

Gefahren sehen und bemessen

In diesem Kapitel möchte wir Ihnen die allgemeinen Gefahren, Bedrohungen und daraus resultierenden Risiken vor Augen führen, denen generell alle IT-Systeme unterliegen. Dazu betrachten wir die unterschiedlichen Angriffsarten und die mannigfachen potentiellen Angreifergruppen. Die juristischen Rahmenbedingungen auf Basis der für die IT-Sicherheit wichtigsten, in der Bundesrepublik Deutschland gültigen Gesetze und Verordnungen runden die Darstellungen dieses Kapitels ab.

Neue Geschäftsvorgänge und die Optimierung vorhandener Prozesse erfordern meist den Einsatz zusätzlicher IT-Komponenten in Form von zusätzlicher Software, Hardware oder einer Kombination aus beidem. Dieser Einsatz zusätzlicher und voneinander abhängiger technischer Komponenten erhöht ohne abgestimmte Planung zwangsläufig die Risiken, denen der Geschäftsbetrieb unterliegt. Daher ist vor dem Einsatz neuer Systeme eine Betrachtung der Gefährdungen dringend angeraten, die durch sie hervorgerufen werden.

Die Risiken der IT-Nutzung werden einschätzbar durch die nähere Betrachtung und detaillierte Analyse der auf ihrer Grundlage umgesetzten Geschäftsprozesse und Geschäftsvorfälle der jeweiligen Organisation. Die Analyse der IT-Dienste, die zur Bearbeitung der einzelnen Geschäftsvorfälle dienen, führt zu einer eingehenden Untersuchung der IT-Systeme und IT-Komponenten, auf die sie zu ihrer Ausführung zurückgreifen. Dies liefert bei adäquatem Detaillierungsgrad der Analyse eine angemessene und hinreichend verlässliche Benennung und Bewertung der relevanten Gefahren.

Zu Bedrohungsszenarien zusammengestellt bilden die Gefährdungen eine unverzichtbare Grundlage für die adäquate Sensibilisierung der beteiligten Entscheidungsträger. Sie bieten so die gemeinsame Grundlage für die effiziente Umsetzung des darauf aufbauenden IT-Sicherheitsprozesses.

1.1 Gefahren erkannt, Gefahr gebannt

Es hilft weder, Hysterien im Angesicht von unermesslichen Bedrohungen der IT-Systeme zu verfallen, noch den Kopf vor ihnen in den Sand zu stecken. Es gilt, den bestehenden Realitäten mit offenen Augen zu begegnen. Das Gefährdungspotential der eigenen Geschäftsprozesse durch den Einsatz von IT-Systemen ist ein wichtiger Einflussfaktor auf den gesamten IT-Sicherheitsprozess.

Das Gefährdungspotential eines IT-Systems ist über eine Gefahrenanalyse kategorisierbar. Mit einem deutlich höheren Aufwand wird es auch bemeßbar. Die Gefahrenanalyse betrachtet die IT-spezifische Gefährdung der relevanten Geschäftsprozesse und der einzelnen darin abgehandelten Geschäftsvorfälle über die eingesetzten IT-Systeme. Hier sind die wesentlichen wertschöpfenden Geschäftsvorfälle und die für ihre Umsetzung genutzten IT-Systeme und IT-Dienste zu identifizieren. Dies erfolgt mit logischer Analyse, Branchenvergleich und detaillierter Kenntnis der betrachteten Organisation. Für die auf diese Weise fokussierten betriebswichtigen IT-Komponenten sind nun die relevanten Bedrohungen zu ermitteln und als typische Bedrohungsszenarien zusammenzustellen und zu bewerten. Sind die drohenden Gefahren als Resultat der Gefahrenanalyse erkannt und benannt, so können auf Basis der Ergebnisse der Risikoanalyse die angemessenen, wirtschaftlich vertretbaren Sicherheitsmaßnahmen ausgewählt und definiert werden.

Dabei geben einschlägige Gefahren- und Maßnahmenkataloge Hinweise auf die typischen Bedrohungen und Bedrohungsszenarien. Diese Kataloge sind standardisierten Methoden und Vorgehensweisen zu entnehmen, zum Beispiel dem Grundschutzhandbuch und dem Sicherheitshandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI), der ISO 13335 und der ISO 17799 (vormals British Standards 7799) sowie der praktischen Erfahrung aus Branchenvergleichen, entsprechenden Anwendungen und vergleichbaren Aufgabenstellungen.

1.2 Allgemeine Risiken und Bedrohungen

Das generelle Ziel des IT-Sicherheitsprozesses ist das Erzeugen und Gewährleisten eines kalkulierbaren akzeptablen Sicherheitsniveaus der IT-Nutzung für den Geschäftsbetrieb der betrachteten Organisation. Daher werden wir uns in den folgenden Ausführungen auf Bedrohungen konzentrieren, die einen ursächlichen Zusammenhang mit dem Einsatz der Informationstechnologie haben.

Die der Bedrohung unterliegenden Wirtschaftsgüter sind entweder die IT-Komponenten selbst (IT-Systeme, Daten und Dienste) oder andere, durch einen erfolgreichen Angriff indirekt betroffene Wirtschaftsgüter, die für die betrachtete Organisation einen wirtschaftlichen oder immateriellen Wert darstellen. Zu diesen Gütern zählen Forschungs- und Entwicklungsdaten, Kalkulationen, Kundeninformationen, Mitarbeiterdaten sowie Information, die das Ansehen und die Integrität von Menschen und Institutionen beeinflussen. Diese Aufzählung ist nicht vollständig und sie werden Sie für ihre Organisation gewiss erweitern können.

Das BSI klassifiziert die Bedrohungen in seinem Grundschutzhandbuch in fünf Gefahrenkategorien:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen

- Technisches Versagen
- Vorsätzliche Handlungen

Höhere Gewalt umfasst Ereignisse, die sich den Einflussmöglichkeiten des Betroffenen entziehen. Typische Beispiele höherer Gewalt sind terroristische oder allgemein kriegerische Handlungen, Hochwasser oder Erdbeben.

Organisatorische Mängel entstehen als Resultat unzureichender Planung der betriebswirtschaftlichen Abläufe und Prozesse, Berichtsstrukturen oder Verantwortungs- und Gestaltungsbereiche. Organisatorische Mängel lassen sich an den Beispielen fehlender Notfallplanung, unzureichender Regelung zum Entzug der Zugriffsrechte für ausscheidende Mitarbeiter oder unzureichender Dokumentation illustrieren. Diese Mängel treten nach Erfahrung der Autoren mit recht hoher Häufigkeit in Analysen zu Tage. Es könnte für Sie lohnenswert sein, auch ihre Organisation auf diese Aspekte zu überprüfen.

Menschliche Fehlhandlungen führen aus Unwissenheit oder aus Böswilligkeit zu Schäden. Das BSI versteht unter menschlichen Fehlhandlungen zunächst nur die unwissentlich durchgeführten. Für die zweite Ausprägung definiert das BSI die eigene Kategorie »Vorsätzliche Handlungen«. Charakteristische Beispiele für (unwissentliche) menschliche Fehlhandlungen sind das unbeabsichtigte Löschen von Daten und Programmen, die Fehlkonfiguration von IT-Komponenten und die Fehlbedienung von Programmen.

Technisches Versagen entspringt dem Fehlverhalten von Hard- und Software. Es wird oft begünstigt durch hohe Komplexität des Schutzsystems, unzureichende Integration in die umgebene IT-Landschaft sowie Überlastung infolge mangelnder Sachkunde der Betreiber. Technisches Versagen zeigt sich oft im Ausfall von Netzteilen, im Absturz von Betriebssystemen und Applikationsprogrammen oder in der Störung von Kommunikations- und Übertragungswegen.

Vorsätzliche Handlungen können von allen Menschen ausgeübt werden, die – berechtigt oder unberechtigt – Zugriff auf die IT-Systeme oder IT-Dienste erlangen können. Der Täterkreis umfasst sowohl die Mitarbeiter der betrachteten Organisation, die sogenannten Innentäter, als auch Externe, die Außentäter.

Die kardinalen Ursachen für Gefahren liegen also bei Naturereignissen, dem Ausfall von Technik und bei Menschen, die willentlich oder unbewusst handeln und so negative Folgen hervorrufen oder nicht unterbinden.

Die Kommunikationssysteme, die IT-Systeme und IT-Dienste, sind also diversen externen Gefahren ausgesetzt. Zusätzlich gehen von den Kommunikationssystemen Gefährdungen für die anderen Komponenten, die die Organisation einsetzt, aus.

1.3 Bedrohungen eines IT-Systems

Die verschiedenen Arten der externen Bedrohungen stellt der folgende Abschnitt allgemein dar. Die aktiven Bedrohungen eines IT-Systems beruhen auf Angriffen, die erst durch die Nutzung eines IT-Systems auftreten. Dies sind in der Regel Angriffe auf die Informationen und Dienste, die das IT-System seinen Nutzern bietet. Für ein einheitliches Verständnis dieser Bedrohungen stellen wir im Folgenden zunächst dar, welche grundlegenden Ideen und Ansatzpunkte hinter der Ausprägung der einzelnen unterschiedlichen Angriffe stecken.

Ein Sender schickt dem Empfänger eine Nachricht. Der Empfänger wertet die Nachricht aus und reagiert auf sie durch ein zum Nachrichteninhalte passendes Verhalten.

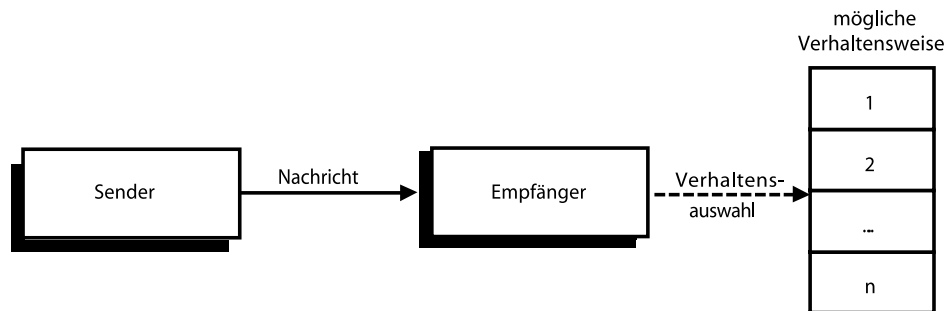


Abb. 1.1: Verhalten des Empfängers bei Erhalt einer Nachricht

Hört ein Angreifer die Kommunikationsverbindung zwischen Sender und Empfänger ab, so kann er die ausgetauschten Nachrichten mitlesen und interpretieren. Ferner erkennt und analysiert er das daraus resultierende Verhalten des Empfängers. Er ist damit in der Lage, den Nachrichten die zugehörigen Reaktionen der Kommunikationspartner zuzuordnen. Er kann aus dieser Korrelation die Reaktion des Empfängers in Grenzen vorhersagen. Er kann in dieser ersten passiven Angriffsart die Reaktion jedoch weder aktiv beeinflussen, noch das Reaktionsmuster verändern.

Vermag der Angreifer zusätzlich die Nachrichten zu manipulieren, so ist er in der Lage, die Reaktionen des Empfängers zielgerichtet zu beeinflussen. Diese aktive Manipulation kann durch das Abfangen oder das Wiederholen ganzer Nachrichten sowie durch die Veränderung, die Löschung von Nachrichtenteilen, Generierung falscher Nachrichtenteile und durch das Einspielen gänzlich neuer Nachrichten erfolgen. Ferner kann der Angreifer durch fortgesetzte Nachrichtenmanipulation auch das Reaktionsmuster des Empfängers beeinflussen und bei strategischem Vorgehen sogar aktiv zielgerichtet verändern.

Aus dieser Überlegung heraus unterscheiden wir zwei grundlegende Bedrohungsarten:

- *passive Angriffe* und
- *aktive Angriffe*

1.3.1 Passive Angriffe

Der passive Angriff erfolgt ohne Modifizierung der übertragenen Nachrichten. Hierbei beeinflusst der Angreifer den Betrieb der betrachteten IT-Systeme nicht oder zumindest nicht merkbar. Er führt einen passiven Angriff im Regelfall willentlich und gezielt durch. Sein Ziel ist die Erlangung wertvoller geheimer Informationen. Dies führt er meist in unzulässiger, strafbarer Weise aus. Ein passiver Angreifer bleibt oft gänzlich oder zumindest für lange Zeit unentdeckt und kann so latent über einen längeren Zeitraum großen Schaden anrichten.

Der Angreifer führt passive Angriffe mit Abgreifklemmen oder Induktionsschleifen an den Netzkabeln und mit Anlagen zum Auffangen der Abstrahlung von Monitoren und LCDs durch. Recht bequeme Angriffswege bietet ihm modifizierte Software, die die Kommunikationsströme kopiert, und die Nutzung drahtloser Netzwerke, die nach den Erfahrungen der Autoren zurzeit noch völlig unzureichend geschützt sind.

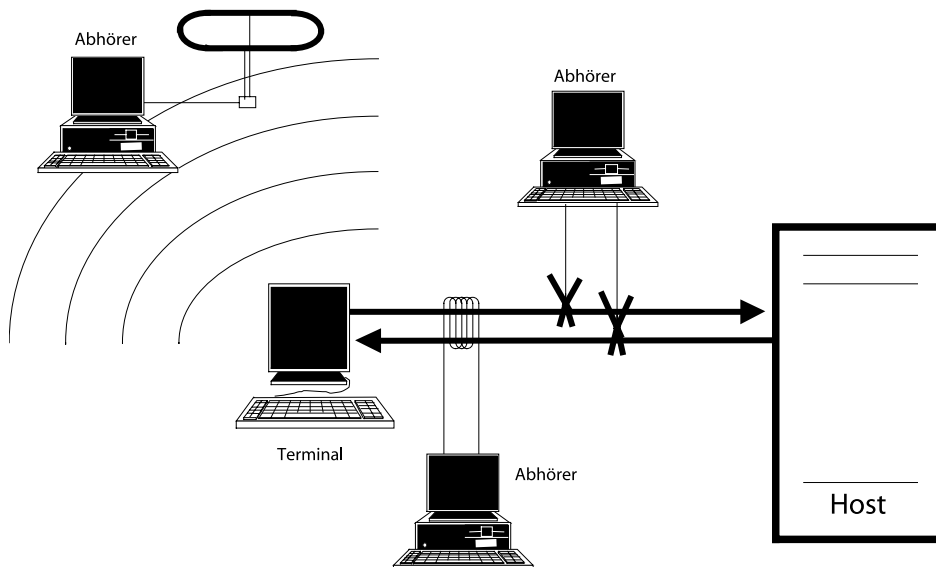


Abb. 1.2: Abhören von Informationen

Passive Angriffe sind in ihrer Zielrichtung und Angriffsart unterscheidbar:

- Abhören der Kommunikation
- Ausforschen der Kommunikationspartner
- Analyse des Kommunikationsflusses

Abhören der Kommunikation

Beim Abhören der Kommunikation gelangt der Angreifer auf dem Übertragungsweg an den Informationsinhalt. Er kann sie als unberechtigter Lauscher zu seinen Zwecken verwerten. Hierbei ist das Kommunikationsmedium selbst sein Angriffsobjekt.

Dies illustrieren die folgenden Beispiele:

- Der Angreifer zeichnet die Faxübertragung eines Angebots auf. Er ist damit in der Lage, das Angebot mitzulesen. Dies gibt Mitbewerbern die Gelegenheit, ein attraktiveres Angebot zu unterbreiten.
- Der Angreifer gelangt an Konto- und Autorisierungsdaten, die eine Funktastatur dem PC einer Bank – und ihm – sendet. Er verschafft sich auf diese Weise die notwendigen Kenntnisse für eine unberechtigte Zugriffsautorisierung im Rahmen eines späteren aktiven Angriffs.
- Der Angreifer liest über die Abstrahlungen der Kathodenstrahlröhre oder das LCD-Display des Monitors die darauf abgebildeten Informationen mit. Er kann dem berechtigten Nutzer so elektronisch »über die Schulter schauen«. Dabei steht er mit seiner Abhöreranlage in einem Fahrzeug auf der Straße vor dem Gebäude.
- Der Angreifer liest die unverschlüsselte Login-Prozedur beim Aufbau einer Verbindung zwischen einem Datenbanksystem und einem Abfrageterminal mit. Er gelangt so in den Besitz einer gültigen Benutzerkennung nebst zugehörigem Passwort. Damit ist er in der Lage, später jederzeit aktiven Zugriff auf die Dienste des Verarbeitungsrechners zu erlangen – mit den vollen Zugriffsrechten des eigentlichen Nutzers.

Ausforschen der Kommunikationspartner

Das Ausforschen der Kommunikationspartner ist die Vorstufe einer umfassenden Kommunikationsflussanalyse. Die Angriffsart erlaubt auch ohne Kenntnis des eigentlichen – möglicherweise verschlüsselten – Nachrichteninhalts Rückschlüsse auf den Nachrichteninhalt. Sie gewinnt ihre Erkenntnisse aus der Ermittlung der Identität der Kommunikationspartner.

Die Kenntnis über die Kommunikationspartner erlangt der Angreifer beim Abhören des Kommunikationsflusses. Selbst bei verschlüsselten Nutzdaten müssen die

für die Kommunikation genutzten Datenpakete genügend Routing-Informationen für ihre Weiterleitung an den gewünschten Kommunikationspartner besitzen. Diese Informationen, zum Beispiel die IP-Adressen der Kommunikationspakete, lassen einen Rückschluss auf die Identität oder zumindest die Gruppenzugehörigkeit der Kommunikationspartner zu. Daraus kann der Angreifer auf die Kommunikationsbeziehung und im Weiteren oft sogar auf die Kommunikationsinhalte schließen.

So ist zum Beispiel der Telefonanruf unter der Nummer 112 mit hoher Wahrscheinlichkeit ein Notruf und der Anruf eines Kassierers bei der Genehmigungsstelle einer Kreditkartengesellschaft lässt auf einen größeren Einkauf schließen. Nachrichten an die Adhoc-Publizitätsstelle der Börse enthalten mit hoher Wahrscheinlichkeit kursbeeinflussende Informationen über das Unternehmen, das sie verschickt. Nachrichten eines Angriffserkennungssystems an das zugehörige Managementsystem berichten in der Regel von erkannten Unregelmäßigkeiten, Angriffsmustern oder Angriffsquellen.

Analyse des Kommunikationsflusses

Die Analyse des Kommunikationsflusses gibt dem passiven Angreifer auch bei Einsatz der wirksamsten Verschlüsselungsverfahren Informationen über Zeitpunkte, Kommunikationsvolumina, Art und Richtung des Datentransfers. Diese Informationen können – mit anderen Informationen zusammengeführt – recht aussagekräftig sein.

So lässt ein hohes Kommunikationsaufkommen zwischen den Vorständen unterschiedlicher Unternehmen auf eine in Zukunft verstärkte Kooperation schließen. Die Häufigkeit des Abrufs von Detailinformationen zu einem Produkt oder zu einer Dienstleistung erlaubt Rückschlüsse auf das Kaufinteresse und die ersten ausgetauschten Nachrichten bei der Kommunikationsaufnahme sind in der Regel Login-Informationen.

Spezielle Gefahren beim Einsatz lokaler Netzwerke

Lokale Netzwerke nutzen häufig Broadcastverfahren für die Nachrichtenübermittlung. Hier werden die Nachrichten über das Kommunikationsmedium stets an alle Teilnehmer gesendet. Diese vertrauensvolle Übertragung setzt voraus, dass die angeschlossenen Kommunikationspartner nur diejenigen Nachrichten verwerten, die auch ihnen zgedacht sind.

Viele Lokale Netzwerke sind so konzipiert, dass im laufenden Betrieb zusätzliche Anschlüsse installiert und deinstalliert werden können, ohne den Datenverkehr erkennbar zu stören. In der Praxis sind meist vorausschauend zusätzliche Anschlussdosen für das Netzwerk eingerichtet, die zunächst nicht genutzt werden. Dies schafft Flexibilität für die Umnutzung von Räumen und die Möglichkeit,

zusätzliche IT-Systeme bei Bedarf ohne Unterbrechung des Netzwerkbetriebs anzuschließen.

Falls diese ungenutzten Anschlussdosen nicht verlässlich gesperrt sind, kann ein Angreifer sie jederzeit für seine Zwecke nutzen. In diesen Fällen betreibt der Angreifer über die nicht blockierten Anschlussdosen Analysegeräte, die den gesamten Nachrichtenstrom mitverfolgen und die für den Angriff relevanten Informationen herausfiltern, auswerten und aufzeichnen.

Bei den drahtgebundenen lokalen Netzwerken muss der Angreifer einen direkten physikalischen Zugang zum Netzkabel erlangen. Drahtlose Netze wie das immer weiter verbreitete WLAN ermöglichen Abhören sogar ohne direkten Zugang in die Gebäude und ohne physischen Zugriff auf die dort verlegten Kabel und Anschlüsse. Die bislang etablierten Schutzmaßnahmen und Sicherheitsstandards gewährleisten keinen hinreichenden Schutz. Die Erfahrung der Autoren zeigt zusätzlich, dass selbst der unzureichende Schutz oftmals durch Fehlkonfiguration der Netzwerkkomponenten aus Unkenntnis der Betreiber unwirksam bleibt.

Die Flexibilität und Robustheit der Netzwerkarchitektur wird aus Sicht der Datensicherheit in beiden Fällen, sei es drahtlos als auch drahtgebunden, zu einem erheblichen Gefährdungspotential. Sie erleichtert die unbemerkte unbefugte Installation zusätzlicher IT-Systeme mit Abhörfunktionalität.

Aber auch die zulässig installierten IT-Systeme nutzen Angreifer zum Abhören des gesamten Nachrichtenstroms. Ihnen genügt eine zusätzliche Software, die eine ordnungsgemäß installierte Netzwerkkarte des IT-Systems in ein Abhörgerät verwandelt. So kann der Angreifer zum Beispiel auf einfache Weise in den Besitz sämtlicher unverschlüsselt übertragenen Benutzerkennungen nebst den zugehörigen Passwörtern gelangen. Dieses unzureichende Sicherheitsniveau zahlreicher lokaler Netze gefährdet die Wirksamkeit des gesamten Zugangs- und Zugriffsschutzes für die unternehmenswichtigen IT-Systeme und IT-Dienste.

Weitere neuralgische Gefahrenpunkte in lokalen Netzen, an denen Angreifer bequem die Nachrichten abhören, sind die Kommunikationsrechner, die die Nachrichten weiterleiten. Dies umfasst Bridges, Router, Switches, Brouter sowie Gateways. Schlecht gesicherte Fernwartungsfunktionen dieser aktiven Netzwerkkomponenten bieten dem Angreifer den idealen und zugleich bequemsten Lauschposten.

1.3.2 Aktive Angriffe

Neben der Gefährdung durch passives Abhören unterliegen die Kommunikationsströme auch der Bedrohung durch aktive Angriffe. Hier manipuliert der Angreifer den Nachrichtenstrom oder er beeinflusst die Verfügbarkeit und Konsistenz der IT-Systeme und IT-Dienste.

Der aktive Angreifer greift direkt in den Kommunikationsstrom oder in eine der Kommunikationskomponenten ein und verfälscht die zu übertragenden Daten. Er setzt seine Angriffe physisch durch das Auftrennen des Kommunikationsmediums oder softwarebasiert durch den Eingriff in die Programme der aktiven Kommunikationskomponenten um. Der aktive Angreifer verursacht Veränderungen. Das bietet im Gegensatz zum passiven Angriff konkrete Ansatzpunkte für eine zeitnahe Erkennung des Angriffs. Diese schnelle Erkennung ist die unverzichtbare Grundlage für eine wirksame Reaktion durch prompte angemessene Gegenmaßnahmen.

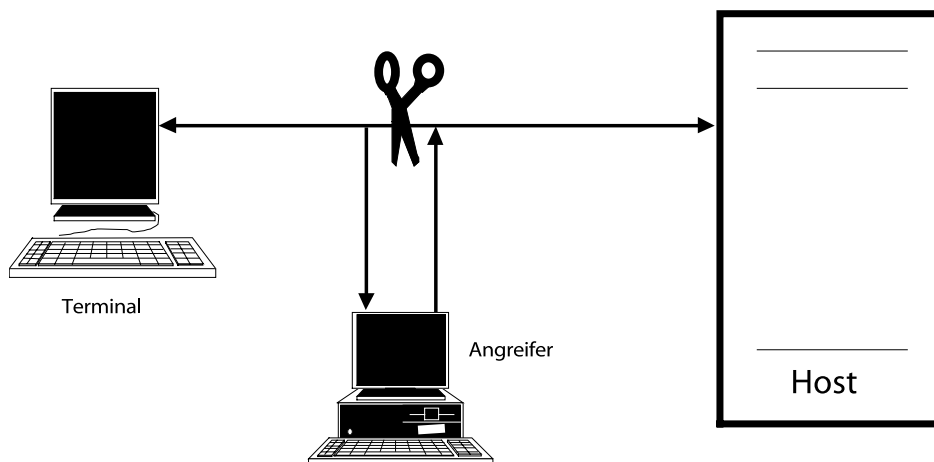


Abb. 1.3: Aktiver Angriff

Bei der Gruppe der aktiven Angreifer lassen sich zwei Grundtypen unterscheiden:

- unbefugte externe und
- berechnete interne Kommunikationspartner

Die Angriffe durch berechnete Kommunikationspartner sind deutlich schwerer von der berechtigten Nutzung zu unterscheiden als die aktiven Angriffe externer unberechtigter Nutzer. Die internen aktiven Angriffe lassen sich so nur mit größerem Aufwand, verbunden mit einem schlechteren Erkennungsgrad, lokalisieren und abfangen. Hat ein Kommunikationspartner die Zugriffsberechtigung erlangt, so ist sein Verhalten kaum mehr vom zulässigen Regelverhalten unterscheidbar. Die Abgrenzung zwischen der berechtigten Nutzung und dem Missbrauch ist nur für wenige explizit benannte IT-Dienste und dort nur mittels aufwendiger Analyseverfahren möglich.

Angriffe externer, unberechtigter Kommunikationspartner lassen sich hingegen einfacher automatisch erkennen und bewerten. Sie sind durch technische Sicherheitsmechanismen meist in gewünschtem Maß in Griff zu bekommen.

Aktive Angriffe können auf vielfältige Weise erfolgen. Der Angriffsort kann entweder auf dem Übertragungsweg oder auf den IT-Systemen der Kommunikationspartner, also beim Sender oder beim Empfänger, liegen. Nachrichten können als Ganzes oder in Teilen manipuliert werden. Typische aktive Angriffe sind:

- Dienst- und Kommunikationsunterbindung
- Nachrichtenverzögerung
- Wiederholungsangriffe
- Nachrichtenverfälschung

Dienst- und Kommunikationsunterbindung (Denial of Service)

Die zeitweilige oder kontinuierliche Unterbindung des IT-Dienstes oder der Kommunikation ist eine der bekanntesten aktiven Angriffsarten. Sie wird meist mit dem englischen Fachbegriff »denial of service« benannt. Hier stört der Angreifer den Transfer einzelner oder zahlreicher Nachrichten. Dies erfolgt entweder durch den störenden Zugriff auf das Kommunikationsmedium oder auf die an der Kommunikation beteiligten IT-Systeme.

Typische Beispiele hierfür sind das Abfangen von Alarmmeldungen eines Angriffserkennungssystems oder das Unterbinden der Kommunikation von Sicherheitssystemen mit ihren externen Logservern und Managementsystemen durch eine Überlastung der Kommunikationswege.

Nachrichtenverzögerung

Die gezielte Verzögerung von Nachrichten bewirkt in zeitkritischen Kommunikationssystemen die Hemmung von Nachrichtenflüssen bis zu deren vollständiger Blockade. Dazu nutzt der Angreifer die Timing- und Lawineneffekte der Protokolle und der IT-Systeme aus.

Wiederholungsangriffe

Eine weitere Angriffsart ist der Wiederholungsangriff. Hier sendet der Angreifer dieselbe Nachricht mehrmals. Als Beispiel sei die mehrfache Übertragung eines Überweisungsauftrags genannt. Auf diese Weise kann der Angreifer die mehrfache Durchführung der Überweisung bewirken.

Nachrichtenverfälschung

Der Angreifer verändert die Dateninhalte der Nachrichten. Auf diese Weise kann er Daten manipulieren, Kommunikationsprotokolle nachhaltig stören und letztlich die Bearbeitung der Geschäftsvorfälle hemmen.

Die Verfälschung von Daten lässt sich auch am elektronischen Überweisungsauftrag illustrieren, hier in Form einer Änderung der Kontodaten und des Betrags. Auf diesem Weg kann der Angreifer den von ihm gewählten Betrag auf das von ihm gewünschte Konto überweisen.

Ein weiteres typisches Beispiel ist die Übernahme einer aktiven Kommunikationsverbindung nach dem erfolgreichen Login, das sogenannte Session-Highjacking. Hier übernimmt der Angreifer die Verbindung eines berechtigten Nutzers. Er sendet dem Nutzer nach dessen erfolgreicher Authentisierung auf dem gewünschten IT-Dienst eine Session-Ende-Nachricht. Zeitgleich greift er die so freiwerdende Session auf und lenkt dabei die Antwortnachrichten des IT-Dienstes auf seinen Rechner um. Er ist so in der Lage, mit dem Rechteprofil des authentisierten Nutzers die IT-Dienste in Anspruch zu nehmen.

Selbst in Hochgeschwindigkeitsnetzen sind solche aktiven Angriffe technisch möglich. Hierzu trennt der Angreifer den Datenstrom physisch oder logisch an einer aktiven Kommunikationskomponente auf. Diese Kommunikationskomponente beherrscht zu beiden Seiten das Medium Access Protokoll der durch sie verbundenen Netze. Sie nimmt dazu eine kurzzeitige Zwischenspeicherung und Auswertung der Nachrichten vor, die der Angreifer lesen und manipulieren kann. Die Überwachungstimer der Übertragungsprotokolle, zum Beispiel des Logical Link Controls, und erst recht der höheren Schichten sind dabei so großzügig eingestellt, dass für die Manipulation und passende Neuberechnung der meist vorhandenen Prüfsummen genügend Zeit besteht.

Hieraus wird deutlich, dass jede aktive Netzwerkkomponente, in der eine Zwischenspeicherung erfolgt oder erfolgen kann, ein hohes Gefahrenpotential für aktive Angriffe darstellt. Dies gilt speziell für sämtliche Bridges, Router, Gateways, Server und sonstige Vermittlungsknoten. Aktive Angriffe sind immer dort möglich, wo der Angreifer die Hard- oder Software in den Kommunikationskomponenten nach seinen Bedürfnissen und Anforderungen ändern kann.

Missbräuchliche Nutzung von IT-Diensten und Daten

Vortäuschen einer falschen Identität Wenn sich ein unberechtigter Angreifer in einer der zuvor aufgezeigten Weisen für einen anderen, berechtigten Kommunikationspartner ausgibt, so kann er Informationen und Dienste erschleichen, die nicht für ihn bestimmt sind. Er gelangt so in die Lage, Aktionen auszulösen, die eigentlich nur von den dazu berechtigten Nutzern ausgelöst werden können.

Ein besonders anschauliches Beispiel für Schäden, die durch das Vortäuschen einer falschen Identität entstehen, ist die Bestellung von individuell anzufertigenden Gütern. Die fälschlich bestellten und nicht benötigten Waren erzeugen Schäden durch die verschwendeten Materialien und die blockierte Fertigung und Logistik.

Eine manipulierte E-Mail mit gefälschtem Absender kann auf ähnliche Weise erhebliche Schäden anrichten. Diese Schäden liegen zwischen Verwirrung, falls die manipulierte Mail rechtzeitig als solche erkannt wird, bis zu Vertrauensschäden, Reputationsverlust und unnötigen beziehungsweise schädlichen Aktionen, die durch die E-Mail veranlasst wurden. Wenn sich ein Angreifer als berechtigter Forschungs- oder Vertriebsmitarbeiter ausweist, kann er sich geheime, für die Organisation lebenswichtige Informationen verschaffen. Auf diese Weise werden Forschungs- und Marketingetats mehrerer Jahre vergeudet.

Besonders leicht fällt das Vortäuschen einer falschen Identität bei Authentifizierungsverfahren, die auf den leicht verfälschbaren IP-Netzwerkadressen beruhen oder die eine unverschlüsselte Übermittlung von Benutzername und Passwort vorsehen.

Leugnen eines Kommunikationsvorgangs

Auch bei einer eigentlich korrekten, technisch unbeeinflussten Kommunikation können sowohl der Urheber als auch der Empfänger einer Nachricht die erfolgte Kommunikation leugnen. Der Absender einer Bestellung kann beispielsweise die Urheberschaft abstreiten. Der Empfänger kann den Empfang einer Nachricht, zum Beispiel einer Vertragskündigung, in Abrede stellen.

1.3.3 Unbeabsichtigte Verfälschung

Neben der Gefährdung durch passive und aktive Angriffe, die einem IT-System drohen, gibt es auch unbeabsichtigte, zufällige Verfälschungen. Typische Ausprägungen dieser unbeabsichtigten Verfälschungen sind

- Übertragungsfehler
- Fehlübermittlung von Nachrichten
- Softwarebugs
- Hardwarefehler
- Umwelteinflüsse
- Fehlbedienung

stellung verwendeten Methodik bestimmt. Zu den Rahmenbedingungen zählen zu oft der Zeitdruck und die beständig wachsende Komplexität der Softwarepakete. Dies provoziert geradezu Fehler.

Zeitdruck beschränkt die Programmierer auf das für sie Unverzichtbare, die Codeerstellung. Dem Zeitdruck wird zuerst die Dokumentation geopfert, die anderen Projektmitarbeitern das detaillierte Verständnis und damit die lückenlose Übernahme der Programmierfähigkeit ermöglicht. Danach spart man an Tests und hinreichenden Testszenarien. Bei vielen der aktuellen Softwarepakete ist aufgrund ihrer Komplexität ein vollständiger Test mit allen Konstellationen der Inputdaten in endlicher Zeit gar nicht mehr möglich. Der Großteil der eingesetzten Software wird nicht mit formalen Methoden überprüft. Software ist im Regelfall nicht durch externe Gremien verifiziert und zertifiziert.

Aus diesen Gründen ist bei jedem Softwarepaket von Programmierfehlern auszugehen, die mehr oder weniger bedeutungsvolle Fehlfunktionen verursachen. Diese Fehlfunktionen können Daten verändern, unberechtigten Zugang zu vertraulichen IT-Diensten und IT-Daten schaffen oder IT-Dienste unterbrechen. Dies gefährdet in erheblichem Umfang die Organisation, in der die Software eingesetzt wird.

Hardwarefehler

Jede Hardware eines IT-Systems hat eine begrenzte Nutzungsdauer. Am Ende der Nutzungsdauer nimmt die Fehlerhäufigkeit drastisch zu. Ferner ist in der Inbetriebnahmephase mit einer deutlich höheren Fehlerrate zu rechnen. Dies visualisiert Abbildung 1.5.

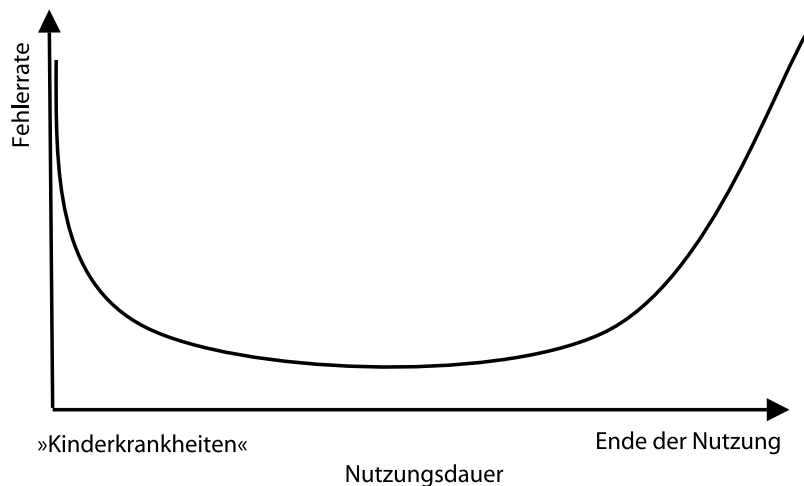


Abb. 1.5: Fehlerrate vs. Nutzungsdauer

Die Einflüsse der Betriebsumgebung wie Überspannung, Stromausfälle, zu hohe oder zu niedrige Temperaturen, Erschütterungen, Schwingungen etc. beschleunigen Hardwareausfälle. Häufig betroffen sind hier die Netzteile der IT-Systeme, die Kommunikationsschnittstellen sowie die beweglichen Teile.

Umwelteinflüsse

Blitzschläge verursachen Überspannung auf den Kommunikations- und Versorgungsnetzen der IT-Systeme. Funkübertragungen werden durch kosmische und solare Strahlung beeinträchtigt. So können Kurzwellenübertragungen bestimmter Wellenlänge in Abhängigkeit von der Sonnenaktivität unmöglich werden. Geostationäre Satelliten sind nicht ungestört nutzbar, solange sie aus der Sicht der Empfangsstation genau vor der Sonne stehen. Die Information, die auf Speicherchips auf Satelliten zwischengespeichert wird, ist speziell gegen Bitfehler aufgrund der kosmischen Strahlung und des Sonnenwinds zu schützen.

Bedienfehler

Bedienfehler resultieren aus Unkenntnis, mangelnder Konzentration oder unzureichender Sensibilisierung der Nutzer des IT-Systems. E-Mails mit vertraulichem Inhalt werden von einem Mitarbeiter unverschlüsselt über das Internet versandt. Firewall-Systeme werden für einen befristeten Installations- oder Wartungsvorgang auf vollständigen Durchlass geschaltet, nach Abschluss der Arbeiten aber weiter unnötig offen gehalten. Virenschutzsysteme werden installiert, aktuelle Erkennungsmuster aber erst nach einem halben Jahr eingespielt. Ein besonders wichtiges Fax wird an eine falsch eingegebene Faxnummer übermittelt.

1.3.4 Spezifische Bedrohungen der Endsysteme

Besonders lohnende Angriffsziele stellen neben den zentralen IT-Servern auch die Endgeräte dar. Dies sind zurzeit meist PCs, die als Software neben dem Betriebssystem anwendungsspezifische Applikationsprogramme enthalten. Sie weisen meist als Folge historischer Entwicklung eine große Anzahl und Vielfalt auf. Viele verantwortliche Systemadministratoren brandmarken diesen Zustand als »Hardware- und Softwarezoo«. Für sie ist eine solche Ansammlung diverser Endgeräte mit unterschiedlichsten IT-Komponenten erheblich aufwändiger sicherheitstechnisch zu betreuen als die überschaubaren zentralen IT-Systeme.

Die in den vorhergehenden Kapiteln benannten Angriffsszenarien sind unter diesen Rahmenbedingungen um Größenordnungen Erfolg versprechender anzuwenden. Eine steigende Anzahl der Angriffe richtet sich so gegen die Endsysteme und die auf ihnen verfügbaren IT-Dienste. Auf diese Weise nutzt der Angreifer nach erfolgreichem Angriff des Endgeräts dieses als Relaisstation für seine Angriffe auf die zentralen IT-Systeme und IT-Dienste.

Zu den typischen Bedrohungen der Endsysteme zählen

- Technische Defekte
- Fehler in Handhabung und Administration
- Falsche Planung der Prozesse und Verantwortungsbereiche
- Gesetzwidrige Handlungen

Technische Defekte

Unter technischen Defekten fassen wir solche Fehler der Endsysteme zusammen, die aufgrund der Unzulänglichkeit der eingesetzten Komponenten im Endsystem und dessen Umgebung auftreten. Solche technischen Defekte können sein:

- Betriebssystemfehler, die Daten/Programme zerstören oder Schwachstellen für Angreifer bieten
- Programmfehler, die Daten beschädigen oder Schwachstellen für Angreifer bieten
- Hardwareausfälle, die Daten zerstören
- Stromausfälle, in den Ausprägungen Kurz- und Langzeit-Stromausfall
- Umwelteinflüsse wie Brand oder Wassereintritt
- elektrostatische Aufladung

Fehler in der Nutzung und Administration

Nutzungs- und Administrationsfehler sind solche Fehler, die aufgrund fehlerhafter, nicht ordnungsgemäßer Handhabung des Endsystems durch seine Nutzer oder seine Administratoren auftreten. Solche Handhabungsfehler sind typischerweise:

- Nicht planmäßiger Programmabbruch, zum Beispiel durch vorzeitiges Ausschalten der Hardware
- Fehler, die im Rahmen von Service- oder Wartungsarbeiten verursacht werden und Daten beziehungsweise Programme beschädigen
- Nutzungsfehler, bei denen Daten beschädigt oder zerstört werden
- Fehler, die aus unzulässiger Dateneingabe resultieren
- Liegen lassen von Ausdrucken oder Testdaten
- Liegen lassen von Passwörtern

Falsche Planung der Prozesse und Verantwortungsbereiche

Fehler in der Planung der Prozesse und Verantwortungsbereiche resultieren aus unzureichender Planung der sicherheitsrelevanten Prozesse und falscher Definition der Verantwortungsbereiche. Typische Fehler dieser Art sind:

- Fehlende personelle Trennung von administrativen und überprüfenden Funktionen
- Fehlende regelmäßige Kontrolle der Funktionsfähigkeit und Wirksamkeit der Systeme
- Unzureichende Qualifikation oder Sensibilisierung der Akteure
- Fehlende Prüfung des Qualifikationsniveaus
- Unwirksame oder nicht vorhandene Stellvertreterregelungen
- Unzureichende Dokumentation der IT-Systeme und Kommunikationskonstellationen
- Wildwuchs an Softwarekonfigurationen
- Unzulänglich definierte Prozesse beim Funktionswechsel von Mitarbeitern (Informationsübergabe und Aktualisierung der Zugangs- und Zugriffsrechte)
- Fehlende Prozesse zur sicheren Hinterlegung von Passwörtern und anderen Zugangs- und Zugriffsschutzsystemen

Gesetzwidrige Handlungen

Unter gesetzwidrigen Handlungen fassen wir die Aktivitäten zusammen, die ein Angreifer bewusst gesetzübertretend begeht, um sich selbst oder anderen Gewinn zu verschaffen oder den berechtigten Nutzern des IT-Systems zu schaden.

Die Motivationen solcher krimineller Aktivitäten sind nach Untersuchungen der Data Processing Management Association (H. Abel und W. Schmolz, Datensicherung für Betriebe und Verwaltung, Verlag Beck, 1987):

- mangelhaftes Berufsethos: 27 %
- Spieleidenschaft: 26 %
- persönlicher Gewinn: 25 %
- Rache: 22 %

Ein weiteres erschreckendes Ergebnis von Untersuchungen zur Computerkriminalität ist, dass die meisten Angriffe (bis zu 98% der Fälle) nicht von Außenstehenden begangen wurden, sondern durch Personen der eigenen Organisation erfolgten.

Zu den wichtigsten in diesem Zusammenhang auftretenden Angriffsarten zählen:

- Manipulation von Daten
- Modifikation der Software
- Daten- und Softwarediebstahl
- Daten- und Softwarte kidnapping
- Sabotage und Vandalismus

Im Folgenden gehen wir näher auf die einzelnen Angriffsarten ein:

Manipulation von Daten

Diese Angriffsart dient der ungerechtfertigten Bereicherung oder der unzulässigen Schädigung. Die manipulierten Daten haben für den Betreiber eines IT-Systems einen bestimmten Informationsgehalt und stellen so einen definierten Wert dar. Typische Beispiele sind hierfür:

- personenbezogene Daten
- firmeninterne Daten wie aktuelle Planung, Leistungsdaten etc.
- kritische Arbeitsdaten wie Kundenstammdaten, Abrechnungsdaten etc.

Ein Anwender verändert die Zeiterfassungsdaten, um sich oder andere zu bevorteilen. Ein Nutzer löscht Daten seines Kommunikationsaufkommens und verringert so die Höhe seiner Kommunikationsrechnung. Ein Konkurrent verfälscht eine E-Mail, um den Absender zu diskreditieren.

Modifikation der Software

Der Angreifer verfälscht die Software gezielt und absichtlich. Er führt seinen Angriff so durch, dass seine Aktionen nicht auf ihn zurückführbar sind. Der Zweck eines solchen Angriffes ist die ungerechtfertigte Bereicherung des Angreifers oder die Absicht, dem Betreiber des IT-Systems oder einem Dritten Schaden zuzufügen.

Es gibt zahlreiche Ausprägungen eines solchen Angriffes:

Computerviren Ein Computervirus ist eine Befehlsfolge, deren Ausführung bewirkt, dass eine Kopie oder ein modifiziertes Abbild mit derselben Befehlsfolge in einem Speicherbereich, der diese Sequenz nicht enthält, reproduziert wird. Dieser Vorgang wird als Infektion bezeichnet. Die Befehlsfolge, der Computervirus, kann neben dieser Minimalanforderung der Reproduzierbarkeit auch noch beliebige weitere Funktionen wie z.B. Löschen, Einfügen oder das Verändern von Software und Daten bewirken.

Trojaner Ein Trojaner oder trojanisches Pferd ist ein Programm, das die spezifischen gewünschten Funktionen ordnungsgemäß ausführt, aber darüber hinaus

noch eine erweiterte Funktionalität aufweist, die dem Angreifer, der das trojanische Pferd installiert hat, die Möglichkeit zu unerlaubten Handlungen auf dem betroffenen IT-System eröffnet.

Logische Bomben Eine logische Bombe ist ein lauffähiges Programm, das so lange die erwartete Funktionalität bietet, bis durch die Erfüllung einer vorgegebenen Bedingung ein (vom Angreifer gewolltes) Fehlverhalten des Programms entsteht. Die logische Bombe ist in diesem Sinne ein Spezialfall eines Trojaners.

Würmer Ein Wurm ist ein lauffähiges Programm (oder eine Ansammlung von lauffähigen Programmen und Dateien), das in der Lage ist, sich über ein Netzwerk auch in andere Rechner zu vervielfältigen. Dies geschieht selbstgesteuert in Kommunikation mit anderen Segmenten. Ein Wurm ist die Vereinigung aller seiner Segmente.

Beispiele für Modifikationen der Software:

- Ein Mitarbeiter baut eine logische Bombe, die Daten und Programme nach seiner Entlassung (Löschen seines Namens in der Personaldatei) oder zu einem anderen festgelegten Zeitpunkt zerstört.
- Missbrauch der Supervisor Calls bei MVS (C. Schramm, Computing Centers Undermine MVS Security, Computer & Security, June 1991)

Daten- und Softwarediebstahl

Dieser Angriff wird meist durch das Kopieren oder Abgreifen der Daten und bzw. Software durchgeführt, um in den Besitz wertvoller Informationen und Funktionalitäten zu erlangen. So erhaltene Software kann selbst eingesetzt oder weiterverkauft werden. Dieser Kopiervorgang geschieht meist unmerklich und spurlos. Er ist daher nur anhand der Kopien und ihrer Verwendung nachzuweisen.

Beispiele:

- Diebstahl von Forschungs- und Entwicklungsdaten zur Erlangung eines Patents oder Wettbewerbsvorteils.
- Kopie der Kundendaten für den Wettbewerb.

Daten- und Softwarekidnapping

Der Angreifer entzieht der angegriffenen Organisation betriebswichtige Daten wie Buchhaltungsdaten, Kontenstände oder Vertriebsinformationen oder er nimmt betriebsnotwendige Applikationsprogramme wie Produktionssteuerungen, spezifische Software zur Kommunikation mit wichtigen Kunden oder Zugangskontrollsysteme von den IT-Systemen. Im nächsten Schritt bietet er der Organisation die Herausgabe der Daten oder der Software gegen Zahlung einer Geldsumme oder

Erfüllung einer sonstigen Forderung an. Die Organisation muss auf dieses Angebot eingehen, wenn sie keine Vorkehrungen gegen diese Straftat getroffen hat.

In unserer betrieblichen Praxis ist es auch vorgekommen, dass Angreifer die Daten oder Software nur logisch, aber nicht physikalisch entfernt hatten. Dazu nutzten die Angreifer kryptographische Verschlüsselungen oder spezifische Konfigurationen des Zugriffsschutzes, die nur sie aufheben konnten. Nach der Zahlung einer Geldsumme gaben sie die kryptographischen Schlüssel oder die Vorgehensweise bekannt, mit deren Hilfe die Daten oder die Software wieder verfügbar werden.

Dieser Angriff funktioniert nur dann, wenn der IT-Betreiber die Daten oder die Software nicht in einer annehmbaren Zeit rekonstruieren, reinstallieren oder rekonfigurieren kann.

Sabotage und Vandalismus

Der Angreifer hat das Ziel, die Dienste des angegriffenen IT-Systems massiv zu stören. Er führt dies zum einen durch physikalische Einwirkungen wie Trennen der Kommunikationsverbindungen, Abschalten der Stromversorgung, Stören der Klimaanlage oder Brandstiftung aus. Ein weiterer Ansatzpunkt ist die Software der IT-Systeme. Hier kann der Angreifer durch logische Bomben, gezieltes Ausnutzen von Programmierfehlern oder durch Überlastung der Programme großen Schaden anrichten. Ferner kann er direkt auf die Daten, die den Diensten zugrunde liegen, zugreifen und sie nmjgentweder löschen oder manipulieren.

Spionage

Der Angreifer verschafft sich wertvolle Unternehmensdaten wie Gehalts-, Vertriebs-, Planungs-, Forschungs- und Entwicklungsdaten. Diese Daten sind dem Mitbewerber bares Geld wert. Typische Angreifer sind frustrierte Mitarbeiter nach deren »innerer Kündigung« sowie gewerbliche oder staatliche Dienstleister. An dieser Stelle sei auf die Ergebnisse des Echelon-Untersuchungsausschusses des Europäischen Parlaments verwiesen, der die privatwirtschaftlichen Aktivitäten der amerikanischen Nationalen Sicherheitsagentur NSA näher beschreibt /ECHELON2001/.

1.4 Die Angreifer

Zur richtigen Einschätzung der Gefährdungen ist es wichtig, ihre Quellen und Verursacher näher zu betrachten: Die Angreifer. Zu einem Angreifer kann jede Person werden, die über einen Zugang zum angegriffenen IT-System bereits berechtigterweise verfügt oder ihn sich verschaffen kann. Wir unterscheiden zwischen den Anwendern, den Administratoren, den Programmierern sowie den externen Technikern.

Berechtigte Nutzer können die ihnen eingeräumten Rechte missbrauchen. Unberechtigten Angreifern gelingt es im Rahmen ihres Angriffs vorzutäuschen, zu einer der berechtigten Kategorien zu gehören.

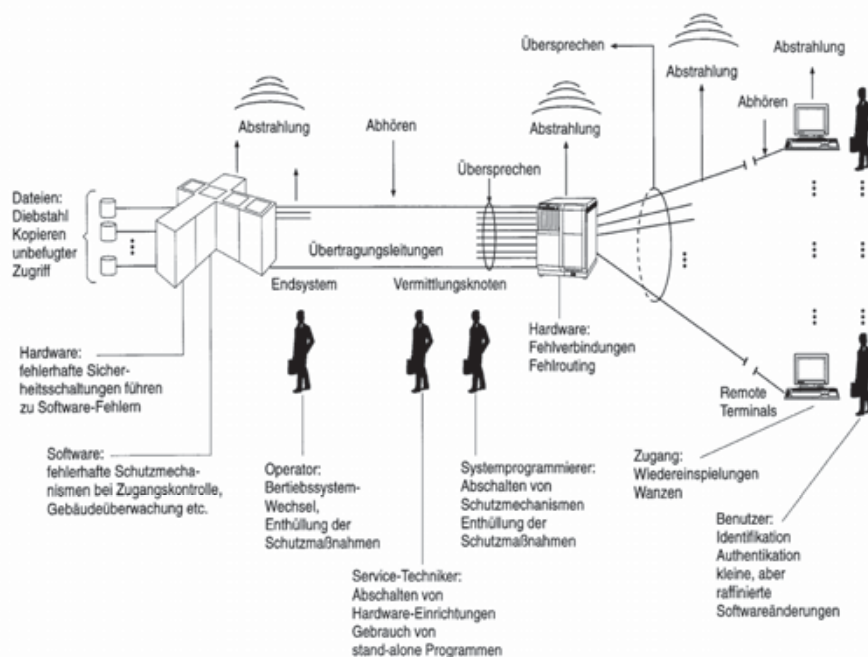


Abb. 1.6: Überblick Angriffsszenarien

Anwender

Anwender sind die Nutzer der IT-Dienste der betrachteten Organisation. Sie rekrutieren sich aus den Mitarbeitern der Organisation sowie Dritten, die mit der Organisation in Geschäftsbeziehung stehen oder eine mögliche Geschäftsbeziehung prüfen. Die Anwender können im Rahmen der ihnen zugebilligten Zugriffsrechte auf Daten zugreifen und auf sie Einfluss nehmen. Sie können Daten abrufen, neu einfügen, modifizieren und löschen.

Administratoren

Administratoren und Systembetreuer unterstützen durch die Verwaltung der IT-Systeme die Nutzer. Sie erhalten dazu Zusatzfunktionen und meist auch erweiterte Zugangs- und Zugriffsrechte für die von ihnen administrierten Systeme. Sie sind dadurch in der Lage, deutlich weitreichenderen Einfluss auf die zugrundeliegenden Daten auszuüben.

Programmierer

Die Programmierer erstellen und verändern die den IT-Diensten zugrundeliegenden System- und Applikationsprogramme. Sie nehmen damit direkten Einfluß auf die Funktionalität der Anwendungsprogramme und der (Betriebs-)Systemprogramme. Falls sie direkten Zugriff auf die Produktivsysteme haben, ist es schwer, ihre Einwirkungsmöglichkeiten einzugrenzen und ihre Aktionen revisionsfest nachzuvollziehen.

Servicetechniker

Servicetechniker warten Systemkomponenten der IT-Systeme. Sie tauschen defekte oder veraltete Komponenten aus und erweitern bestehende Systeme. Für den Test und die Inbetriebnahme erhalten sie ähnliche Zugangs- und Zugriffsrechte wie die Administratoren. Die Wartung der Systeme wird von zahlreichen Organisationen in Form von Wartungsverträgen an externe Unternehmen vergeben. Die Servicetechniker sind zumeist externe Mitarbeiter, die nicht der umfassenden Weisungsbefugnis und den Verpflichtungen der Organisation unterliegen.

Sonstige Dienstleister

Sonstige Dienstleister wie Handwerker, Reinigungskräfte und Kommunikationstechniker erhalten auf Grund ihrer Tätigkeit Zugang zu den Räumlichkeiten der IT-Systeme. Sie können so direkt physikalisch auf die Systeme Einfluss nehmen.

1.5 Juristische Rahmenbedingungen

Der IT-Sicherheitsprozess muss die juristischen Rahmenbedingungen einhalten. Dies gilt zunächst für den Sicherheitsprozess selbst, dann auch für die einzelnen Schutzmaßnahmen. Der IT-Sicherheitsprozess ist im Einklang mit dem geltenden Recht zu planen und umzusetzen. Ferner muss er externe Einwirkungen durch Angreifer entsprechend den anzuwendenden Gesetzen und Vorschriften hinreichend hemmen.

Der IT-Sicherheitsprozess hat alle Gefahren zu berücksichtigen, die aus dem Einsatz der Informationstechnologie erwachsen. Da auch die Übertretung von Gesetzen und Verordnungen im Zusammenhang mit dem Einsatz der IT zu Schäden führen kann (z.B. Imageschäden, Geldstrafen), haben die Sicherheitsverantwortlichen eine Reihe von einschlägigen Gesetzen und Verordnungen in der Bedrohungsanalyse zu berücksichtigen. Dieser Abschnitt fasst die wichtigsten Gesetze und Verordnungen, die für den IT-Einsatz relevant sind, kurz zusammen.

Diese sind:

- das Grundgesetz (GG)
- das Bundesdatenschutzgesetz (BDSG)

- die Landesverfassungen
- das Volkszählungsurteil
- das Signaturgesetz und die Signaturverordnung
- weitere Gesetze und Verordnungen

1.5.1 Das Grundgesetz

Auszüge aus dem Grundgesetz vom 23. Mai 1949 (BGBl. S. 1):

Artikel 1 Abs. 1

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.

Artikel 2 Abs. 1

Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Artikel 10 Abs. 1

Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Aus den beiden ersten Artikeln des Grundgesetzes leitet sich ab, dass auch durch den Einsatz der IT weder die Würde von Menschen angetastet noch ihre freie Entfaltung eingeschränkt werden darf.

1.5.2 Das Volkszählungsurteil

Dieser Sachverhalt ist auch in das »Volkszählungsurteil« mit eingeflossen.

Leitsätze zum Volkszählungsurteil vom 15.12.1983 (Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983), Urteil des Bundesverfassungsgerichtes v. 15.12.1983 – 1 BvR 209/83 u. a. (BVerfGE 65,1 oder NJW 1984, S. 419 ff):

1. *Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikel 2 Abs. 1 i. V. mit Artikel 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*
2. *Einschränkungen dieses Rechts auf »informationelle Selbstbestimmung« sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei der Regelung hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.*

Somit kann eine Gefährdung entstehen, falls ein Mitarbeiter IT-Systeme der Organisation nutzt, um Material zu verbreiten, das die Würde anderer verletzt. In diesem Fall kann der so Diskreditierte erfolgreich gegen den Mitarbeiter klagen. Die Organisation trifft dann eine Mitschuld, da sie die notwendige Infrastruktur bereitgestellt hat bzw. Gesetzesverletzungen nicht wirksam unterbunden hat.

Darüber hinaus fordert das Grundgesetz die Wahrung des Post- und Fernmeldegeheimnisses. So könnte eine Gefährdung entstehen, wenn von Mitarbeitern private per IT erstellte oder versandte Briefe von einem Administrator geöffnet werden. Artikel 10 des GG wird allerdings durch das *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (Gesetz zu Artikel 10 Grundgesetz – G 10) dahingehend eingeschränkt, dass berechtigten Stellen zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung die Einsicht in Kommunikationen gewährt werden muss.

1.5.3 Landesverfassungen

Exemplarisch seien hier einige Auszüge aus der Verfassung des Landes Sachsen-Anhalt vom 16. Juli 1992 (GVBl. S. 600) aufgeführt:

Art. 6 (Datenschutz, Umweltdaten)

(1) Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. In dieses Recht darf nur durch oder aufgrund eines Gesetzes eingegriffen werden. Dabei sind insbesondere Inhalt, Zweck und Ausmaß der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zu bestimmen und das Recht auf Auskunft, Löschung und Berichtigung näher zu regeln.

Art. 63 (Datenschutzbeauftragter)

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Träger öffentlicher Stellen im Lande wird von einem Landesbeauftragten für den Datenschutz überwacht. Das Gesetz kann weitere Aufgaben für den Landesbeauftragten für den Datenschutz vorsehen.

(2) Der Landtag wählt auf Vorschlag der Landesregierung den Landesbeauftragten für den Datenschutz mit der Mehrheit von zwei Dritteln der anwesenden Abgeordneten, mindestens mit der Mehrheit seiner Mitglieder für die Dauer von 6 Jahren.

(3) Der Landesbeauftragte ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er berichtet über seine Tätigkeit und deren Ergebnisse dem Landtag, an den er sich jederzeit wenden kann.

(4) Das Nähere regelt ein Gesetz.

Also hat jeder das Recht auf den Schutz seiner personenbezogenen Daten. Das Nähere im Umgang mit personenbezogenen Daten regelt ein weiteres Gesetz, in diesem Fall das Datenschutzgesetz für das Land Sachsen-Anhalt.

Gesetz zum Schutz personenbezogener Daten der Bürger

Das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) regelt im Detail die Rechte und Pflichten öffentlicher Stellen des Landes sowie der Betroffenen beim Umgang mit personenbezogenen Daten.

Es gibt natürlich eine Vielzahl von Gelegenheiten, den Schutz personenbezogener Daten zu verletzen. Es können zum Beispiel mehr Daten als notwendig erhoben werden, Daten für weitere Zwecke benutzt werden oder Anonymisierungen nicht durchgeführt werden.

Daneben können auch Fristen verletzt werden, wenn zum Beispiel kein Datenschutzbeauftragter für jede Organisation eingesetzt ist oder die Nutzung personenbezogener Daten nicht binnen drei Jahren mit dem Gesetz in Einklang gebracht wird.

1.5.4 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetzes (BDSG) in seiner aktuellen Fassung mit der letzten Änderung vom 18.05.2001 dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Es hat Gültigkeit für öffentliche Stellen der Länder, soweit der Datenschutz nicht durch das Landesgesetz geregelt ist. Da für Sachsen-Anhalt ein Landesdatenschutzgesetz (DSG-LA) vorhanden ist, treffen für die Behörde nur die Abschnitte des BDSG zu, die nicht im DSG-LA geregelt sind.

1.5.5 Signaturgesetz und Signaturverordnung

Sollte die Organisation rechtsgültige Handlungen auf rein digitaler Weise tätigen wollen, so ist die Verwendung qualifizierter elektronischer Signaturen im Sinne vom *Gesetz über Rahmenbedingungen für elektronische Signaturen* (Signaturgesetz – SigG) vom 16. Mai 2001 Bedingung. Die Anforderungen der *Verordnung zur elektronischen Signatur* (Signaturverordnung – SigV) sind in diesem Zusammenhang zu beachten.

Ob eine qualifizierte elektronische Signatur bei Verträgen rechtsgültig ist, hängt von der geforderten Vertragsform ab. Wo die Vertragsform freigestellt ist, kann eine elektronische Signatur das Abschließen eines Vertrages bekunden. Die zivile Prozessordnung in Form des BGB schreibt jedoch für einige Verträge explizit die Schriftform vor.

Deshalb hat die Bundesregierung am 6. September 2000 einen »Gesetzentwurf zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr« vorgelegt. Er führt neben der bereits existierenden Schriftform u.a. eine neue »Textform« sowie die »elektronische Form«

ins Bürgerliche Gesetzbuch (B#GB) ein, die in den meisten Fällen der Schriftform gleichgestellt werden soll. Diese »elektronische Form« stützt sich dabei auf die qualifizierte elektronische Signatur nach dem neuen Signaturgesetz.

1.5.6 Weitere Gesetze und Verordnungen

Neben den bisher aufgeführten Gesetzen und Verordnungen können die Mitarbeiter der Organisation in ihrem Gebrauch der IT gegen weitere Gesetze, zum Beispiel des StGB, verstoßen. Da die Organisation die IT zur Verfügung stellt, übertritt damit eventuell die Organisation Gesetze, wird strafbar oder muss Schadensersatz leisten.

Auch wenn die beiden folgenden Beispiele noch nicht eindeutig in der Rechtsprechung beurteilt sind, kann sich in Zukunft die Verantwortung von Institutionen, die IT bereitstellen, weiter ausweiten, so dass schon frühzeitig diese Gefahren berücksichtigt werden sollten.

Beispiel 1: Mitarbeiter der einzelnen Abteilungen gestalten den Inhalt von sowohl internen Web-Servern als auch von öffentlichen Web-Servern (z.B. durch die Pressestelle). Sollten Mitarbeiter (versehentlich) Links auf Webseiten bereitstellen, die auf Webseiten mit »illegalem« Inhalt verweisen, so übertreten diese Mitarbeiter und damit auch die Organisation verschiedene Gesetze.

Beispiel 2: Ein Angreifer benutzt Rechner der Organisation, um verschiedene andere Organisationen anzugreifen. Er fügt diesen beträchtlichen Schaden zu. Der zum Angriff genutzten Organisation ist unterlassene Vorsorge vorwerfbar, so dass auch die Organisation haftbar für die entstandenen Schäden ist.

Sollte die Organisation einen eigenen Web-Server bereitstellen, auf dem Informationen für die Öffentlichkeit bereitgestellt werden, so können auch das Teledienstgesetz (TDG) sowie das Teledienstedatenschutzgesetz (TDDSG) zur Anwendung kommen. Beispielsweise wäre es möglich, dass in diesem Falle Zugriffsdaten (= personenbezogene Daten) ohne Einwilligung der Nutzer gespeichert werden (Stichwort »Logdateien«).

1.6 Gefahren am Beispiel einer Verwaltungsbehörde

In den folgenden Abschnitten werden konkrete Gefährdungen aufgeführt, die Werte einer Organisation bedrohen und die über die allgemeinen Bedrohungen hinausgehen. Die Struktur der Darstellung dieser Gefährdungen und Bedrohungen folgt der des Grundschutzhandbuches des BSI /GSHB/.

1.6.1 Sicherheitsmanagement

Das Grundschutzhandbuch gibt als Gefahr zum Thema Sicherheitsmanagement lediglich global die Gefährdung durch »Unzureichendes IT-Sicherheitsmanagement (G 2.66)« an.

Die wesentliche Gefahr eines fehlenden Sicherheitsmanagements liegt in der mangelnden Steuerung des Sicherheitsprozesses. Um ein angemessenes Sicherheitsniveau für alle Bereiche des IT-Einsatzes der Organisation zu erreichen, ist ein sorgfältig organisierter Sicherheitsprozess notwendig, der die Organisation als Gesamtheit betrachtet. Es besteht also die Gefahr, dass ein unzureichendes IT-Sicherheitsmanagement keinen angemessenen Sicherheitsprozess definiert und herbeiführt. So bleiben viele potentielle Gefahren unberücksichtigt. Es ist dann nur eine Frage der Zeit, bis ein schädigender Sicherheitsvorfall eintritt.

1.6.2 Kontinuitätsplanung

Die Gefahr, der eine Notfallvorsorge entgegenwirkt, wird im Grundschutzhandbuch mit »Ausfall eines IT-Systems (G1.2)« benannt.

Darüber hinaus bestehen natürlich weitere spezielle Gefahren, die im Falle eines Notfalles die Eindämmung oder Behebung von Schäden behindern. Zu diesen Gefahren können gehören:

- **Unzureichende Datensicherung**
 - Datenverlust durch unzureichende oder fehlerhafte Datensicherung
 - verzögerter Wiederanlauf von Systemen durch fehlendes Backup oder fehlende Dokumentation
- **Unzureichendes Notfallkonzept**
 - Ausbreitung der Schäden sowie Folgeschäden durch fehlende Sicherheitsmaßnahmen
 - zu spätes Erkennen eines Notfalls wegen fehlender Kontrollmechanismen (technisch und organisatorisch) oder Schulung der Mitarbeiter
- **Fehlendes Sicherheitsbewusstsein**
 - Unwissen der Mitarbeiter über das angemessene Verhalten bei Sicherheitsvorfällen
 - fehlendes Verständnis der Ursachen von Notfällen aufgrund unzureichender Protokollierung
 - fehlende Nachbearbeitung von Notfällen, so dass keine Lehren aus ihnen gezogen werden

1.6.3 Datensicherungskonzept

Es besteht die Gefahr, dass gespeicherte Daten verloren gehen, die gar nicht oder nur unter sehr hohem Aufwand wiederbeschafft werden können. Deshalb ist ein Datensicherungskonzept für alle Daten der Organisation notwendig, die kontinuierlich verfügbar gehalten oder aufgrund von Bestimmungen für längere Zeit dokumentiert werden müssen.

Ein unzureichendes Datensicherungskonzept fördert die folgenden Gefahren:

- Technisches Versagen
 - Datenträger mit gesicherten Daten altern schneller als erwartet und sind nicht mehr lesbar.
 - Der Rückspielvorgang von Datensicherungen funktioniert nicht.
 - Die Datensicherung verläuft unbemerkt nicht erfolgreich.
- Organisatorische Mängel
 - Sicherungsbedürftige Daten werden nicht gesichert.
 - Sicherungsbedürftige Daten werden nicht häufig genug gesichert.
 - Gesicherte Daten gehen durch nochmalige Überschreibung verloren.
 - Verantwortungsbereichen für die Datensicherungen sind nicht geklärt.
 - Mit dem Wechsel von Verantwortungsbereichen ist der Zugriff auf Datenträger nicht mehr gewährleistet (evtl. fehlende Zugriffsberechtigungen, fehlende kryptographische Schlüssel).
- Datenträger zur Datensicherung werden nicht unverzüglich in das Datenträgerarchiv überführt
- Infrastrukturmängel
 - Die notwendige Soft- und/oder Hardware ist nicht mehr vorhanden, um gesicherte Daten zurückzuspielen.
 - Die Datenträger zur Datensicherung werden nicht sicher aufbewahrt (fehlendes Datenträgerarchiv, siehe Abschnitt 1.6.7).

1.6.4 Computervirenschutz-Konzept

Aus- und eingehende E-Mails werden zentral auf dem E-Mail-Server der Organisation auf Virenbefall hin untersucht. Darüber hinaus werden E-Mails lokal auf den Arbeitsplatzrechnern durch eine Virus-Scan-Software untersucht.

Falls ein Virenschutzkonzept nicht in schriftlicher Form vorliegt, so besteht die Gefahr, dass die Maßnahmen (organisatorisch, administrativ und technisch) nicht ausreichend definiert sind. Dies kann bei Personalausfall oder in Notfällen zu erheblichen Folgeschäden führen.

Neben Viren, die Arbeitsplatzrechner meistens per E-Mail befallen, sind alle IT-Systeme durch Würmer bedroht.

Ein fehlendes oder unzureichend dokumentiertes Virenschutzkonzept kann die folgenden Bedrohungen für Systeme und Daten der Organisation hervorrufen:

- Fehlverhalten des Benutzers
 - Der Virenschutz auf den Arbeitsplatzrechnern ist deaktiviert.
 - Die Benutzer wissen nicht, wie sie einen Virenbefall erkennen sollen.

- Den Benutzern ist nicht bekannt, wie sie sich bei einem Virenbefall verhalten sollen.
- Benutzer versuchen den Virenschutz zu umgehen.
- Benutzer wissen nicht mit dem Virenschutz zu arbeiten.
- Unzureichendes Sicherheitsbewußtsein
 - Benutzer wissen nicht um die Bedeutung des Virenschutzes.
 - Benutzer erkennen einen Virenbefall nicht.
- Organisatorische Mängel
 - Die zur Erkennung benutzten Virenmuster werden nicht häufig genug erneuert.
 - Der Virenschutz auf Arbeitsplatzrechnern ist nicht installiert, fehlerhaft realisiert oder gänzlich deaktiviert.
 - Bei einem Virenbefall ist das notwendige sachkundige Sicherheitspersonal nicht verfügbar.
- Technisches Versagen
 - Das automatische Erneuern von Virenmustern ermöglicht dennoch die Einschleusung von Viren und Trojanern

1.6.5 Gebäudesicherheit

Die gesamte Gebäudesicherheit sprengt den Rahmen eines IT-Sicherheitskonzeptes. Die Organisation des Zutrittschutzes birgt jedoch Gefahren, die sich nicht ausschließlich auf die bauliche Sicherheit beschränken und deshalb hier betrachtet werden.

Die Gebäude einer Organisation besitzen meist eine Vielzahl von Eingängen. Der Haupteingang und der Nebeneingang werden jeweils durch eine Pförtnerloge bewacht. Andere Außentüren des Gebäudes können entweder

- mit einem Schlüssel geöffnet werden,
- durch den Pförtner nach Überprüfung der Identität über eine Intercom-Anlage geöffnet werden oder
- direkt geöffnet werden, da sie unverschlossen sind.

Zutritt zu den unverschlossenen Türen ist allerdings z.B. nur über den Parkplatz der Organisation möglich, dessen Zugang an der Pförtnerloge des Nebeneinganges vorbeiführt. Ganz klar besteht die Gefahr des unbefugten Zutritts zum Gebäude der Organisation.

Ein Besucher der Organisation, der nicht ständig begleitet wird, kann alle Korridore ungehindert betreten. Da in der Regel unbesetzte Büros unverschlossen sind (teilweise stehen die Türen sogar offen), kann ein Besucher Büros betreten, sich an

Geräten zu schaffen machen, zusätzliche Geräte installieren (zur Spionage oder Sabotage) oder evtl. vertrauliche Dokumente und Geräte (Diebstahl) entwenden.

1.6.6 Räume für Server und technische Infrastruktur

Die Serverräume sind meist abgeschlossen. Ein Feuerlöscher ist in jedem Raum vorhanden. Gas- oder Wasserleitungen sind in der Regel nicht sichtbar, jedoch sind meist Heizkörper mit Heizungsrohren vorhanden. Die Server stehen oft nicht erhöht. Die meisten Schäden können entstehen durch

- technisches Versagen
 - Die Stromversorgung ruft technische Probleme hervor.
- unkontrollierten Zugang
 - Unbefugte Zutritt zu den Räumen erlangen können.
- Höhere Gewalt
 - Die Räume und die technische Infrastruktur sind nicht vor höherer Gewalt geschützt.

Es besteht die Gefahr, dass die technischen Geräte Bedrohungen durch Feuer, Wassereintritt, Luftfeuchtigkeit, Wärmeentwicklung, Stromausfall, Strom- und Spannungsspitzen, Staub, Verschmutzung, Vandalismus, Manipulation oder Diebstahl ausgesetzt sind.

1.6.7 Datenträgerarchiv

Die meisten Organisationen besitzen kein dediziertes Datenträgerarchiv für die Speichermedien der Datensicherung. Es besteht die Gefahr, dass diese Datenträger, nicht angemessen geschützt sind (siehe Abschnitt 1.6.3).

Ein Datenträgerarchiv muss ausreichenden Schutz vor Feuer, Wasserschäden, extremen Temperaturen und Luftfeuchtigkeit sowie Staub und Verschmutzung bieten, damit Datenträger und damit die gespeicherten Daten nicht zerstört werden.

Ein Datenträgerarchiv soll einerseits vor unbefugtem Zutritt geschützt werden. Andererseits muss durch geeignete organisatorische Maßnahmen sichergestellt sein, dass innerhalb kurzer Zeit der Zugriff zu den Datenträgern möglich ist, andernfalls ist eine evtl. geforderte sehr hohe Verfügbarkeit von Daten nicht gewährleistet.

Ähnlich wie bei Serverräumen besteht die Gefahr eines Einbruchs mit Diebstahl und/oder Vandalismus, der den Verlust der Daten zur Folge hätte. Außerdem besteht die Gefahr von Datenverlust durch Unlesbarkeit der Datenträger.

1.6.8 PC-Systeme

Die Workstations der Organisation, die auf den Zugang zum Netzwerk der Organisation abgestimmt sind, besitzen meist eine lokale Festplatte, ein Diskettenlaufwerk sowie überwiegend ein CD-ROM-Laufwerk.

Alle Standard-Arbeitsplätze verfügen in der Regel über einen Internet-Zugang für E-Mail und Internet. Das verwendete Betriebssystem ist zum überwiegenden Teil ein Microsoft Windows-Derivat wie NT, Windows 2000 oder Windows XP.

Es bestehen folgende Gefahren:

Unautorisierter Zugang zum IT-System

- Die Rechtevergabe und Konfiguration eines Arbeitsplatz-PCs ist nicht restriktiv genug. Falls beispielsweise die Möglichkeit besteht, von Diskette oder CD zu booten, kann ein unbefugter Dritter Daten von dem Arbeitsplatz-PC stehlen, Daten zerstören oder zusätzliche (Spionage-) Software installieren.
- Es bleibt unerkannt, wenn unautorisierte oder autorisierte Benutzer zusätzliche Software auf einem Arbeitsplatz-PC installiert haben.
- Der Autorisierungsvorgang an einem Arbeitsplatz-PC ist nicht sicher genug. Der Passwortmechanismus von Windows NT ist keinesfalls sicher. Es kommt hinzu, dass einfache Passwörter gewählt werden können und Passwörter nicht regelmäßig neu gewählt werden müssen. So ist ein Zugriffsschutz auf die Arbeitsplatz-PCs praktisch nicht gegeben.
- Lokale Daten können gelesen werden. In Zusammenhang mit den in der Regel unverschlossenen Büros ist es für einen Angreifer leicht, sich Zugang zu einem IT-System zu verschaffen. Hat der Angreifer Zugriff auf ein IT-System, so kann er auch lokale Daten ohne Authentisierung am IT-System stehlen, indem er über das Diskettenlaufwerk oder CD-Laufwerk sein eigenes Betriebssystem startet.
- Vertrauliche Daten, die von Servern gelesen werden, werden als temporäre Dateien auf dem Arbeitsplatz-PC gespeichert und können von unberechtigten Benutzern gelesen werden.

Datenverlust

- Lokale Daten gehen bei einem Plattencrash oder als Folge versehentlichen Löschens verloren (siehe Abschnitt 1.6.3).
- Lokale Datenträger (Disketten oder Festplatten) werden gestohlen.

Integritätsverlust durch multiple Datenbestände

- Werden für bestimmte Informationen mehrere Datenbestände auf unterschiedlichen Datenträgern gespeichert, besteht die Gefahr, dass es zu Versionskonflikten kommt, insbesondere dann, wenn mehrere Personen diese Informationen bearbeiten.

Fehlendes Sicherheitsbewusstsein

- Die Benutzer sind sich der Ausprägung, Wirksamkeit und Notwendigkeit der getroffenen Sicherheitsmaßnahmen nicht bewusst. Sie erkennen Sicherheitsvorfälle nicht oder wissen nicht, wie sie sich verhalten sollen. Der Arbeitsplatz-PC ist in der Regel nicht ausreichend vor Viren oder aktivem Code geschützt (vgl. Abschnitte 1.6.4 und 1.6.13).

1.6.9 Laptops, Notebooks und PDAs

Meist setzt die Organisation eine kleine Anzahl von Laptops und PDAs ein. Bei diesen Geräten treffen im Wesentlichen die gleichen Gefahren zu wie bei den Standard-Arbeitsplatz-PCs. Als besondere Gefahren kommen allerdings für diese mobilen Geräte hinzu:

Diebstahl

- Laptops und PDA werden außerhalb der Organisation benutzt; somit greifen viele Sicherheitsmaßnahmen nicht mehr und es besteht eine erhöhte Diebstahlgefahr.

Unzureichende Datensicherung

- Die Standard-Datensicherung bezieht diese mobilen Geräte nicht mit ein, so dass durch Diebstahl oder technischen Defekt wichtige Daten verloren gehen können.
- Die unkontrollierte Nutzung mobiler Datenträger (Disketten, CDs, ZIPs) kann zum Verlust oder Bekanntwerden vertraulicher Informationen führen, da die Verantwortlichen für die Datensicherheit keine Kenntnis von diesen Datenträgern haben.

Integritätsverlust durch multiple Datenbestände

- Speziell durch den Laptoneinsatz werden für bestimmte Informationen mehrere Datenbestände auf unterschiedlichen Datenträgern gespeichert. Es besteht die Gefahr, dass es zu Versionskonflikten kommt, insbesondere dann, wenn mehrere Personen diese Informationen bearbeiten.

Mangelnde Verschlüsselung der Daten

- Wegen der erforderlichen Mobilität werden sensible Daten lokal auf den Laptops und PDAs gespeichert – allerdings im Regelfall unverschlüsselt.
- Vertrauliche Daten werden bewusst nur auf Disketten und nicht auf dem Laptop selbst gespeichert. Die unverschlüsselten Daten sind allerdings auf Disketten noch mehr den Gefahren Diebstahl, Verschmutzung und technische Defekte ausgesetzt als auf der Festplatte des Laptops. Darüber hinaus ist es sehr wahrscheinlich, dass vertrauliche Daten ohne das Wissen des Benutzers in temporären Dateien auf dem Laptop gespeichert sind, auch wenn der Benutzer die Daten auf der Diskette bearbeitet.

Keine starken Authentisierungsmaßnahmen

- Möglicherweise nutzen mehrere Benutzer einen Laptop; der Autorisierungsmechanismus ist daher für alle standardisiert. Eine Authentisierung des einzelnen Benutzers fehlt.

1.6.10 Server

Neben den im Grundschutzhandbuch angegebenen allgemeinen Gefahren haben Untersuchungen einiger als repräsentativ ausgewählter Server ergeben, dass die folgenden speziellen Gefahren bestehen:

Sicherheitslücken der Betriebssysteme und der Software

- Die meisten Server benutzen leicht erratbare TCP-Sequenznummern und IP IDs. Diese technischen Eigenschaften des TCP/IP-Stapels können für Angriffe auf die Kommunikationsverbindungen von Servern benutzt werden.
- Der Intranet-Web-Server und der MS Exchange Server haben Schwachstellen, die es einem lokalen Benutzer mit bestimmten Rechten ermöglichen können, beliebige Befehle auf dem entsprechenden Server auszuführen.
- Der Intranet-Web-Server und der MS Exchange Mail-Server stellen auch einen Mail-Dienst zur Verfügung, der es ebenfalls erlauben könnte, beliebige Befehle auf dem entsprechenden Server auszuführen.
- Der DNS-Server stellt eine Version des SSH-Dienstes zur Verfügung, die es einem Angreifer erlauben könnte, root-Rechte zu erlangen.

Konfigurationsprobleme

- Einige Server zeigen offene Ports (= bereitstehende Dienste), die eventuell nicht notwendig sind.

1.6.11 Heterogenes Netzwerk

Die Mitarbeiter der Organisation gehören zu verschiedenen Abteilungen und Referaten. Neben ihnen sind externe Dienstleister wie Wartungstechniker, Schulungsleiter und Schulungsteilnehmer in der Organisation tätig. Diese organisatorische Trennung spiegelt sich nicht in der Strukturierung des Netzwerkes der Organisation wieder. Netzwerktechnisch (physikalisch) sind alle Computer miteinander verbunden und können miteinander kommunizieren. Das bedeutet auch, dass externe Schulungsleiter und Schulungsteilnehmer während Schulungen auf die Arbeitsplatz-PCs und Server der Organisation zugreifen könnten. Die Bedrohungen sind eindeutig: der mögliche Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit von Daten und IT-Systemen.

Die eingesetzte Switching-Technologie bietet nur scheinbar einen Schutz vor dem Mitlesen von Kommunikationsdaten. Es ist bekannt, dass Switches dies normalerweise nicht unterbinden können, so dass Daten von einem Spionage-Computer mitgelesen werden können.

1.6.12 E-Mail-Kommunikation

Wie bereits kurz beschrieben, haben die Mitarbeiter jeder Organisation die Gelegenheit, einen E-Mail-Dienst zu nutzen, mit dem sie sowohl innerhalb der Organisation als auch über das Internet E-Mails versenden und empfangen können. Dabei bestehen grundsätzlich die folgenden Gefahren:

Fehlendes Sicherheitsbewusstsein

- Ein Mitlesen von E-Mails durch unautorisierte Personen ist möglich, da E-Mails nicht verschlüsselt werden. Nach Aussage der meisten interviewten Mitarbeiter werden vertrauliche Daten ausschließlich per Brief-Post verschickt. Einzelne Personen empfangen allerdings Informationen, die ihrer Ansicht nach nicht per E-Mail versendet werden sollten. Selbst der Einsatz von Switches in einem Netzwerk verhindert nicht, dass Kommunikationsdaten von Dritten mitgelesen werden können.
- Die Mitarbeiter verfügen nur unzureichend über Wissen zu den Sicherheitsrisiken im Umgang mit E-Mails (vgl. Abschnitt 1.6.4).

Technische Schwachstellen

- Durch eine reine Ende- zu- Ende- Verschlüsselung von E-Mails wird die Content- und Virenprüfung unterbunden. Hier sind Konzepte der »virtuellen Poststelle« anzuwenden.

Unzureichende organisatorische Sicherheitsmaßnahmen

- Unzureichende organisatorische Sicherheitsmaßnahmen umfassen u.a. eine unvollständige oder fehlende E-Mail-Regelung, die den Gebrauch von E-Mail definiert. Organisatorische und administrative Regelungen müssen festlegen, welche Daten per E-Mail versandt werden dürfen.
- Die Vertreterregelung ist unzureichend.
- Es erfolgt keine Trennung zwischen personenbezogenen und funktionsbezogenen E-Mail-Accounts. Dies kann dazu führen, dass bei fehlender Vertreterregelung wichtige E-Mails unbearbeitet bleiben oder dass bei ungenügender Vertreterregelung der entsprechende Vertreter vertrauliche personenbezogene E-Mails erhält; die Gefahr ist Verlust der Verfügbarkeit oder Verlust der Vertraulichkeit.

Vorsätzliches Fehlverhalten

- Bei unsignierten E-Mails kann sowohl der Absender als auch der Inhalt der E-Mail verfälscht werden.

Angriffe und Beeinträchtigung von aussen

- Das Eindringen von Viren, Würmern und Trojanischen Pferden über E-Mail auf das System des Benutzers ist möglich.
- Der unlimitierte Erhalt unerwünschter E-Mail, sogenannter SPAM-Mail, führt zu Arbeitszeitverlust, Belästigung oder – bei besonderer Häufung – auch Blockierung und Ausfall des E-Mail-Systems.

1.6.13 Internetzugriff

Neben der E-Mail-Kommunikation können die Mitarbeiter jeder Organisation meistens von ihrem Arbeitsplatz-PC aus auf das World Wide Web (Internet) zugreifen. Die folgenden Gefahren bestehen:

Organisatorische Gefahren

- fehlende Regelung der »Internetnutzung«

Fehlendes Sicherheitsbewusstsein

- Unwissen der Benutzer bezüglich der Gefahren bei Nutzung des Internet
- Unwissen der Benutzer über angemessene Verhaltensregeln im Fall einer akuten Gefahr
- Verlust der Vertraulichkeit von Informationen

Fehlender Inhaltsschutz

- Einschleppung von Malicious Codes wie Viren, Würmern, Trojanischen Pferden oder Spam

Fehlverhalten durch den Nutzer

- Installation unerwünschter und unerlaubter Programme
- Zerstörung von Daten und Programmen
- Übermäßige private Nutzung des Internet
- Fehlinformation der Mitarbeiter über das Internet
- Verletzung von Gesetzen und Verordnungen beim Aufruf »illegaler« Web-Seiten
- Mitverantwortung der Organisation für illegale Handlungen von Mitarbeitern im Internet oder Schädigungen von Mitarbeitern über das Internet

1.6.14 IT-Dienste und Anwendungen

Jede Organisation nutzt eine Vielzahl von Anwendungen, um spezifische Aufgaben zu erfüllen. Im Zusammenhang mit diesen Anwendungen bestehen zwei wesentliche Gefahren:

- Dienste, die nur auf einem IT-System zur Verfügung stehen, fallen mit dem IT-System aus und können in der Regel nicht zeitnah genug auf einem anderen IT-System zu Verfügung gestellt werden.
- Anwender speichern mit den Anwendungen bearbeitete Daten lokal auf ihren Arbeitsplatzrechnern. Dabei besteht die Gefahr, dass Daten ungeordnet gespeichert werden, ungeschützt lokal gespeichert werden oder gänzlich ungesichert bleiben.

1.7 Zusammenfassung

Die Quelle eines möglichen Angriffs muss lokalisiert werden, um den Angriff im Voraus unterbinden zu können. Dabei dürfen die juristischen Rahmenbedingungen nicht außer Betracht gelassen werden, denn es ist unverzichtbar, die für den Anwendungsfall relevanten Gesetze entsprechend zu kennen. Die Sicherheitsbestimmungen betreffen dabei nicht nur die Rechnersysteme selbst, sondern auch die Systemumgebung, in der sie stehen. Auch hier ist es wichtig die genannten Sicherheitsrisiken nicht zu unterschätzen. Der Raum bzw. das Gebäude, in dem der Rechner steht, ist adäquat abzusichern. Ebenso sollte genau überdacht werden, wie und auf welchen Speichermedien die Daten gesichert werden. Da

immer das Risiko eines Diebstahls besteht, sollten die Daten stets verschlüsselt transportiert und übertragen werden.

Alle Gefahren, die bei der IT-Nutzung entstehen, müssen erkannt und abgeschätzt werden können. Die Risiken sollten auf ein kalkulierbares und akzeptables Niveau gebracht werden. Die verschiedenen Arten von Bedrohungen, seien sie nun durch Menschen oder durch das IT-System selbst erzeugt, sollten einschätzbar sein, und das vor allem durch die Kenntnis der Angreifer und der Angriffsmöglichkeiten. Die aufgeführten Beispiele haben uns gezeigt, wie schnell Gefahren entstehen und wie schwer sie oftmals im Nachhinein zu beheben sind.

