



MICHAEL HAACK,
Diplom-Informatiker, ist Unternehmens-
berater mit dem Spezialgebiet IT-Sicher-
heit/Datenschutz bei der UBIS GmbH

MICHAEL HAACK

Zwischen fehlendem Bewußtsein und übertriebener Angst: Die Sicherheit in Computernetzen

Nach „Multimedia“ wird in diesem Jahr wahr-
scheinlich „Internet“ das Wort des Jahres
werden. Aus gutem Grund, denn es ist in aller
Munde. Ebenso wie etwa „Telearbeit“, „Elec-
tronic Data Interchange“ oder „Electronic
Cash“. Alle diese Worte haben etwas gemein-
sam: sie werden im Kontext von Computer-
netzen gebraucht. Aber genauso wie neue Ent-
wicklungen immer große Chancen für Unter-
nehmen bilden, so sind sie auch immer mit
Risiken behaftet. Immer öfter wird in den
Medien von Hackerangriffen, Datenschutzver-
letzungen, Datenspionage oder Viren-Epide-
mien berichtet. Nicht wenige Unternehmen
werden von diesen teilweise überzogenen
oder sogar falschen Behauptungen dermaßen
abgeschreckt, daß sie aufgrund übertriebe-
ner Angst gleich gar nichts mit Computer-
netzen zu tun haben wollen.

Das andere Extrem bilden diejenigen Unter-
nehmen, die aufgrund ihres „up to date“-Strebens
schon „on-line“ sind, bevor sie überhaupt an
Sicherheitsaspekte denken konnten. In diesem
Fall ergeben sich große Sicherheitsrisiken.

Eine Einteilung der Unternehmen je nach
ihrer Strategie in bezug auf Computernetze zeigt
die Abbildung.

Ziel dieses Beitrages soll es sein, die in den
schraffierten Bereichen angesiedelten Unter-
nehmen in das Feld der optimalen Situation rechts
oben zu bringen. Dazu müssen zum einen die
übertriebenen Ängste der bisherigen Computernetz-
Ablehner abgebaut werden und zum anderen
die risikobehafteten Anwender über geeig-
nete Sicherheitsmaßnahmen aufgeklärt werden.

Abhängigkeiten und Bedrohungen

Mit der zunehmenden Vernetzung der Stand-
orte eines Unternehmens und neuen Thematiken
wie der Anbindung von Heimarbeitsplätzen, dem
elektronischen Dokumentaustausch (electronic
data interchange, EDI), dem Internetanschluß
und dem Intranet bekommt die Abhängigkeit der

Unternehmen von der Informa-
tionstechnik eine neue Dimen-
sion.

Die schon durch die wach-
sende Integration der Ablaufor-
ganisation in informationstech-
nische Prozesse auf ein hohes
Niveau gebrachte Abhängigkeit
erfährt folglich eine weitere
Steigerung. Und je abhängiger
ein Unternehmen von der Infor-
mationstechnik ist, desto grö-
ßer sind auch die Risiken, die
sich aus den vorhandenen
Bedrohungen ergeben.

Alle denkbaren Bedro-
hungen, die den Geschäfts-
ablauf bzw. die Existenz eines
Unternehmens gefährden, wie

- höhere Gewalt (Naturkata-
strophe, technisches Versa-
gen, Personalausfall),
- menschliches Versagen (Fal-
scheingabe/Bedienungsfeh-
ler, fahrlässige Beschädi-
gung, Hardwarefehler, Soft-
warefehler),
- unberechtigten Informa-

tionsgewinn (Leitung abhören, Daten am
Gerät abfragen, Diebstahl von Datenträgern
oder Ausdrucken, Abfrage von Daten beim
Benutzer),

- Sabotage (Ändern/Löschen von Daten durch
Hacker oder Insider, Gerätediebstahl, Vanda-
lismus)

können in drei Hauptkategorien eingeordnet wer-
den – je nachdem, ob die

- Vertraulichkeit,

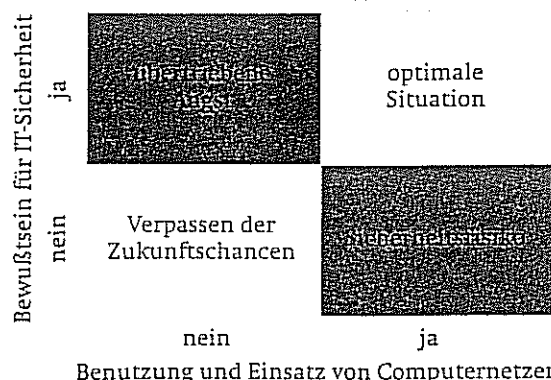


Abb. 1:
Klassifizierung
der Unternehmen

- Integrität oder
 - Verfügbarkeit
- der verarbeiteten Daten und Informationen verletzt wird.

Die erste Kategorie bezieht sich auf Geschäftsgeheimnisse und nach dem Bundesdatenschutzgesetz zu schützende (personenbezogene) Daten, die nicht an die Öffentlichkeit gelangen dürfen.

In die zweite Kategorie fallen vorsätzliche Datenveränderungen etwa durch Hacker oder Viren und fahrlässige Falscheingaben durch Benutzer.

Die für die meisten Unternehmen wichtigste Kategorie ist die der Verfügbarkeit. Durch die gewachsene Abhängigkeit von den DV-Systemen kann auch schon ein kurzer Ausfall gravierende Folgen haben.

Neben den finanziellen Schäden spielen in Zeiten eng umkämpfter Märkte Folgen wie Ansehensbeeinträchtigung, Vertrauensverlust und Image-Schädigung eine immer stärkere Rolle.

Was kann passieren?

Die folgenden Beispiel-Szenarios sollen verdeutlichen, auf welchen diversen Wegen die Netzsicherheit beeinträchtigt werden kann. Dabei zeigt es sich, daß es viele realistische Fälle gibt, die nicht durch entsprechende Maßnahmen verhindert werden können, weil sie extern verursacht sind. Diese Fälle gilt es in der Analyse zu erkennen und zu berücksichtigen, damit im Notfall diejenigen Maßnahmen getroffen sind, die den Schaden so gering wie möglich halten.

Szenario 1

Wird bei Bauarbeiten in der Nähe eines Firmenstandortes die Leitung zur Ortsvermittlungsstelle des Netzbetreibers unterbrochen, so ist dieser Standort weder telefonisch noch datentechnisch zu erreichen. Ist in diesem Fall keine zweite (redundante) Leitung zur Ortsvermittlungsstelle oder ein zweiter Anschluß (an eine andere Ortsvermittlungsstelle) vorhanden und kann der Netzbetreiber die Störung nicht in der für das Unternehmen maximal tolerierbaren Ausfallzeit beheben, drohen Umsatzeinbußen und Image-Schäden.

Die entscheidende Grundbedrohung, gegen die es in diesem Fall Maßnahmen zu ergreifen gilt, ist die Verletzung der Verfügbarkeit der Telekommunikationsleitung – und damit des Telekommunikationsnetzes.

Szenario 2

Zum Angreifen eines Kommunikationsnetzes kommen zwei mögliche Angriffspunkte in Frage: die Leitung selbst und die Netzknoten (z. B. Vermittlungsstellenrechner).

Desgleichen kann der Angriff verschiedene Ziele haben. Zum einen kann ein Angreifer es auf vertrauliche Daten abgesehen haben, um damit das angegriffene Unternehmen per Erpressung oder Preisgabe an Konkurrenten bzw. die Öffentlichkeit zu schädigen. Ein anderes Ziel wäre das mutwillige Beeinflussen der Verfügbarkeit des

Netzes bzw. der Daten. Hierbei legt der Angreifer entweder das Netz durch Überlastung lahm oder er modifiziert bzw. löscht die übertragenen Daten.

In diesem Szenario spielen folglich alle drei Grundbedrohungen eine Rolle.

Szenario 3

Neben dem Angriff auf das Netz an sich ist auch ein direkter Angriff auf ein im Netz befindliches IT-System möglich. Hierbei benutzt der Angreifer das Kommunikationsnetz als Hilfsmittel für seine Tat, die ein Verändern, Löschen oder Stehlen von Daten zum Gegenstand haben kann. Das Verhängnisvolle an einem Datendiebstahl ist, daß er nicht sofort bemerkt

wird, da die Daten nicht physikalisch gestohlen, sondern nur kopiert wurden. Werden die Daten nicht auf irgendeine Weise veröffentlicht oder auf andere Art gegen den Angegriffenen verwendet, bleibt ihm eventuell lange verborgen, daß etwa ein Mitbewerber viel mehr über ihn weiß, als er denkt.

In diesem Fall gezielte Maßnahmen zu ergreifen heißt, etwas gegen die Grundbedrohungen, Verletzung der Vertraulichkeit und Verletzung der Integrität, zu unternehmen.

Wie kann man sich schützen?

Um beliebige Maßnahmen ergreifen zu können, muß zunächst einmal die Situation und damit die Schutzbedürftigkeit der Daten und IT-Systeme eines Unternehmens untersucht werden. Insbesondere stellen sich folgende Fragen:

- Wie abhängig ist das Unternehmen von der Datenverarbeitung bzw. von den Netzen?
- Welche Anforderungen werden an die Vertraulichkeit, Integrität und Verfügbarkeit gestellt?
- Welche Maßnahmen sind bereits vorhanden?
- Welches Restrisiko ist vorhanden – wieviel davon kann bewußt getragen werden?
- Welche Maßnahmen müssen noch getroffen werden?

Beim Ergreifen von Maßnahmen muß anschließend beachtet werden, daß diese nur in einer für sie günstigen Umgebung greifen. Das heißt, daß technische Maßnahmen meist nicht ausreichen – es müssen Änderungen in der Organisation (Aufbauorganisation) bzw. den organisatorischen Abläufen (Ablauforganisation) vorgenommen werden.

Ein Beispiel hierfür ist die Erstellung einer Netzwerksicherheitspolitik, die u. a. die Struktur der Sicherheitslevel in den Abteilungen definiert, d. h., die angibt, wer welche Daten lesen oder schreiben darf.

Ein weiteres Beispiel ist die Schaffung einer Planstelle des IT-Sicherheitsbeauftragten. Um die IT-Sicherheit durchgängig zu konzipieren, bedarf es der Initiierung eines kontinuierlichen IT-Sicherheitsprozesses, dessen Koordinierung und Kontrolle durch den IT-Sicherheitsbeauftragten wahrgenommen werden muß.

Je abhängiger ein Unternehmen von der Informationstechnik ist, desto größer sind auch die Risiken.

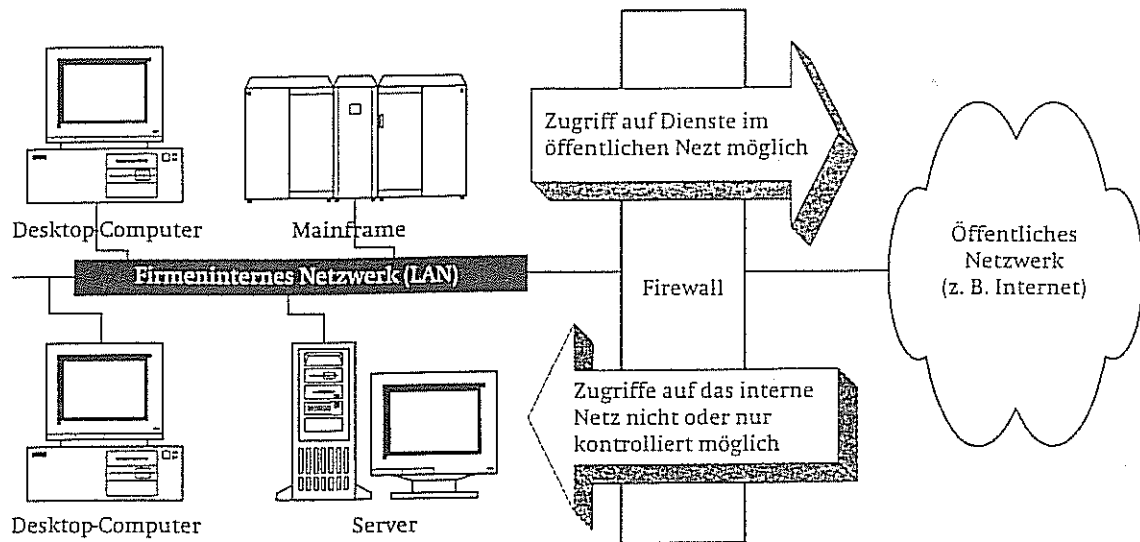


Abb. 2:
Sicherung des internen LANs durch ein Firewall-System

Eine generelle Anforderung an die zu treffenden Maßnahmen ist, daß sie einerseits mit der Unternehmenskultur konform sind und sich andererseits auch darin wiederfinden, um die Konformität zu wahren.

Konkrete Maßnahmen aus technischer Sicht gegen die Sicherheitsverletzungen der beschriebenen Szenarios wären im ersten Fall redundante Leitungen zur Ortsvermittlungsstelle bzw. sogar ein redundanter Anschluß, der zu einer anderen Ortsvermittlungsstelle führt.

Im zweiten Fall könnte die Verschlüsselung der Daten ein Abhören sinnlos machen. Als Optimallösung sollte ein Verfahren zum Einsatz kommen, das eine Kombination von Ende-zu-Ende- und Verbindungs-Verschlüsselung darstellt. So können die Daten einerseits nicht in den Vermittlungsstellen eingesehen werden und andererseits die Adressen (und somit der Datenverkehr an sich) nicht unnötig weit verfolgt werden. Außerdem sollte die Sicherheit des eingesetzten Verfahrens nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus, sondern lediglich auf der der Schlüssel (z. B. Paßworte) beruhen.

Im Fall des Einbruchs in ein Computersystem über ein Netz, an dem es angeschlossen ist, könnte ein sogenannter „Firewall“ einen Einbruch verhindern. Ein Firewall-System kontrolliert sämtliche Verbindungen von Rechnern des öffentlichen Netzes mit Rechnern im internen Netz (LAN) und schützt somit u. a. vor Angriffen wie dem Vorgeben einer falschen Identität („IP-Spoofing“) und dem Übernehmen von bereits aufgebauten Verbindungen durch einen Dritten („Hijacking“).

Das Firewall-System gibt somit die Möglichkeit, die Sicherheit des eigenen Netzwerkes zu gewähren und dabei den Zugang ins öffentliche Netz transparent zu halten.

Das Ziel einer Firewall-Installation ist es, daß kein Rechner im internen Netz eine direkte Verbindung in das öffentliche Netz aufbauen kann. Jede Verbindung wird von dem als „Dual-Homed-Gateway“ bezeichneten Bindeglied vermittelt. Hierdurch lassen sich an einem Ort sämtliche ein-

und ausgehenden Verbindungen kontrollieren und steuern.

Das Schema eines Firewall-Systems ist in der folgenden Abbildung dargestellt.

Warum wird nichts getan?

Das Problem an sich ist nicht, daß Unternehmen immer abhängiger von der Datenverarbeitung werden und Bedrohungen vorhanden sind, sondern daß nichts getan wird, um die Sicherheit zu erhöhen.

Welche Gründe hat diese Situation?

Einer der Hauptgründe ist sicherlich, daß trotz vermehrter Veröffentlichungen in der jüngeren Vergangenheit kein bzw. kein ausreichendes Sicherheitsbewußtsein vorhanden ist. Dieses dürfte unter anderem an der Komplexität der Materie liegen. Insbesondere für diejenigen, die über entsprechende Investitionen zu entscheiden haben, ist es oftmals zu aufwendig, den wirklichen Nutzen aus zu technisch und damit unverständlich formulierten Publikationen herauszufiltern.

Vielerorts wird auch argumentiert, daß bisher noch

nichts passiert ist und man noch mit Glück zwei Jahre überstehen kann, um dann das ersparte Geld in die IT-Sicherheit zu investieren. Sind diese zwei Jahre dann um und ist das Geld schon anderweitig ausgegeben, wird in gleicher Weise weiterargumentiert. Spätestens wenn etwas passiert ist dann guter Rat jedoch teuer.

Bei der IT-Sicherheit ist ähnlich wie bei Versicherungen und anderen reinen Vorsorge-Maßnahmen kein direktes Ergebnis von Investitionen zu sehen. Lediglich im Ausnahmefall zeigt sich, ob die „Hausaufgaben“ gemacht wurden oder nicht.

Als zusätzlicher Handlungsdämpfer in Sachen IT-Sicherheit kommt in Zeiten leerer Kassen und Sparmaßnahmen der Kostenfaktor hinzu. Gerade in solchen Zeiten lassen sich Kosten für Sicherheitsmaßnahmen gegen vermeintlich unrealistische Schäden schlecht vertreten.

Die anfallenden Kosten lassen sich in die vier Kategorien Projektkosten, Investitionen, Personal

Im Ausnahmefall zeigt sich, ob die „Hausaufgaben“ gemacht wurden.

und Administration sowie Schulung einordnen.

Projektkosten beziehen sich auf die Analyse des Ist-Zustandes (Schutzbedarfsfeststellung, Abhängigkeits- und Risikoanalyse) und die Pflege des Konzeptes, d. h. die Anpassung an Änderungen in der Systemumgebung.

Hat die Analyse Schwachstellen offenbart, ist anschließend in geeignete Maßnahmen zu investieren.

Die Kosten für Personal und Administration bezeichnen Kosten im Personalbereich für IT-Sicherheitsbeauftragte und die Administration der sicherheitsrelevanten Systeme – etwa Zugriffsschutz- oder Firewall-Systeme.

Wenn Maßnahmen zur Sicherung der Netze eingeführt werden, ist es für die optimale Nutzung ebenfalls notwendig, daß deren Benutzer adäquat geschult werden.

Fazit

Um dem Hauptproblem der IT-Sicherheit – dem fehlenden Bewußtsein – entgegenzutreten, ist es zwingend erforderlich, die Thematik aus der technischen Diskussion in die allgemeine Diskussion zu überführen. Genauso wie sich das Internet als das Computernetzwerk schlechthin von der Ebene der sich mit der Technik auskennenden Spezialisten zu einem Kommunikationsmedium für jedermann entwickelt hat, muß auch das Thema der IT-Sicherheit eine derartige Entwicklung erfahren.

Allerdings muß dieser Prozeß schnell gehen, um wenigstens ansatzweise mit der rasenden Ausbreitung des Internets Schritt halten zu können. Hierbei kann dann sogar die Panikmache in den Medien mit ihren meistens übertriebenen und sachlich falschen Beiträgen helfen – bringt sie doch das Thema der IT-Sicherheit mehr und mehr in das Bewußtsein der Öffentlichkeit.