Buch Internet - die Sicherheitsfragen

Antworten für Manager und Techniker

Christian Reiser
Ueberreuter, 2000

Rezension

Der Autor Christian Reiser gibt fachkundig und verständlich Antworten auf Fragen der Sicherheit bei Computernetzwerken, die einen Internetzugang besitzen. Er macht deutlich, dass dieses Thema nicht auf die leichte Schulter genommen werden darf, und sensibilisiert Manager und Techniker für Sicherheitsfragen. Gleichzeitig malt er keine Schreckensszenarien an die Wand, sondern erklärt sachlich und unaufgeregt, welche Angriffe aus dem Internet zu befürchten sind, von wem diese stammen können und wie man sich dagegen schützt. Dabei wird sowohl die technische Seite, beispielsweise die Frage nach der richtigen Firewall, als auch die organisatorische, also wer z. B. für die Wartung der Firewall zuständig ist, angesprochen. Das ist wichtig, weil beide Seiten bei allen Sicherheitsvorkehrungen beachtet werden müssen. Der Autor vermittelt zudem Grundsätzliches zum Thema Internet und Kommunikation, sodass ein Problembewusstsein beim Leser geschaffen wird. Fallbeispiele und ein ausführlicher nützlicher Anhang, der beispielsweise die klassische "Netiquette" enthält, runden den Ratgeber ab. *BooksInShort.com* empfiehlt dieses Buch allen, die für ein firmeninternes Netzwerk verantwortlich sind und nicht Gefahr laufen wollen, dass sie Sicherheitsmängel übersehen oder nicht für ausreichende Sicherheit sorgen. Aber auch für den normalen User bietet das Werk viele interessante Informationen - und dies in gut lesbarer Form.

Take-aways

- Das Internet besteht aus unterschiedlichen Diensten, die entsprechend unterschiedliche Sicherheitsvorkehrungen erfordern.
- Das eigene Rechnernetzwerk ist immer gefährdet, auch wenn man annimmt, man hätte keine Daten, die jemanden interessieren könnten.
- Angriffe können von verärgerten ehemaligen Mitarbeitern, unehrlichen Mitarbeitern, Mitbewerbern oder Hackern kommen.
- Die meisten Probleme entstehen durch schlecht geschulte Mitarbeiter, denen ein ausreichendes Sicherheitsbewusstsein fehlt.
- Bei bewussten oder unbewussten Angriffen kann einiges passieren: Geheime Daten werden bekannt, wichtige Daten werden gelöscht, Daten werden verfälscht, Rechner und Netzwerke werden beschädigt und können nicht mehr benutzt werden.
- E-Mails werden durch Verschlüsselung geschützt, das eigene Rechnernetzwerk durch eine Firewall.
- Es gibt unterschiedliche Konfigurationen für den Einbau einer Firewall.
- Schwachpunkt ist weniger die Software, sondern der Mensch, dem Fehler bei der Konfiguration unterlaufen.

- Neben den technischen Fragen ist die organisatorische Seite von grosser Bedeutung.

Zusammenfassung

Sicherheit im Internet

Jeder Computer, der mit dem Internet verbunden ist, stellt ein Sicherheitsrisiko dar. Wer also ein internes Computernetzwerk (das LAN) an das Internet anbinden will, muss sich zwangsläufig mit Sicherheitsfragen beschäftigen und adäquate Massnahmen ergreifen, um sich vor Schäden zu schützen. Diese Massnahmen sind technischer und organisatorischer Art. Denn genauso wie die Hard- und Software muss auch die Schnittstelle Mensch auf zahlreiche Sicherheitsfragen eingestellt werden.

Am Anfang Problembereiche erkennen

Sicherheitsfragen, die das Internet betreffen, drehen sich um fünf Bereiche: Sicherheit der Übertragung durch Verschlüsselung, Sicherheit der eigenen Rechner oder Netzwerke durch Firewalls, Virtuelle Private Netzwerke (VPN) als Kombination von Verschlüsselung und Firewalls, elektronischer Zahlungsverkehr sowie Rechtssicherheit.

Grundlegendes zum Internet

Wer sich mit Internet-Sicherheitsfragen beschäftigt, sollte sich zuerst einmal mit dem Wesen des Internets, seinen Einrichtungen und der entsprechenden Begrifflichkeit vertraut machen. Grundsätzlich gibt es keine Firma "Internet", sondern eine grosse Anzahl miteinander kooperierender Internet Service Provider (ISP). Die eigene Firma ist an einem bestimmten ISP angeschlossen, meist mittels Standleitung. Das interne Firmennetzwerk (Local Area Network = LAN) bekommt so den Kontakt zur Aussenwelt.

Dienste im Internet

Das Internet hat verschiedene Ebenen und Funktionen. Die unterste ist das physikalische Medium. Darauf arbeiten verschiedene Protokolle, die für Sicherheitsfragen von Belang sind. Für den "normalen" Nutzer sind vorwiegend die Dienste des Internets interessant. An erster Stelle ist hier E-Mail zu nennen, also elektronische Post, die übers Internet versandt wird. Eine weitere Funktion des Internets sind Usenet News. Diese erfüllen die Funktion von "schwarzen Brettern" und gelten als schnellstes und ausführlichstes Informationsmedium im Internet. Über 30 000 Newsgroups mit einem täglichen Datenaufkommen von mehr als 700 000 Artikeln täglich stehen zur Verfügung.

> „Das Internet ist ein Kommunikationsmedium, das Daten von einem Ort zum anderen transportiert, wobei die ersten Enden dieser Verbindung aus Computern bestehen.“

Wohl der bekannteste Dienst und jener, dem der grosse Aufschwung des Internets zu verdanken ist, ist das World Wide Web (WWW). Den Austausch der Daten über das WWW regelt als Protokoll das Hyper Text Transfer Protocol (HTTP). Die Web-Seiten selbst sind in Hyper Text Markup Language (HTML) geschrieben. HTML definiert die Formatierung der Seiten. Fast nur für Profis ist der Telnet-Dienst von Bedeutung. Das ist ein Programm, das es erlaubt, über das Internet mit einem anderen Computer zu arbeiten, wobei der eigene Computer dann nur noch die Funktion eines Terminals hat.

> „Es gibt eine Gruppe von Menschen, die nicht die Absicht haben, der Organisation, in der sie arbeiten, zu schaden. Viele Sicherheitsvorfälle entstehen dadurch, dass ein interner Mitarbeiter etwas macht, wovon er nicht einmal ahnt, dass es gefährlich sein könnte.“

Ein Dienst, den der Nutzer kaum wahrnimmt ist, z. B. das Domain Name System (DNS). Das DNS gewährleistet eine eindeutige Adressierung jedes am Netz befindlichen Computers. Die Adresse besteht aus vier Zahlen, jeweils zwischen 1 und 255, die durch Punkte getrennt sind. Da Menschen besser mit Wörtern als mit Zahlen umgehen können, werden diesen Adressen die bekannten Domain-Namen zugeordnet - als XY.com statt 123.234.1.12.

Wer sind die Bösen?

Bei jeder Überlegung zum Thema "Wie schütze ich mein Firmennetz" vor Angriffen, sollte man sich überlegen, von wo diese Angriffe kommen können. Grundsätzlich gib es vier Gruppen von Angreifern, die mit unterschiedlichem Wissen und unterschiedlicher Absicht bzw. ohne Absicht die Sicherheit von Daten und Programmen gefährden: verärgerte ehemalige Mitarbeiter, unehrliche Mitarbeiter, Mitbewerber, Hacker. Ausserdem gibt es eine Gefährdung durch schlecht geschulte Mitarbeiter. Verschiedene Studien kommen zu dem Ergebnis, das 60-80 % der sicherheitskritischen Vorfälle aus den eigenen Reihen stammen. Von grosser Bedeutung sind hier die "Unwissenden". Deshalb sollten Mitarbeiter dringend geschult werden, damit diese ein Bewusstsein für Sicherheitsfragen entwickeln.

Was kann passieren?

Das Problem Sicherheit und Internet sollte kein Unternehmen auf die leichte Schulter nehmen. Denn überall gibt es Daten, die nicht jedermann zugänglich sein sollten. Wer leichtfertig Sicherheitsrisiken in Kauf nimmt, wird überrascht sein, wenn geheime Daten bekannt werden, wenn diese gelöscht oder verfälscht werden, wenn Rechner und Netzwerke nicht mehr funktionieren oder diese von unerlaubter Stelle benutzt werden. Solche Angriffe, nach denen Computer oder einzelne Funktionen nicht mehr benutzt werden können, so genannte "Denial-of-Service-Attacken" verursachen hohe Kosten - von der Fehlerbehebung bis zum Arbeitsausfall. Bisweilen benutzen Hacker auch die Computer-Infrastruktur, um einen Angriff auf ein anderes, wertvolleres Unternehmen zu fahren.

Schutz durch Verschlüsselung

Um Daten abhör- und fälschungssicher über ein öffentliches unsicheres Netz zu transportieren, sollten sie verschlüsselt werden. Verschlüsselung bedeutet, Daten und Informationen so zu verändern, dass Unberechtigte sie nicht verwenden können. Vom Altertum bis heute wurden immer wieder Systeme zur Verschlüsselung entwickelt. Heutzutage gelten nur noch die Systeme als sicher, deren Algorithmus offen gelegt und bekannt ist. Dass sie dennoch funktionieren, liegt daran, dass mit vertretbarem Aufwand der Text nicht lesbar gemacht werden kann, solange man den Schlüssel nicht hat. Grundsätzlich wird bei Verschlüsselungssystemen zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden.

> „Der Bereich, der in der Praxis am meisten vernachlässigt wird, ist die Dokumentation im Zusammenhang mit dem Internet-Sicherheitssystem.“

Bei symmetrischer Verschlüsselung, auch Private-Key-Verfahren genannt, wird zum Ver- und Entschlüsseln derselbe Schlüssel benutzt. Das Problem bei diesem schnellen Verschlüsselungsverfahren ist der Transport des Schlüssels, z. B. via Diskette. Bei asymmetrischen Verschlüsselungssystemen (Public-Key-Systeme) werden zum Ver- und Entschlüsseln verschiedene Schlüssel benutzt. Jede am Kommunikationsvorgang beteiligte Person verfügt dabei über einen öffentlichen und einen geheimen Schlüssel. Dadurch wird gewährleistet, dass nur autorisierte Personen die Nachricht lesen können.

Verschlüsselungsprogramme

Es gibt eine Vielzahl von Verschlüsselungsprogrammen, die z. T. auch als Public Domain oder Shareware zu haben sind. So ist zum Verschlüsseln von E-Mails das Programm Pretty Good Privacy (PGP) besonders weit verbreitet. Für die Übertragung von Kreditkartendaten kommen Secure Web-Server, die über das Secure-Socket-Layer-Protokoll (SSL) einen verschlüsselten Kanal realisieren, zum Einsatz. Das Risiko ist für Kreditkarteninhaber heute eher gering, da vielfach der Händler das Risiko trägt. Der Kreditkartenbesitzer kann jede Buchung wieder zurückbuchen lassen.

Wie schützte ich meinen Rechner und mein Rechnernetzwerk?

Um Rechner und Rechnernetzwerk zu schützen, werden so genannte Firewalls oder Firewall-Systeme eingesetzt. Firewalls schreiben mit, welche Verbindungen und Verbindungsversuche über sie geführt werden. Ziel ist es, auf diese Weise Einbruchsversuche zu erkennen. Bei der Architektur einer Firewall gibt es dann zahlreiche Möglichkeiten.

Viele Wege - ein Ziel

Sobald ein Rechner im Firmennetz als Server fungiert und damit Kontakt zum Internet geschaffen wird, muss über den Einsatz einer

Firewall nachgedacht werden. Verschiedene Systeme kommen dafür in Frage. Statistische Filterlisten entscheiden anhand der Daten im Header, welche Datenpakete passieren dürfen. Diese Lösung ist riskant, da diese Informationen dürftig sind. Dafür können die Entscheidungen sehr schnell getroffen werden.

> „Interessanter sind all die kleinen Spuren, die man bei seinen Reisen durch das Internet hinterlässt. Diese Daten liegen in den Händen der verschiedensten Firmen, Organisationen und Personen - teils im In-, teils im Ausland - und können kaum kontrolliert werden."

Dynamische Filterlisten arbeiten mit einer Art Rückantwort-System, bei dem die Beziehung zwischen Client und Server überprüft wird. Beispiel dafür ist das FTP-Protokoll. Bei einer Proxy-Firewall werden "Statthalter" (Proxies) eingesetzt, die für den Client die Leitung aufbauen. Die Adresse des Proxys ist also bekannt, die des eigentlichen internen Netzwerks nicht. In der Praxis wachsen die beiden Firewall-Technologien, also Filtering- und Proxy-Systeme, immer stärker zusammen.

"Möglichst wenig"

"Möglichst wenig" ist die Hauptregel beim Aufbau einer Firewall. Im Einzelnen heisst das: "Möglichst wenig Software", "Möglichst wenig erlauben", "Möglichst wenig Benutzer", "Möglichst wenig Wartung".

Viren - eine weitere Gefährdung

Viren und Trojaner sind keine typischen Internet-Probleme, obwohl sie gerade wegen ihrer Verbreitung über das Internet eine verstärkte Beachtung erfahren. Neueste Entwicklungen im Bereich des Datenverkehrs erlauben es, bereits auf der Firewall nach Viren zu suchen. Dies sollte jedoch immer in eine flächendeckende Virenstrategie eingebettet sein. Das heisst, dass alle im internen Netz befindlichen Computer mit Virenscanner ausgestattet sind und diese regelmässig aktiviert werden.

Welche Firewall ist die Richtige?

Die Qualität einer Firewall ist schwer zu beurteilen. Meist tauchen Probleme auch eher in der Konfiguration als bei der Software auf. Ein Einbruch ist meist durch eine fehlerhafte Konfiguration möglich. Bei den am Markt befindlichen Produkten reicht die Palette von kostenloser Public-Domain-Software bis zu kombinierten Hard- und Software-Angeboten.

Aussendienstler mit Laptop

Es ist üblich geworden, Aussendienstlern bei ihrer Arbeit durch Anschluss an das interne Netzwerk Daten zur Verfügung zu stellen und ihnen die Möglichkeit zu geben, Daten abzugleichen. Auch Mitarbeiter, die von zu Hause aus Daten benötigen, kann der Zugriff auf Firmenrechner möglich gemacht werden. Diese Virtual Private Networks (VPN) können ein Sicherheitsrisiko darstellen und müssen daher in die Schutzmechanismen eingeplant und eingebaut werden. Das gleiche gilt für die Vernetzung mit Aussenstellen des Unternehmens.

Schwachpunkt Mensch: organisatorische Massnahmen

Der Aufbau einer Firewall ist nur ein Schritt in Richtung Sicherheit. Der grösste Teil der Arbeit ist im organisatorischen Bereich angesiedelt. Hierfür muss ein Sicherheitskonzept entwickelt werden, in dem klar geregelt ist, wer welche Befugnisse hat. Benutzungsrichtlinien unterrichten jeden Mitarbeiter, was er beim Nutzen seines Rechners und des Internets zu beachten hat. Ein Sicherheitsverantwortlicher sorgt dann für die Einhaltung der Regelungen.

Über den Autor

Dr. **Christian Reiser** studierte Informatik an der Technischen Universität Wien. Neben seiner Tätigkeit im Alcatel-Elin-Forschungszentrum dissertierte er im Bereich "Künstliche Intelligenz". Seit 1995 ist Christian Reiser im Security-Solutions-Management bei einem der grössten kommerziellen europäischen Internet-Provider. Darüber hinaus hält er Vorträge, ist Lektor an zwei Fachhochschulen und veröffentlicht Bücher und Artikel in diversen Fachzeitschriften.