Optionen .....	7
Die Wahl der richtigen Sicherheitslösung .....	8
Von der UNIX-Administration zur Protokollsuite für umfassende Sicherheitsbelange .....	9

# Fortified SSH: Ein kostengünstiger Weg zum Schutz Ihres Netzwerks

Die Gefahren für Unternehmenssysteme und -daten nehmen weiterhin in alarmierendem Tempo zu. Für Hacker ist es nach wie vor recht einfach, in die Netzwerke von Unternehmen oder Behörden einzudringen und irreversiblen Schaden anzurichten. Die Risiken beschränken sich nicht auf die Offenlegung von Daten. Auch Datenintegrität, Datenzugriff und Datenauthentifizierung sind gefährdet.

Eines der führenden Produkte im Kampf um die Datensicherheit ist eine kleine, robuste, leicht konfigurierbare Softwarelösung namens Secure Shell oder SSH. SSH ist eine Gruppe von Hilfsprogrammen, die auf dem SSH-Protokoll basiert. Hauptzweck von SSH ist die sichere Datenübertragung über Netzwerkverbindungen mit Hilfe leistungsstarker Verschlüsselungs- und Authentifizierungsmethoden. SSH ist ein Ersatz für ungesicherte Lösungen wie Telnet und FTP sowie für X11 und Berkeley r-Befehle (rlogin, rcp und rsh), die Daten unverschlüsselt übermitteln.

Aktuellen Schätzungen zufolge, hat die SSH-Lösung in ihren zahlreichen Anwendungsmöglichkeiten über zwei Millionen Benutzer in mehr als 80 Ländern. Mehr und mehr Unternehmen entscheiden sich für SSH, und zwar aus folgenden Gründen:

- SSH bietet ein sicheres Client/Server-Protokoll, das Daten während der Übertragung über ein Netzwerk verschlüsselt.
- SSH bietet leistungsstarke Authentifizierungsmethoden, die die Kommunikation von Client und Server mit zuverlässigen Hosts gewährleisten.
- SSH verhindert den für unsichere Netzwerkanwendungen wie Telnet und FTP charakteristischen Root-Zugriff.
- SSH ist transparent für die Endbenutzer.
- Die gewerblichen Versionen von SSH umfassen technischen Support auf hohem Niveau, Wartung und Problembehandlung bei Schwachstellen der Plattform. (Kostenlose, nicht gewerbliche Anwendungen von SSH bieten nicht das gleiche Support-Niveau wie die gewerblichen Versionen.)

SSH ist zwar kein „Allheilmittel“ für sämtliche netzwerkbezogenen Sicherheitsprobleme, aber es schaltet die derzeit größten Sicherheitsgefahren aus. Dieses Whitepaper bietet einen ausführlichen Überblick über SSH, die Funktionen, die SSH so leistungsfähig machen, die Methoden von SSH zur Abwehr von Angriffen sowie über die Fälle, in denen SSH nicht helfen kann. Es enthält Fallstudien aus der

Praxis sowie einen Abschnitt, in dem die gewerblichen mit den nicht gewerblichen Versionen verglichen werden. Nach der Lektüre dieses Dokuments werden Sie verstehen, warum Unternehmen weltweit zu SSH wechseln.

## Zwei Versionen von SSH

SSH1 wurde 1995 von Tatu Ylönen entwickelt. Ihm ging es zunächst um die Sicherung aller gespeicherten oder auf dem Übertragungsweg befindlichen Daten (Kennwörter, E-Mails, Protokollschnittflächen usw.), da es relativ einfach war, diese abzufangen oder aus einem Netzwerk abzurufen.

Nachdem Ylönen an verschiedene Grenzen des Protokolls gestoßen war, ging er 1996 zur Entwicklung von SSH2 über. SSH1 und SSH2 basieren auf völlig unterschiedlichen Protokollen, die nicht miteinander kompatibel sind. Die Internet Engineering Task Force (IETF) hat das SSH2-Protokoll übernommen und Standards (RFCs) veröffentlicht, die die Implementierung des Protokolls regeln.

SSH1 und SSH2 haben die folgenden Funktionen gemeinsam:

- Client-Programme, die Remote-Anmeldungen, Remote-Befehle und sicheres Kopieren von Dateien in einem Netzwerk ausführen
- Ein hochgradig konfigurierbarer SSH-Server
- Eine Reihe auswählbarer Verschlüsselungsalgorithmen und Authentifizierungsmechanismen
- Ein SSH-Agent, der zur Erleichterung des Zugriffs Schlüssel im Cache hinterlegt

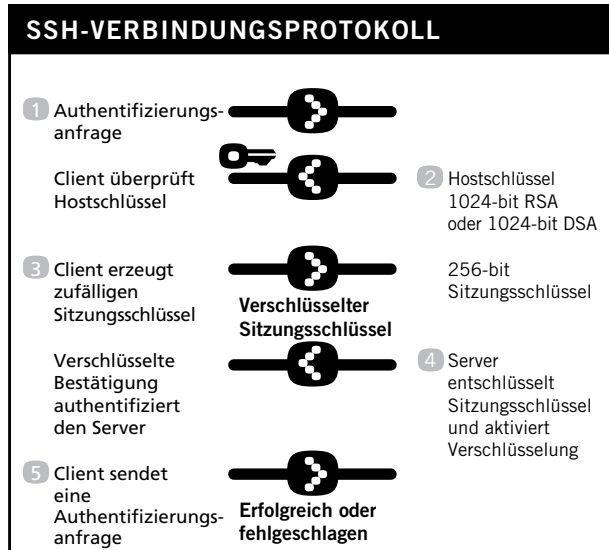
SSH2 verfügt über zahlreiche weitere Funktionen, die das Produkt leistungsfähiger und umfangreicher machen. Zu diesen Funktionen gehören:

- Codeschlüssel zur Verschlüsselung, z. B. 3DES und AES
- Die Verwendung solider Message Authentication Code (MAC)-Verschlüsselungsalgorithmen zur Integritätsprüfung
- Unterstützung von öffentlichen Schlüsselzertifikaten

SSH1 und seine zahlreichen Anwendungen werden nach wie vor im Internet eingesetzt. Diese Situation ändert sich jedoch rasch, da mittlerweile SSH2 eingesetzt wird, welches nach den Verschlüsselungsstandards FIPS 140-1 und 140-2 NIST der US-Regierung zertifizierbar ist. Auch im Wirtschaftssektor findet ein umfangreicher Wechsel zu SSH2 statt, um die Vorteile der erweiterten Sicherheit und des technischen Supports zu nutzen.

## SSH-Funktionen

In diesem Abschnitt werden die Funktionen aufgeführt, die SSH zu einem so leistungsfähigen Hilfsmittel in der Bemühung um sichere Netzwerke machen.



Sofern nicht anders angegeben, sind diese Funktionen Standard für SSH1, SSH2, OpenSSH und gewerbliche Produkte wie Reflection® for Secure IT.

### Sichere Remote-Anmeldungen

Sowohl Telnet als auch die gängigen Berkeley r-Befehle (rsh, rlogin und rcp) übermitteln Benutzernamen und Kennwortdaten in reinem Textformat über das Netzwerk, wodurch sie von Dritten relativ leicht abgefangen werden können. Telnet-Sitzungen sind auch lesbar, wenn leicht verfügbare Netzwerkanalyseprogramme zum „Abhören“ der Leitung verwendet werden.

SSH ist ein Ersatz sowohl für Telnet als auch für rlogin. Wird statt Telnet das SSH-Programm ausgeführt, erfolgt die Authentifizierung beim SSH-Server des externen Computers über eine verschlüsselte Verbindung. Die gesamte Sitzung ist sicher, und dank der transparenten Verschlüsselung stellt der Benutzer keinen Unterschied fest.

### Sichere Dateiübertragungen

Für die Dateiübertragung in gemischten Umgebungen wird FTP (File Transfer Protocol) verwendet. Als Standardkomponente jedes Betriebssystems ist FTP das gängigste Hilfsmittel zur Übertragung von Dateien mit einer Größe von mehr als 5 MB, die nicht per E-Mail verschickt werden können. FTP funktioniert schnell und ist kostenlos – soweit die Vorteile.

Aber FTP ist problematisch, da es die von einem Computer zum anderen über das Internet verschickten Daten nicht verschlüsselt. Daher können Datenpakete auf dem Übertragungsweg leicht abgefangen und

gelesen werden. Außerdem müssen Kennwörter für automatisierte Sitzungen in Scripts programmiert werden.

Im Vergleich ergeben sich klare Vorteile für SSH. Mit SSH sind Dateiübertragungen leicht und sicher zu automatisieren. SSH verschlüsselt Dateien vor deren Übertragung und entschlüsselt sie wieder, nachdem sie am Bestimmungsziel angekommen sind. Ein weiterer Vorteil neben der überaus sicheren Benutzerauthentifizierung liegt darin, dass SSH keine Kennwörter in Scriptform benötigt.

### Sichere Remote-Administration

Telnet ist ein weit verbreitetes Protokoll für den Remote-Zugang zu UNIX-Servern und deren Administration. Wie FTP gehört es standardmäßig zum Lieferumfang von UNIX. Die Vorteile von Telnet liegen darin, dass es kostenlos und leicht zu verwenden ist und keine Konfiguration benötigt. Die Einschränkungen von Telnet sind jedoch erheblich. Es bietet keine Sicherheit vor Abhöraktionen oder Kennwortdiebstahl, jediglich die Authentifizierung von Kennwörtern aus reinem Text.

Auch hier erweist sich SSH als überlegen. Es bietet sicheren Remote-Zugang und sichere Remote-Administration von UNIX-Servern, einschließlich verschiedener Benutzerauthentifizierungsmethoden. Bei der Nutzung grafischer X11 Window-Systemanwendungen überträgt SSH den Netzwerkdatenverkehr automatisch durch einen sicheren Tunnel.

### Sichere Ausführung von Remote-Befehlen

Systemadministratoren müssen häufig denselben Befehl auf mehreren Computern ausführen. Das ist mit dem Berkeley rsh-Befehl möglich, aber wie bei den verwandten r-Befehlen werden auch hier die Befehle nur in reiner Textform übermittelt. SSH hingegen verschlüsselt alle Befehle für die Übertragung im Netzwerk.

### Schlüssel und Agenten

Wenn ein Benutzer innerhalb eines Netzwerks auf mehreren Computern über Konten verfügt, muss normalerweise jedes Konto durch ein individuelles Kennwort geschützt sein. Benutzer müssen sich Kennwörter merken und wiederholt eingeben – ein aufwändiger und risikoreicher Vorgang.

Mit der SSH-Funktion zur Authentifizierung des öffentlichen Schlüssels erübrigt es sich, Kennwörter im Gedächtnis behalten und wiederholt eingeben zu müssen. Ein Schlüssel ist eine Folge von Bits, mit der sich ein SSH-Client eindeutig identifizieren kann. Das SSH-Programm bietet einen ssh-Befehl zur Schlüsselgenerierung, mit dem der Benutzer ein Schlüsselset erstellen kann. Der private Schlüssel, der geheim gehalten werden muss, verkörpert die Identität des Benutzers bei ausgehenden Verbindungen. Der öffentliche Schlüssel symbolisiert die Identität des

Benutzers für Verbindungen, die auf seinem Konto eingehen. Schlüssel und der Authentifizierungsagent des SSH-Programms erleichtern Benutzern und Administratoren die Arbeit gleichermaßen.

### **Anschlussweiterleitung**

Mithilfe der Anschlussweiterleitung, auch „Tunneling“ genannt, wird potenziell unsicherer TCP/IP-Datenverkehr über eine SSH-Verbindung weitergeleitet. Dies ist eine einfache, kostengünstige Möglichkeit, Verbindungen über POP3, SMTP und HTTP sowie FTP-, NMTP- und sonstige TCP-basierte Dienste zu schützen. Jede TCP-basierte Anwendung kann auch durch einen SSH-Tunnel gesichert werden. So sind für diese Anwendungen Datenschutz, Integritätsprüfung, Authentifizierung und Autorisierung gewährleistet.

### **SSH-Schutz**

In diesem Kapitel werden denkbare Methoden aufgezeigt, mit denen Hacker während der Übertragung auf Ihre Daten zugreifen können. Außerdem wird erläutert, wie SSH diese Angriffe abwehrt.

#### **Abhören**

Mithilfe so genannter Packet-Sniffer-Software können Eindringlinge unverschlüsselt im Netzwerk übertragene Daten ausspionieren, ohne dass Absender oder Empfänger davon etwas bemerken. Kostenlose Abhörprogramme dieser Art sind im Internet leicht zu finden und können unverschlüsselte Kennwörter, Benutzernamen oder sonstige über ein Netzwerk übermittelte Daten zusammentragen. Selbst wenn ein Kennwort verschlüsselt ist, können Eindringlinge allein durch Beobachtung des nach Eingabe des Kennworts entstehenden unverschlüsselten Datenverkehrs persönliche Informationen aufgreifen.

SSH schützt vor Abhörangriffen, indem alle Daten verschlüsselt und damit für potenzielle Eindringlinge unlesbar werden.

#### **DNS- und IP-Spoofing**

Trickst ein Angreifer einen DNS-Server so aus, dass er einem unzuverlässigen Host vertraut, spricht man von DNS (Domain Name System)-Spoofing. Auf diese Weise können Personen auf E-Mails Ihrer Website zugreifen oder Benutzer auf falsche Internetseiten lenken. Nach Angaben des Magazins „Information Security“ ist jedes dritte Unternehmen mit Internetpräsenz anfällig für DNS-Spoofing.

Beim IP-Spoofing kann durch Versenden einer Nachricht mit der IP-Adresse eines zuverlässigen Hosts auf einen Computer zugegriffen werden. Dieses Verfahren ist zwar etwas arbeitsaufwändig für den Angreifer, aber es stellt eine wirksame Hackingmethode dar.

SSH wehrt derartige Angriffe durch kryptografische Überprüfung der Server-Identität ab. Der SSH-Client

gleicht für jede Sitzung den Host-Schlüssel des Servers mit einer lokalen Liste verfügbarer Schlüssel ab, die Servernamen und Adressen zugeordnet sind. Stimmen die Schlüssel nicht überein, wird sofort eine Warnmeldung ausgegeben.

### **Connection Hijacking**

Trennt ein Angreifer Benutzer von deren TCP-Verbindung, so spricht man von Connection Hijacking oder Spoofing von TCP-Paketen. Angreifer müssen „aktiv“ sein, d. h., um ein Connection Hijacking auszuführen, müssen sie sowohl Netzwerkdatenverkehr abfangen als auch eigenen Datenverkehr in die Übertragung einbringen können.

Beim Connection Hijacking „lauert“ ein Angreifer im Netzwerk und fahndet nach Paketen, die vom Client an den Server übermittelt werden. Dadurch erhält der Angreifer dann die IP-Adressen und die dazugehörigen Port-Nummern des Hosts, mit denen er TCP/IP-Pakete manipulieren kann. Angriffe dieser Art können trotz leistungsfähiger Authentifizierungsmethode verheerend sein.

SSH kann Hijackings auf Grund einer Schwachstelle in der TCP-Schicht nicht verhindern. SSH vermag jedoch das Hijacking durch die Integritätsprüfung unwirksam zu machen. Wird eine Sitzung während der Übertragung verändert, unterbricht SSH die Verbindung sofort, ohne dass es zur Verwendung der schädlichen Daten kommt. Für die Integritätsprüfung verwendet SSH2 die kryptografisch starken Hash-Funktionen MD5 und SHA-1.

### **Man-in-the-Middle-Angriffe**

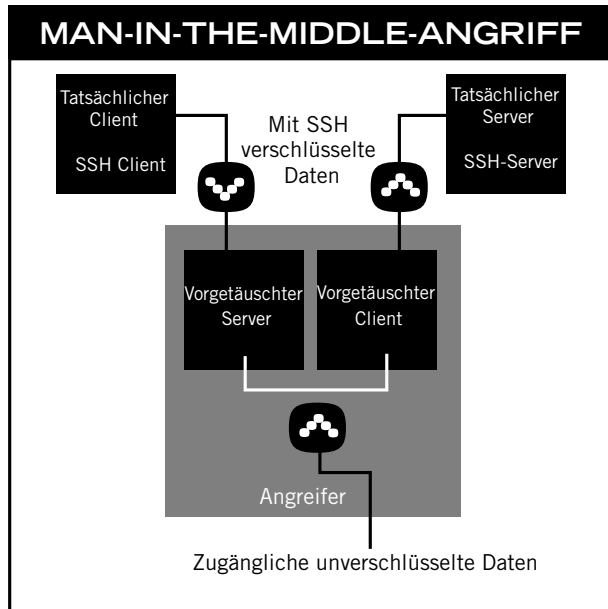
Ein Man-in-the-Middle-Angriff liegt vor, wenn die Kommunikation zwischen zwei Verbindungspartnern über einen dritten Host läuft. Ein Angreifer schaltet sich während einer Sitzung zwischen den SSH-Client und den Server und überzeugt beide Hosts davon, dass er selbst der jeweils andere Host ist.

Nachdem ein Client authentifiziert und ihm von einem Server Zugang gewährt wurde, ist der Angreifer in der Lage, die für die Datenübertragung verwendeten Port- und Sequenz-Nummern zu erfahren. Mit diesen Informationen kann der Angreifer den Datenverkehr anzapfen, Daten lesen, abfangen oder löschen. Der Hacker verwendet denselben Sitzungsschlüssel wie der rechtmäßige Benutzer und täuscht damit eine direkte Verbindung zwischen Client und Server vor.

Es gibt zwei Möglichkeiten, wie SSH vor Man-in-the-Middle-Angriffen schützen kann:

- Das erste Verfahren ist die SSH-Server-Host-Authentifizierung. Da der Angreifer nicht über den privaten Hostschlüssel des Servers verfügt, müsste er in den Server-Host „einbrechen“, um den Identitätswechsel durchzuführen. Damit dieser Schutz vollständig wirksam ist, muss der Client den vom Server bereitgestellten Schlüssel mit der Liste der bekannten Hosts abgleichen.

- Die zweite Schutzmaßnahme von SSH besteht in einer höheren Authentifizierungssicherheit für den Client. Kennwörter sind anfällig, während öffentliche Schlüssel und Zertifikate gegenüber solchen Angriffen im Wesentlichen immun sind.



### Insertion Attacks

Bei Insertion Attacks, auch bekannt als Replay Attacks, ermittelt der Hacker ein Datenpaket, das einen speziellen Befehl enthält. Dieses Paket wird zu einem anderen Zeitpunkt während der Sitzung erneut versendet, um den Befehl wiederverwenden zu können. Wie beim Hijacking von TCP-Verbindungen werden auch bei Insertion Attacks veränderte Daten in den Übertragungsverkehr des Netzwerks eingeschleust. Im Falle von Insertion Attacks werden die Daten jedoch verschlüsselt eingebracht und entweder an den Client oder an den Server zur Entschlüsselung gesendet.

SSH2 setzt kryptografisch leistungsfähige Integritätsprüfungen, nämlich SHA-1 und MD5, zur Abwehr von Insertion Attacks ein.

### Wann bietet SSH keinen Schutz?

SSH hat keine Verteidigungsmöglichkeit, wenn ein Angreifer eine Root-Verbindung zu einem Computer erlangt hat. An diesem Punkt kann der Angreifer SSH von innen destabilisieren und damit die Sicherheit vollkommen ausschalten. Die folgenden Beispiele schildern die Angriffsarten und die Situationen, die die Sicherheit Ihres Netzwerks trotz SSH unterlaufen können.

### Knacken von Kennwörtern

Zwar verschlüsselt SSH Kennwörter während der Übertragung über ein Netzwerk, aber dennoch ist ein Kennwort eine Art der Authentifizierung,

die leicht angreifbar ist. Beispielsweise kann ein Angreifer mithilfe eines Programms, das eine Liste von Wörterbucheinträgen verwendet, einen frontalen „Wörterbuch-Angriff“ starten, um sich als Administrator anzumelden.

Die nahe liegende Gegenmaßnahme zu dieser Art von Angriffen ist die Wahl eines komplexen Kennworts. Es ist grundsätzlich zu empfehlen, dass Benutzer Kennwörter aus einer Kombination von Groß- und Kleinbuchstaben und Zahlen erstellen und dass diese nur dem Administrator bekannt sind. Mit SSH können Server auch für die Verwendung öffentlicher Schlüssel an Stelle von Kennwörtern konfiguriert werden, sodass das Problem unsicherer Kennwörter entfällt.

### IP- und TCP-Angriffe

Da SSH auf TCP (Transmission Control Protocol) und IP (Internet Protocol) aufsetzt, ist es anfällig gegenüber Angriffen auf die immanenten Schwachstellen dieser beiden Protokolle. Die Angriffe setzen auf Netzwerkebene an, sodass SSH nicht davor schützen kann. Dazu gehören Dienstverweigerungen (Denial of Service) und die Umleitung von Daten zu nicht beabsichtigten Bestimmungsziele. Methoden auf niedrigerer Ebene (z. B. IPSec) können Angriffe auf TCP/IP-Ebene abwehren.

### Analyse des Datenverkehrs

Obwohl SSH Eindringlinge am Lesen des Netzwerkverkehrs hindert, kann ein Angreifer immer noch recht viele Informationen aus einfacher Beobachtung ziehen. Übertragungsmenge, -ziele und -zeitpunkt dienen Eindringlingen zur Ermittlung von Transaktionen, Zeitplänen der Datensicherung oder dem günstigsten Zeitpunkt zum Start eines Denial-of-Service-Angriffs. SSH-Datenverkehr ist leicht ausfindig zu machen und üblicherweise auf den bekannten Port 22 ausgerichtet.

Eine Möglichkeit, dieses Risiko zu senken, ist die Erzeugung eines ständigen Datenstroms, unabhängig davon, ob das Netzwerk aktiv ist oder nicht. Dadurch wird verhindert, dass Angreifer den tatsächlichen Datenverkehr ermitteln können.

### Verborgene Kanäle

Verborgene Kanäle (Covert Channels) übermitteln Daten auf nicht vorhersehbare und unbemerkte Weise. Mitarbeiter mit Nutzungsbeschränkungen für E-Mails können beispielsweise miteinander kommunizieren, indem sie Nachrichten in ihre Home-Verzeichnisse aufnehmen. Ein Systemadministrator erwartet diese Art der Kommunikation nicht und hätte Schwierigkeiten, diese zu unterbinden.

SSH ergreift keine Abwehrmaßnahmen gegen Covert Channels. Es kann aber selbst als verborgener Kanal verwendet werden, indem gerade und ungerade Paketlängen die Punkte und Striche des Morsecodes simulieren.

## Fünf Fallstudien aus der Praxis

Wie gut passt SSH in ein verantwortungsbewusstes, umfassendes Programm zur Unternehmenssicherung? Technologien zur Informationssicherheit (InfoSec-Technologien) dienen in der Regel dem Schutz von drei Elementen: Vertraulichkeit, Integrität und Verfügbarkeit. Die Beeinträchtigung eines dieser drei Elemente hat wirtschaftliche, politische und gesellschaftliche Konsequenzen.

Da Informationen einen Wert besitzen, sind sie ein attraktives Ziel für Kriminelle. Gemäß den InfoSec-Grundsätzen werden Computer so entwickelt, implementiert und betrieben, dass nur befugte Personen auf vertrauliche Daten zugreifen, Informationen ändern oder vernichten bzw. den Zugriff auf Informationen ggf. verweigern können. Doch möglicherweise reicht die herkömmliche InfoSec-Gestaltung nicht aus, um die heutzutage für Computer bestehenden Gefahren abzuwehren.

Um Verluste zu mindern und einen Standard gebührender Sorgfalt zu etablieren, müssen sich die InfoSec-Fachleute mit den zusätzlichen Elementen von Authentizität, Besitz und Zweckmäßigkeit befassen. Die ersten drei Fallstudien erläutern, wie SSH die InfoSec-Ziele aktiv unterstützt. Die beiden letzten Fallstudien zeigen, was passieren kann, wenn SSH nicht eingesetzt wird. Alle Fälle basieren auf tatsächlichen Erlebnissen von Kunden.

### Fall 1: Fernzugriff und -administration

Im ersten Fall geht es um ein mittelständisches Unternehmen. Es hat fünf Niederlassungen mit Internetverbindungen, Standleitungen und einer gemischten Umgebung aus UNIX- und Windows-Servern, die eine kleine Gruppe von Administratoren und eine größere Gruppe von Benutzern unterstützen. Erwartungsgemäß müssen die Unternehmensserver regelmäßig gewartet und einem Cleanup unterzogen werden.

Ohne SSH verwalten die Administratoren die Hosts mit Hilfe unsicherer UNIX-Dienstprogramme (rlogin, rcp und FTP). Diese Dienstprogramme sind deshalb nicht sicher, weil sie für Hacker leicht zugänglich sind und Denial-of-Service-Angriffe zulassen, die Vertraulichkeit, Integrität und Authentifizierung unterwandern. Der Windows-Server wird mit Hilfe eines unsicheren Zugriffs auf die Funktionen des Windows Terminal Servers verwaltet. Das Unternehmen verwendet pro Niederlassung eine Standleitung, sodass Kennwörter und Daten nicht ungeschützt übermittelt werden müssen.

Durch den Einsatz von SSH kann das Unternehmen seine Kosten senken, da sich die Technologie in die bestehende Netzwerkinfrastruktur einbinden lässt. Zusätzlich zur Sicherung von Dateiübertragungen können Administratoren mit Hilfe von SSH sicher auf die UNIX- und Windows-Server zugreifen. Und da sich Kennwörter und Daten sicher über das Internet

übertragen lassen, benötigt das Unternehmen nicht so viele teure Standleitungen. Zudem sind die Firewalls zwischen den Niederlassungen leicht konfigurierbar und können als gesonderte Authentifizierungshosts für Benutzer dienen. Mit dieser Methode wird eine erhebliche Menge an Zeit und Geld eingespart. Noch wichtiger ist, dass SSH die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen schützt und deren unbefugte Offenlegung, Änderung, Löschung oder Verwendung verhindert. In den meisten Fällen verringern sich dadurch gesetzliche Haftungsansprüche und Verluste.

### Fall 2: Sichere Übermittlung von Finanzdaten

Als nächstes wollen wir einen Blick auf die Finanzkreise und deren Bedarf an sicherer Datenübermittlung werfen. Banken führen Transaktionen durch und unterhalten zahlreiche überaus wichtige Datenbanken, die zum Abschluss eines jeden Geschäftstags synchronisiert werden müssen. Um die Integrität und Vertraulichkeit der Daten zu gewährleisten, werden dort Batch-Übertragungen (viele zu einem zufälligen Zeitpunkt im Verlauf von 24 Stunden) ausgeführt. Dabei darf es nicht zu Fehlern oder Störungen kommen, und die Ausführung muss in einer robusten, authentifizierten Umgebung erfolgen.

Ohne SSH benötigt jeder Bankserver seine eigenen Netzwerkverschlüsselungsgeräte. Die Zahl der zu verwaltenden Geräte kann recht groß sein, und die Verbindungen bleiben unsicher, da sie durchgängig sind. Dies wurde bei den Sicherheitsnachteilen von ungeschützten Netzwerken bereits aufgezeigt. Beide Enden der Verbindung zwischen Server und Verschlüsselungsgerät sind unsicher und daher leichte Ziele für Abhörangriffe.

Ein weiteres Problem besteht darin, dass Kennwörter während der Datenübermittlung in Scripts kodiert werden müssen, damit eine Authentifizierung am Remote-Server stattfinden kann. Dadurch wird das Verbergen der Verbindungskennwörter erschwert. Und noch schwieriger wird die regelmäßige, zur Aufrechterhaltung der Sicherheit notwendige Änderung der Kennwörter. Schließlich sind die Verbindungskennwörter möglicherweise mehreren Personen bekannt. Das heißt, sie sind nicht persönlich oder zufällig genug, um sie vor Sicherheitsverstößen zu schützen.

Eine vernünftige Lösung bestünde darin, die Sicherheit durchgängiger Verbindungen mit SSH und einer Authentifizierung über öffentliche Schlüssel sicherzustellen. Eine Batch-Übertragungsverbindung ist mit SSH durchgängig gesichert, ohne dass Server-Verschlüsselungsgeräte oder Script-Verbindungskennwörter erforderlich sind. Zudem bietet SSH effektiveren Schutz bei der Benutzerauthentifizierung. Das Ergebnis ist ein höheres Sicherheitsniveau mit geringerem Verwaltungsaufwand.

### Fall 3: Kommunikation zwischen Geschäftspartnern

In diesem Fall wird ein Software-Unternehmen mit seinen Kommunikationsanforderungen betrachtet. Das Unternehmen entwickelt und vermarktet Software in Zusammenarbeit mit verschiedenen Entwicklungspartnern, Vertriebspartnern und Wiederverkäufern. Mit diesen Partnern werden während der Produktentwicklung und vor der Produktfreigabe Daten aus Forschung, Entwicklung, Verkauf und Marketing über das Internet ausgetauscht. Die Partner suchen über eine Website nach Produktmaterial und Aktualisierungen und laden diese herunter. E-Mails werden für Massensendungen und zum Verteilen großer Materialmengen wie Datenblätter oder Preisinformationen genutzt, während FTP gelegentlich zum Versenden von CD-Images verwendet wird.

Aufgrund des eigentumsrechtlichen Schutzes der ausgetauschten Daten sind strenge Sicherheitsrichtlinien und eine Verschlüsselung des Netzwerkverkehrs erforderlich. Das heißt, für jeden Partner ist ein eigens konfigurierter Kommunikationsweg mit den von den Beteiligten eingesetzten verschiedenen VPN (Virtual Private Network)-Geräten notwendig. Netzwerk-Administratoren wissen, dass eine derartige Aufgabe nicht leicht zu bewältigen ist.

Der Austausch von Daten per FTP ist nachweislich unsicher. Zudem verwendet in diesem Fall jeder Beteiligte ein anderes VPN-Gerät mit unterschiedlichen Zugangsarten (und uneinheitlichen Handshakes) zum entsprechenden internen Netzwerk. Dadurch entstehen erhebliche Mehrkosten für den Netzwerkbetrieb, und Benutzerauthentifizierung sowie Anforderungen der Schlüsselverwaltung werden komplizierter.

SSH hingegen lässt sich in bestehende Netzwerkinfrastrukturen integrieren, wobei keine Einzelheiten zu Produkten in unbefugte Hände gelangen können. Es ist möglich, jeden Partner und Benutzer persönlich zu identifizieren, da die Zugangs-Tokens unverwechselbar sind. Risiken und Anfälligkeit werden dadurch reduziert. Durch eine Standardisierung von SSH in der Forschungs- und Entwicklungskommunikation wird das Problempotenzial hinsichtlich Partner-Zugangsverwaltung drastisch gesenkt. Zugang wird nur zu Einzelpersonen und nicht zu ganzen Netzwerken gewährt, wodurch sich Verluste identifizierbaren Einheiten zuordnen lassen.

### Fall 4: Server mit Sicherheitslücke als Einfallstor für Kennwortjäger

Ein Unternehmen ist im E-Commerce tätig und betreibt verschiedene Server in demselben Netzwerk. Aufgrund einer falsch konfigurierten Firewall war ein Server direkt vom Internet aus zugänglich. Dieser Server wurde mit Hilfe eines verwertbaren Fehlers im

Webserver von außerhalb durchsucht und damit in seiner Sicherheit beeinträchtigt. Der Hacker hat einen RAT (Remote Access Trojan) mit Spionageprogramm eingesetzt, um von allen Netzwerkbenutzern, die Verbindung zu diesem Server aufnehmen, die Kennwörter zu sammeln.

Als das fremde Programm entdeckt wurde, stellte sich heraus, dass es schon mindestens einen Monat lang ausgeführt wurde und nahezu alle Benutzernamen und Kennwörter gesammelt hatte. Der beeinträchtigte Server wurde sofort heruntergefahren. Alle Benutzerkonten wurden gesperrt, und die Benutzer mussten ihre Kennwörter ändern. Anschließend wurden die anderen Server im Netzwerk auf Anzeichen einer Sicherheitsgefährdung untersucht.

Der Hacker, der niemals gefasst wurde, hat auch andere Unternehmen erfolgreich infiltriert. Der betroffene Server lag eine Woche lang still. Zum Glück für das Unternehmen wurde kein weiterer Host angegriffen. Die Benutzer verloren einige Arbeitsstunden, um ihre Kennwörter zu ändern, und eine Woche lang waren sie in ihrer Arbeit beeinträchtigt. Dieser eine Sicherheitsverstoß verursachte wesentlich höhere Kosten, als wenn die erforderlichen Sicherheitsmaßnahmen von vornherein implementiert worden wären.

### Fall 5: Verdacht auf Datendiebstahl durch einen Wettbewerber

In diesem Beispiel befand ein Unternehmen das Internet als die einzige kostengünstige Möglichkeit zum Austausch großer Datenmengen mit Entwicklungspartnern in anderen Ländern. Obwohl die verschiedenen Datenteile einen gewissen Wert besaßen, glaubte man, der Großteil des Wertes würde erst in einer späteren Projektphase, nach der Produktentwicklung, entstehen. Die Administratoren gingen davon aus, dass Standardkommunikationsmittel wie E-Mail und FTP ausreichende Sicherheitsmaßnahmen böten und daher keine Verschlüsselung von Nöten sei.

Während der Produktentwicklung wurde deutlich, dass der direkte Wettbewerber des Unternehmens immer dieselben Etappenziele erreichte – nur jeweils ein bisschen später. Auch wenn das Unternehmen seine Innovationen als erstes eingeführt hatte, so schien doch die Tatsache, dass der Wettbewerber kurze Zeit später ähnliche Innovationen anbot, einen schlechten Einfluss auf den Absatz zu haben. Zwar konnte keine Wirtschaftsspionage nachgewiesen werden, aber es kam der Verdacht auf, einer oder mehrere ehemalige Mitarbeiter oder Partner könnten in den Diebstahl der Produktdaten verwickelt sein. Bedrohungen durch Insider allein können schon zerstörerisch sein, aber der Schaden, der durch eine Zusammenarbeit inner- und außerbetrieblicher Beteiligter angerichtet werden kann, ist potenziell noch größer. Das betreffende Unternehmen war vermutlich Ziel eines solchen koordinierten Angriffs.

Am Ende wusste niemand sicher, ob die Daten gestohlen worden waren oder nicht. Fest stand nur, dass das Unternehmen anfällig für Wirtschaftsspionage war und dass jeder Diebstahl von Produktentwicklungen das Potenzial besaß, den Aktienkurs des Unternehmens negativ zu beeinflussen. Das Unternehmen ergriff daraufhin Maßnahmen zum Schutz von Daten vor allen möglichen Formen der Spionage, ob durch Firmenfremde oder gegenwärtige bzw. ehemalige Mitarbeiter.

### Abwägung der Kosten für SSH

Die größten IT-Ausgaben werden im Allgemeinen für Personalkosten aufgewendet. Eine schwerwiegende Verletzung der Datensicherheit auf Netzwerkebene bedeutet aber einen Zeitverlust überall im gesamten Unternehmen. Unter anderem nehmen die IT-, Rechts-, Risiko-, und PR-Abteilung sowie die Geschäftsführung Schaden.

Das folgende hypothetische Kostenbeispiel zur Einrichtung eines Basisdienstes (wie eine Website oder Datenbank) soll den Aufwand verdeutlichen, den es im Zusammenhang mit allen Systemen gibt, die wertvolle Geschäftsdaten verarbeiten, speichern oder austauschen.

- Einfache Server kosten normalerweise ca. 2.300 \$.
- Für Softwarelizenzen kommen weitere 2.000 \$ hinzu.
- Die Einrichtung des Servers (Gestaltung und Installation) kostet mindestens weitere 2.000 bis 2.500 \$.
- Nach der Installation fallen durchschnittlich 200 bis 250 \$ im Monat für die Wartung des Dienstes an.

In diesem Beispiel betragen die Kosten für die Einrichtung ca. 10.000 \$, worin die gesamte Hardware, Software und Wartung für das erste Jahr enthalten sind.

Eine Lizenz für einen gewerblichen SSH-Server kostet weniger als 10 Prozent des oben genannten Preises für diese extrem einfache Systemeinrichtung. Verfügt ein System jedoch nicht über SSH-Schutz und wird angegriffen, kommen Administratoren nicht umhin, Arbeitsschritte zu wiederholen, Kennwörter zu ändern und eine Reihe anderer reaktiver Maßnahmen zur Sicherung des Systems zu ergreifen.

Bei 50 \$ pro Stunde und pro Administrator, ergibt sich für SSH ein Preis, der unter dem für 10 administrative Arbeitsstunden zur Sicherung des Systems liegt. Und bei diesem Vergleich sind die während des Stillstands und der Instandsetzung des Dienstes verlorenen Einnahmen oder die unvermeidlichen Kosten im Zusammenhang mit einer folgenden Rufschädigung nicht mitgerechnet.

### Vergleich der Optionen

Seit fast 10 Jahren sichert SSH Netzwerkverbindungen, und es stehen eine ganze Reihe von Implementierungs-

möglichkeiten zur Verfügung. Einige Versionen beinhalten ein Server-Betriebssystem oder können kostenlos im Internet heruntergeladen werden. OpenSSH ist ein Beispiel für Letzteres. Außerdem können Sie voll unterstützte gewerbliche Versionen von Drittanbietern erwerben, beispielsweise Reflection for Secure IT. In diesem Abschnitt werden beide Optionen erläutert.

### OpenSSH

Zu den Vorteilen von OpenSSH gehören eine große Benutzer-Community, Support für die meisten UNIX-Plattformen und die Tatsache, dass es kostenlos verfügbar ist. Doch trotz dieser Vorteile bringt OpenSSH erhebliche Risiken mit sich, die Administratoren bei der Auswahl eines SSH-Anbieters berücksichtigen müssen.

- Die Zahl der unterstützten Plattformen ist begrenzt, und es fehlt an integriertem Windows-Support.
- Die Qualitätskontrolle ist gering bis nicht vorhanden. Jedes Jahr müssen mehrere wichtige Aktualisierungen installiert werden, was ebenfalls Gefahren mit sich bringt.
- Es gibt keinen einheitlichen Anlaufpunkt für den Bezug von Aktualisierungen.
- Es gibt keinen verlässlichen Support, keinen zweifelsfrei zuständigen Ansprechpartner bei Fragen, und selbst bei den einfachsten Anfragen in Newsgroups besteht die Gefahr einer ablehnenden Antwort.
- Die Funktionalität ist technisch begrenzt. Viele Implementierungen von OpenSSH unterstützen beispielsweise PKI nicht oder nur unvollständig. Bei OpenSSH sind mehr als fünf größere Produkterweiterungen noch nicht berücksichtigt, daher wird es mit der unterstützten Technologie nicht gleichziehen.
- Es gibt keine Haftungs- oder Patentgarantien, was für Unternehmen das Risiko von Urheberrechts- und Patentklagen mit sich bringt.

### Reflection for Secure IT

Seit der Einführung im Jahr 1996 haben sich zahlreiche Netzwerkadministratoren für Reflection for Secure IT entschieden. Die meisten Kunden von Reflection for Secure IT sind Behörden, große Banken, Versicherungen sowie Firmen aus dem Telekommunikationsbereich. Sie alle bedürfen einer leistungsfähigen Netzwerksicherheit.

Zu den Vorteilen von Reflection for Secure IT gehören:

- Qualitativ hochwertige Software
- Geringere Verwaltungskosten (im Vergleich zu anderen Optionen)
- Geringe Gesamtbetriebskosten
- Umfassender Support und umfassende Wartung durch professionelles Personal, das Fragen beantwortet, kundenspezifische Ausführungen bietet und bei Bedarf Probleme löst

- Rechtzeitige Softwareaktualisierungen
- Die Gelegenheit, neue Geschäftswege zu nutzen

### Die Wahl der richtigen Sicherheitslösung

Für die meisten Softwareprodukte gilt: Die Gesamtkosten haben nicht viel mit dem Wert auf dem Preisschild zu tun, sondern vielmehr mit dem Arbeitsaufwand, der für die Einrichtung, den Betrieb und die Wartung des Systems erforderlich ist. Die folgenden Faktoren sind bei der Auswahl einer Sicherheitslösung für Netzwerke zu berücksichtigen:

- Support rund um die Uhr
- Schulungen und Fortbildungen
- Qualitätssicherung
- FIPS-Zertifizierung durch die US-Regierung (NIST)
- Unterstützung zahlreicher Plattformen
- Kundenspezifische Optionen
- Schutz vor gesetzlichen Haftungsansprüchen
- Anfälligkeitsbenachrichtigungen
- Gewährleistung geistiger Eigentumsrechte (um Rechtsstreitigkeiten vorzubeugen)

Wie zuvor bereits erwähnt, liegt das Problem der in Betriebssystemen enthaltenen Optionen wie FTP und Telnet darin, dass diese keine oder nur wenig Sicherheit bieten.

SSH-Freewareoptionen umfassen keine Support-Verträge, und bei Aktualisierungen fehlt häufig eine entsprechende Qualitätskontrolle, wodurch Systeme für Angriffe anfällig werden. Da es keinen Verkäufer gibt, liegt die Verantwortung für Softwareanfälligkeiten ausschließlich beim Benutzer. Ähnlich sieht es bei den meisten in Betriebssystemen enthaltenen SSH-Anwendungen aus: Sie bieten keinen entsprechenden Anbietersupport und wurden möglicherweise aus einem älterem Code mit entsprechenden Sicherheitslücken generiert.

### Von der UNIX-Administration zur Protokollsuite für umfassende Sicherheitsbelange

Anfänglich war die SSH-Protokollsuite für fast alle UNIX-Server das bevorzugte Sicherheitsprogramm. SSH-Entwickler wie Attachmate erweiterten ihre Plattformunterstützung (z. B. um Windows) und führten neue Funktionen ein. Diese robuste Sicherheitstechnologie bewältigt eine ganze Reihe von Problemen, nicht nur Administration und einfache Dateiübertragungen. SSH kann auf alle Sicherheitsprobleme im Zusammenhang mit drahtlosen Verbindungen, PDAs und spezialisierten Sicherheitsarchitekturen eingehen.

Wir sind der Ansicht, dass gewerbliche Fortified-Versionen (d. h. kontinuierlich verbesserte und unterstützte Versionen) von SSH dazu beitragen, den Löwenanteil heutiger Sicherheitsanforderungen zu erfüllen. Kurz gesagt: SSH vereinigt sichere Kommunikation, stabile Authentifizierung, bessere

Zugangskontrolle, leichtere Firewall-Konfiguration und Zugang zu UNIX und Windows Servern in einem einzigen Programm. Gewerbliche SSH-Versionen – insbesondere die FIPS-zertifizierte SSH-Version – senken das Risiko deutlich, erfüllen einen Standard gebührender Sorgfalt und erreichen das höchste Sicherheitsniveau.

## Informationen zu Attachmate

Attachmate hilft Unternehmen bei der Erweiterung, Verwaltung und Sicherung ihrer IT-Investitionen. Wir bieten eine große Bandbreite von Lösungen – von Terminalemulation, Legacy-Integration und PC-Lifecycle-Management bis zu innovativen Systemen und Sicherheitsmanagementwerkzeugen. Weltweit nutzen mehr als 65.000 Kunden unsere Technologie, um ihre IT-Anlagen auf neuartige Weise sinnvoll einzusetzen. Weitere Informationen finden Sie auf unserer Website unter [www.attachmate.de](http://www.attachmate.de).



### Hauptsitz

1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL +1 206 217 7500  
FAX +1 206 217 7515

### Europäische Zentrale

Niederlande  
TEL +31 71 368 1100  
FAX +31 71 368 1181

### Österreich

TEL +43 1 595 4335 0  
FAX +43 1 595 4335 11  
[www.attachmate.at](http://www.attachmate.at)  
[info-at@attachmate.com](mailto:info-at@attachmate.com)

### Schweiz

TEL +41 43 399 2090  
FAX +41 43 399 2099  
[www.attachmate.ch](http://www.attachmate.ch)  
[InfoCH@attachmate.com](mailto:InfoCH@attachmate.com)

### Deutschland

TEL +49 89 99 351 0  
FAX +49 89 99 351 111  
TEL +49 2102 4965 0  
FAX +49 2102 4965 65  
TEL +49 711 67 968 0  
FAX +49 711 67 968 33  
[www.attachmate.de](http://www.attachmate.de)  
[info-de@attachmate.com](mailto:info-de@attachmate.com)