Bundesamt
für Sicherheit in der
Informationstechnik

Elementare Gefährdungen

Inhaltsverzeichnis

G 0.1 Feuer

Feuer können schwere Schäden an Menschen, Gebäuden und deren Einrichtung verursachen. Neben direkten durch Feuer verursachten Schäden lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. durch unbeaufsichtigte offene Flammen, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- unsachgemäße Lagerung brennbarer Materialien (z. B. Altpapier),
- Nichtbeachtung der einschlägigen Normen und Vorschriften zur Brandvermeidung,
- fehlende Brandmeldeeinrichtungen (z. B. Rauchmelder),
- fehlende oder nicht einsatzbereite Handfeuerlöscher oder automatische Löscheinrichtungen (z. B. Gaslöschanlagen),
- mangelhaften vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen oder Verwendung ungeeigneter Dämmmaterialien zur Wärme- und Schallisolierung).

Beispiele:

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte, wie z. B. Kaffeemaschinen oder Tischleuchten, unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen.

G 0.2 Ungünstige klimatische Bedingungen

Ungünstige klimatische Bedingungen wie Hitze, Frost oder hohe Luftfeuchtigkeit können zu Schäden verschiedenster Art führen, beispielsweise zu Fehlfunktionen in technischen Komponenten oder zur Beschädigung von Speichermedien. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Ungünstige klimatische Bedingungen können auch dazu führen, dass Menschen nicht mehr arbeiten können oder sogar verletzt oder getötet werden.

Jeder Mensch und jedes technische Gerät hat einen Temperaturbereich, innerhalb dessen seine normale Arbeitsweise bzw. ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Umgebungstemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Arbeitsausfällen, Betriebsstörungen oder zu Geräteausfällen kommen.

Zu Lüftungszwecken werden oft unerlaubt Fenster von Serverräumen geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Beispiele:

- Bei hochsommerlichen Temperaturen und unzureichender Kühlung kann es bei IT-Geräten zu temperaturbedingten Ausfällen kommen.
- Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen.
- Durch zu hohe Temperaturen können magnetische Datenträger entmagnetisiert werden.

G 0.3 Wasser

Durch Wasser kann die Integrität und Verfügbarkeit von Informationen beeinträchtigt werden, die auf analogen und digitalen Datenträgern gespeichert sind. Auch Informationen im Arbeitsspeicher von IT-Systemen sind gefährdet. Der unkontrollierte Eintritt von Wasser in Gebäude oder Räume kann beispielsweise bedingt sein durch:

- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Besonders wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Probleme können außerdem durch Frost entstehen. Beispielsweise können Rohre in frostgefährdeten Bereichen undicht werden, wenn darin Wasser bei anhaltendem Frost stillsteht. Auch eine vorhandene Wärmedämmung wird mit der Zeit vom Frost überwunden.

Beispiel:

- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskartonelementen verkleidet war. Als eine Verbindung der Wasserleitung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils komplett abgeschaltet werden musste.

G 0.4 Verschmutzung, Staub, Korrosion

Viele IT-Geräte enthalten neben der Elektronik auch mechanisch arbeitende Komponenten, wie z. B. bei Fest- und Wechselplatten, DVD-Laufwerken, Druckern, Scannern etc., aber auch Lüftern von Prozessoren und Netzteilen. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch folgende Tätigkeiten in größerem Maße entstehen:

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor).

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den direkten Schaden am Gerät, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Die Geräte und die Infrastruktur können außerdem durch Korrosion angegriffen werden. Dies kann sich nicht nur auf die IT, sondern sogar auf die Sicherheit von Gebäuden negativ auswirken.

Durch Korrosion können auch indirekt weitere Gefährdungen entstehen. So kann beispielsweise Wasser aus korrodierten Stellen austreten (siehe G 0.3 Wasser).

Insgesamt können Verschmutzung, Staub oder Korrosion somit zu Ausfällen oder Beschädigungen von IT-Komponenten und Versorgungseinrichtungen führen. Als Folge kann die ordnungsgemäße Informationsverarbeitung beeinträchtigt werden.

Beispiele:

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

G 0.5 Naturkatastrophen

Unter Naturkatastrophen werden natürliche Veränderungen verstanden, die verheerende Auswirkungen auf Menschen und Infrastrukturen haben. Ursachen für eine Naturkatastrophe können seismische, klimatische oder vulkanische Phänomene sein, wie beispielsweise Erdbeben, Hochwasser, Erdrutsche, Tsunamis, Lawinen und Vulkanausbrüche. Beispiele für extreme meteorologische Phänomene sind Unwetter, Orkane oder Zyklone. Je nach Standort der Institution ist diese den Risiken durch die verschiedenen Arten von Naturkatastrophen unterschiedlich stark ausgesetzt.

Beispiele:

- Für Rechenzentren in Hochwasser-gefährdeten Gebieten besteht oft in besonderem Maße die Gefahr, dass unkontrolliert Wasser in das Gebäude eindringt (Überschwemmungen oder Anstieg des Grundwasserspiegels).
- Die Häufigkeit von Erdbeben und somit auch das damit verbundene Risiko hängen stark von der geografischen Lage ab.

Unabhängig von der Art der Naturkatastrophe besteht auch in nicht unmittelbar betroffenen Gebieten die Gefahr, dass Versorgungseinrichtungen, Kommunikationsverbindungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden. Besonders der Ausfall zentraler Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) kann sehr hohe Schäden nach sich ziehen. Betriebs- und Service-Personal kann aufgrund von großflächig eingerichteten Sperrbereichen der Zutritt zur Infrastruktur verwehrt werden.

Beispiele:

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist von keiner Versicherung gedeckt.
- Ein IT-System wird an einem Standort untergebracht, dessen geografische Lage für vulkanische Aktivität bekannt ist (zeitweilig aussetzendes Phänomen, bei dem die Emissionsphasen mit zum Teil langen Ruhephasen abwechseln).

G 0.6 Katastrophen im Umfeld

Eine Behörde bzw. ein Unternehmen kann Schaden nehmen, wenn sich im Umfeld ein schwerer Unglücksfall ereignet, zum Beispiel ein Brand, eine Explosion, die Freisetzung giftiger Substanzen oder das Austreten gefährlicher Strahlung. Gefahr besteht dabei nicht nur durch das Ereignis selbst, sondern auch durch die häufig daraus resultierenden Aktivitäten, beispielsweise Sperrungen oder Rettungsmaßnahmen.

Die Liegenschaften einer Institution können verschiedenen Gefährdungen aus dem Umfeld ausgesetzt sein, unter anderem durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetriebe oder Wohngebiete.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Solche Maßnahmen können auch dazu führen, dass Mitarbeiter ihre Arbeitsplätze nicht erreichen können oder Personal evakuiert werden muss. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

Beispiel:

- Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeiters (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

G 0.7 Großereignisse im Umfeld

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören unter anderem Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Zusammenhang mit solchen Veranstaltungen können zusätzliche Auswirkungen, wie die Einschüchterung von Mitarbeitern bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude, nach sich ziehen.

Beispiele:

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

G 0.8 Ausfall oder Störung der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Neben Störungen im Versorgungsnetz können jedoch auch Abschaltungen bei nicht angekündigten Arbeiten oder Kabelbeschädigungen bei Tiefbauarbeiten dazu führen, dass die Stromversorgung ausfällt.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Viele Infrastruktur-Einrichtungen sind heute vom Strom abhängig, z.B. Aufzüge, Klimatechnik, Gefahrenmeldeanlagen, Sicherheitsschleusen, automatische Türschließanlagen und Sprinkleranlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druck-Erzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig. Bei längeren Stromausfällen kann der Ausfall der Infrastruktur-Einrichtungen dazu führen, dass keinerlei Tätigkeiten mehr in den betroffenen Räumlichkeiten durchgeführt werden können.

Neben Ausfällen können auch andere Störungen der Stromversorgung den Betrieb beeinträchtigen. Überspannung kann beispielsweise zu Fehlfunktionen oder sogar zu Beschädigungen von elektrischen Geräten führen.

Zu beachten ist außerdem, dass durch Ausfälle oder Störungen der Stromversorgung in der Nachbarschaft unter Umständen auch die eigenen Geschäftsprozesse betroffen sein können, beispielsweise wenn Zufahrtswege blockiert werden.

Beispiele:

- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien (nach etwa 40 Minuten) fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.
- Im November 2005 waren nach heftigen Schneefällen in Niedersachsen und Nordrhein-Westfalen viele Gemeinden tagelang ohne Stromversorgung, weil viele Hochspannungsmasten unter der Schnee- und Eislast umgestürzt waren. Die Wiederherstellung der Stromversorgung dauerte einige Tage.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Für viele Geschäftsprozesse werden heutzutage zumindest zeitweise intakte Kommunikationsverbindungen benötigt, sei es über Telefon, Fax, E-Mail oder andere Dienste über Nah- oder Weitverkehrsnetze. Fallen einige oder mehrere dieser Kommunikationsverbindungen über einen längeren Zeitraum aus, kann dies beispielsweise dazu führen, dass

- Geschäftsprozesse nicht mehr weiterbearbeitet werden können, weil benötigte Informationen nicht abgerufen werden können,
- Kunden die Institution nicht mehr für Rückfragen erreichen können,
- Aufträge nicht abgegeben oder beendet werden können.

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorhanden sind.

Zu ähnlichen Problemen kann es kommen, wenn die benötigten Kommunikationsnetze gestört sind, ohne jedoch vollständig auszufallen. Kommunikationsverbindungen können beispielsweise eine erhöhte Fehlerrate oder andere Qualitätsmängel aufweisen. Falsche Betriebsparameter können ebenfalls zu Beeinträchtigungen führen.

Beispiele:

- Das Internet ist heute für viele Institutionen zu einem unverzichtbaren Kommunikationsmedium geworden, unter anderem zum Abruf wichtiger Informationen, zur Außendarstellung sowie zur Kommunikation mit Kunden und Partnern. Unternehmen, die sich auf Internet-basierte Dienstleistungen spezialisiert haben, sind natürlich in besonderem Maße von einer funktionierenden Internet-Anbindung abhängig.
- Im Zuge der Konvergenz der Netze werden Sprach- und Datendienste häufig über die gleichen technischen Komponenten transportiert (z. B. VoIP). Dadurch steigt jedoch die Gefahr, dass bei einer Störung der Kommunikationstechnik die Sprachdienste und die Datendienste gleichzeitig ausfallen.

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der grundlegenden Ver- und Entsorgung und somit als Basis für alle Geschäftsprozesse einer Institution einschließlich der IT dienen. Beispiele für solche Versorgungsnetze sind:

- Strom,
- Telefon,
- Kühlung,
- Heizung bzw. Lüftung,
- Wasser und Abwasser,
- Löschwasserspeisungen,
- Gas,
- Melde- und Steueranlagen (z. B. für Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen.

Der Ausfall oder die Störung eines Versorgungsnetzes kann unter anderem dazu führen, dass Menschen nicht mehr im Gebäude arbeiten können oder dass der IT-Betrieb und somit die Informationsverarbeitung beeinträchtigt wird.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

Beispiele:

- Ein Ausfall von Heizung oder Lüftung kann zur Folge haben, dass alle Mitarbeiter die betroffenen Gebäude verlassen müssen. Dies kann unter Umständen hohe Schäden nach sich ziehen.
- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind unter Umständen elektrische Hebepumpen vorhanden.
- Der Ausfall der Wasserversorgung beeinträchtigt eventuell die Funktion von Klimaanlagen.

G 0.11 Ausfall oder Störung von Dienstleistern

Kaum eine Institution arbeitet heute noch ohne Dienstleister wie Zulieferer oder Outsourcing-Anbieter. Wenn Organisationseinheiten von Dienstleistern abhängig sind, kann durch Ausfälle externer Dienstleistungen die Aufgabenbewältigung beeinträchtigt werden. Der teilweise oder vollständige Ausfall eines Outsourcing-Dienstleisters oder eines Zulieferers kann sich erheblich auf die betriebliche Kontinuität auswirken, insbesondere bei kritischen Geschäftsprozessen. Es gibt verschiedene Ursachen für solche Ausfälle, beispielsweise Insolvenz, einseitige Kündigung des Vertrags durch den Dienstleister oder Zulieferer, betriebliche Probleme beispielsweise durch Naturgewalten oder Personalausfall. Probleme können auch entstehen, wenn die vom Dienstleister erbrachten Leistungen nicht den Qualitätsanforderungen des Auftraggebers entsprechen.

Zu beachten ist außerdem, dass Dienstleister ebenfalls häufig auf Unterauftragnehmer zurückgreifen, um ihre Leistungen gegenüber dem Auftraggeber zu erbringen. Störungen, Qualitätsmängel und Ausfälle seitens der Unterauftragnehmer können dadurch indirekt zu Beeinträchtigungen beim Auftraggeber führen.

Auch durch Ausfälle von IT-Systemen beim Dienstleister oder der Kommunikationsanbindungen zu diesem können Geschäftsprozesse beim Auftraggeber beeinträchtigt werden.

Eine gegebenenfalls notwendige Rückholung ausgelagerter Prozesse kann stark erschwert sein, beispielsweise weil die ausgelagerten Verfahren nicht hinreichend dokumentiert sind oder weil der bisherige Dienstleister die Rückholung nicht unterstützt.

Beispiele:

- Ein Unternehmen hat seine Server in einem Rechenzentrum eines externen Dienstleisters installiert. Nach einem Brand in diesem Rechenzentrum war die Finanzabteilung des Unternehmens nicht mehr handlungsfähig. Es entstanden erhebliche finanzielle Verluste für das Unternehmen.
- Die Just-in-Time-Produktion eines Unternehmens war von der Zulieferung von Betriebsmitteln externer Dienstleister abhängig. Nachdem ein LKW durch einen Defekt beim Dienstleister ausfiel, verzögerte sich die Lieferung dringend benötigter Teile drastisch. Eine Reihe von Kunden konnte dadurch nicht fristgerecht beliefert werden.
- Ein Bankinstitut wickelte alle Geldtransporte mit einem Werttransportunternehmen ab. Das Werttransportunternehmen meldete überraschend Konkurs an. Die Vereinbarung und Tourenplanung mit einem neuen Werttransporter dauerte mehrere Tage. Als Folge kam es zu erheblichen Problemen und Zeitverzögerungen bei der Geldversorgung und -entsorgung der Bankfilialen.

G 0.12 Elektromagnetische Störstrahlung

Informationstechnik setzt sich heute zu einem großen Teil aus elektronischen Komponenten zusammen. Zwar wird zunehmend auch optische Übertragungstechnik eingesetzt, dennoch enthalten beispielsweise Computer, Netzkoppelelemente und Speichersysteme in der Regel sehr viele elektronische Bauteile. Durch elektromagnetische Störstrahlung, die auf solche Bauteile einwirkt, können elektronische Geräte in ihrer Funktion beeinträchtigt oder sogar beschädigt werden. Als Folge kann es unter anderem zu Ausfällen, Störungen, falschen Verarbeitungsergebnissen oder Kommunikationsfehlern kommen.

Auch drahtlose Kommunikation kann durch elektromagnetische Störstrahlung beeinträchtigt werden. Hierzu reicht unter Umständen eine ausreichend starke Störung der verwendeten Frequenzbänder.

Weiterhin können Informationen, die auf bestimmten Arten von Datenträgern gespeichert sind, durch elektromagnetische Störstrahlung gelöscht oder verfälscht werden. Dies betrifft insbesondere magnetisierbare Datenträger (Festplatten, Magnetbänder etc.) und Halbleiter-Speicher. Auch eine Beschädigung solcher Datenträger durch elektromagnetische Störstrahlung ist möglich.

Es gibt viele unterschiedliche Quellen elektromagnetischer Felder oder Strahlung, zum Beispiel Funknetze wie WLAN, Bluetooth, GSM, UMTS etc., Dauermagnete und kosmische Strahlung. Außerdem strahlt jedes elektrische Gerät mehr oder weniger starke elektromagnetische Wellen ab, die sich unter anderem durch die Luft und entlang metallischer Leiter (z. B. Kabel, Klimakanäle, Heizungsrohre etc.) ausbreiten können.

In Deutschland enthält das Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) Regelungen zu diesem Thema.

G 0.13 Abfangen kompromittierender Strahlung

Elektrische Geräte strahlen elektromagnetische Wellen ab. Bei Geräten, die Informationen verarbeiten (z. B. Computer, Bildschirme, Netzkoppelelemente, Drucker), kann diese Strahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende oder kompromittierende Abstrahlung genannt. Ein Angreifer, der sich beispielsweise in einem Nachbarhaus oder in einem in der Nähe abgestellten Fahrzeug befindet, kann versuchen, diese Abstrahlung zu empfangen und daraus die verarbeiteten Informationen zu rekonstruieren. Die Vertraulichkeit der Informationen ist damit in Frage gestellt. Eine mögliche Zielsetzung eines solchen Angriffes ist Industriespionage.

Die Grenzwerte des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) reichen im Allgemeinen nicht aus, um das Abfangen der bloßstellenden Abstrahlung zu verhindern. Falls dieses Risiko nicht akzeptiert werden kann, müssen deshalb in aller Regel zusätzliche Schutzmaßnahmen getroffen werden.

Bloßstellende Abstrahlung ist nicht auf elektromagnetische Wellen beschränkt. Auch aus Schallwellen, zum Beispiel bei Druckern oder Tastaturen, können unter Umständen nützliche Informationen gewonnen werden.

Zu beachten ist außerdem, dass bloßstellende Abstrahlung in bestimmten Fällen auch durch äußere Manipulation von Geräten verursacht oder verstärkt werden kann. Wird zum Beispiel ein Gerät mit elektromagnetischen Wellen bestrahlt, kann es passieren, dass die reflektierten Wellen vertrauliche Informationen mit sich führen.

G 0.14 Ausspähen von Informationen (Spionage)

Mit Spionage werden Angriffe bezeichnet, die das Ziel haben, Informationen über Unternehmen, Personen, Produkte oder andere Zielobjekte zu sammeln, auszuwerten und aufzubereiten. Die aufbereiteten Informationen können dann beispielsweise eingesetzt werden, um einem anderem Unternehmen bestimmte Wettbewerbsvorteile zu verschaffen, Personen zu erpressen oder ein Produkt nachbauen zu können.

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen, beispielsweise indem Informationen aus mehreren öffentlich zugänglichen Quellen zusammengeführt werden, die einzeln unverfänglich aussehen, aber in anderen Zusammenhängen kompromittierend sein können. Da vertrauliche Daten häufig nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischem Weg ausgespäht werden.

Beispiele:

- Viele IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzerkennung- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer unter Umständen möglich, dieses auszulesen.
- Um Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN für die verwendete ec- oder Kreditkarte eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn der Angreifer hinterher die Karte stiehlt, kann er damit das Konto plündern.
- Um Zugriffsrechte auf einem PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Neben unmittelbaren Schäden können über Trojanische Pferde vielfältige Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausgespäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.
- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher eventuell Gespräche mithören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

G 0.15 Abhören

Mit Abhören werden gezielte Angriffe auf Kommunikationsverbindungen, Gespräche, Geräuschquellen aller Art oder IT-Systeme zur Informationssammlung bezeichnet. Dies beginnt beim unbemerkten, heimlichen Belauschen eines Gesprächs und reicht bis zu hoch technisierten komplexen Angriffen, um über Funk oder Leitungen gesendete Signale abzufangen, z. B. mit Hilfe von Antennen oder Sensoren.

Nicht nur wegen des geringen Entdeckungsrisikos ist das Abhören von Leitungen oder Funkverbindungen eine nicht zu vernachlässigende Gefährdung der Informationssicherheit. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischen Aufwand feststellbar.

Besonders kritisch ist die ungeschützte Übertragung von Authentisierungsdaten bei Klartextprotokollen wie HTTP, FTP oder Telnet, da diese durch die klare Strukturierung der Daten leicht automatisch zu analysieren sind.

Der Entschluss, irgendwo Informationen abzuhören, wird im Wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig.

Beispiele:

- Bei Telefonaten kann für einen Angreifer nicht nur das Abhören von Gesprächen interessant sein. Auch die Informationen, die bei der Signalisierung übertragen werden, können von einem Angreifer missbraucht werden, z. B. falls durch eine fehlerhafte Einstellung im Endgerät das Passwort bei der Anmeldung im Klartext übertragen wird.
- Bei ungeschützter oder unzureichend geschützter Funkübertragung (z. B. wenn ein WLAN nur mit WEP abgesichert wird), kann ein Angreifer leicht die gesamte Kommunikation abhören.
- E-Mails können während ihres gesamten Weges durch das Netz gelesen werden, wenn sie nicht verschlüsselt sind. Unverschlüsselte E-Mails sollten daher nicht mit klassischen Briefen, sondern mit Postkarten verglichen werden.

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Durch den Diebstahl von Datenträgern, IT-Systemen, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Wenn durch den Diebstahl vertrauliche Informationen offengelegt werden, kann dies weitere Schäden nach sich ziehen. Neben Servern und anderen teuren IT-Systemen werden auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig gestohlen. Es gibt aber auch Fälle, in denen gezielt Datenträger, wie Dokumente oder USB-Sticks, entwendet wurden, um an die darauf gespeicherten vertraulichen Informationen zu gelangen.

Beispiele:

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptographisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Ob Akten kopiert oder manipuliert wurden, konnte nicht zweifelsfrei ausgeschlossen werden.
- In Großbritannien gab es eine Reihe von Datenpannen, bei denen vertrauliche Unterlagen offengelegt wurden, weil Datenträger gestohlen wurden. In einem Fall wurden bei der britischen Luftwaffe mehrere Computer-Festplatten gestohlen, die sehr persönliche Informationen enthielten, die zur Sicherheitsüberprüfung von Mitarbeitern erfasst worden waren.
- Ein Mitarbeiter eines Call-Centers erstellte, kurz bevor er das Unternehmen verlassen musste, Kopien einer großen Menge von vertraulichen Kundendaten. Nach seinem Ausscheiden aus dem Unternehmen hat er diese Daten dann an Wettbewerber verkauft. Da anschließend Details über den Vorfall an die Presse gelangten, verlor das Call-Center viele wichtige Kunden.

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Es gibt eine Vielzahl von Ursachen, die zu einem Verlust von Geräten, Datenträgern und Dokumenten führen können. Hierdurch ist unmittelbar die Verfügbarkeit betroffen, es können aber auch vertrauliche Informationen in fremde Hände gelangen, wenn die Datenträger nicht komplett verschlüsselt sind. Durch die Wiederbeschaffung von Geräten oder Datenträgern entstehen Kosten, aber auch, wenn diese wieder auftauchen, können Informationen offengelegt oder unerwünschte Programme aufgespielt worden sein.

Besonders mobile Endgeräte und mobile Datenträger können leicht verloren gehen. Auf kleinen Speicherkarten können heute riesige Datenmengen gespeichert werden. Es kommt aber auch immer wieder vor, dass Dokumente in Papierform versehentlich liegen gelassen werden, beispielsweise in Gaststätten oder Verkehrsmitteln.

Beispiele:

- Eine Mitarbeiterin nutzt in der Straßenbahn die Fahrt zum Arbeitsplatz, um einige Unterlagen zu sichten. Als sie hektisch an der Zielhaltestelle aussteigt, lässt sie die Papiere versehentlich auf ihrem Nachbarplatz liegen. Zwar sind die Unterlagen nicht vertraulich, in der Folge müssen jedoch mehrere Unterschriften hochrangiger Führungskräfte erneut eingeholt werden.
- Auf einer Großveranstaltung fällt einem Mitarbeiter beim Suchen in seiner Aktentasche versehentlich und unbemerkt eine Speicherkarte mit vertraulichen Kalkulationen auf den Boden. Der Finder sichtet den Inhalt auf seinem Laptop und verkauft die Informationen an die Konkurrenz.
- Ein Hersteller sendet CDs mit Software-Updates zur Fehlerbehebung per Post an seine Kunden. Einige dieser CDs gehen auf dem Versandweg verloren, ohne dass Absender oder Empfänger darüber informiert werden. In der Folge kommt es bei den betroffenen Kunden zu Fehlfunktionen der Software.

G 0.18 Fehlplanung oder fehlende Anpassung

Wenn organisatorische Abläufe, die direkt oder indirekt der Informationsverarbeitung dienen, nicht sachgerecht gestaltet sind, kann dies zu Sicherheitsproblemen führen. Obwohl jeder einzelne Prozessschritt korrekt durchgeführt wird, kommt es oft zu Schäden, weil Prozesse insgesamt fehlerhaft definiert sind.

Eine weitere mögliche Ursache für Sicherheitsprobleme sind Abhängigkeiten mit anderen Prozessen, die selbst keinen offensichtlichen Bezug zur Informationsverarbeitung haben. Solche Abhängigkeiten können bei der Planung leicht übersehen werden und dadurch Beeinträchtigungen während des Betriebes auslösen.

Sicherheitsprobleme können außerdem dadurch entstehen, dass Aufgaben, Rollen oder Verantwortung nicht eindeutig zugewiesen sind. Unter anderem kann es dadurch passieren, dass Abläufe verzögert, Sicherheitsmaßnahmen vernachlässigt oder Regelungen missachtet werden.

Gefahr besteht auch, wenn Geräte, Produkte, Verfahren oder andere Mittel zur Realisierung der Informationsverarbeitung nicht sachgerecht eingesetzt werden. Die Auswahl eines ungeeigneten Produktes oder Schwachstellen beispielsweise in der Anwendungsarchitektur oder im Netzdesign können zu Sicherheitsproblemen führen.

Beispiele:

- Wenn Wartungs- oder Reparaturprozesse nicht auf die fachlichen Anforderungen abgestimmt sind, kann es dadurch zu inakzeptablen Ausfallzeiten kommen.
- Es kann ein erhöhtes Risiko durch Angriffe auf die eigenen IT-Systeme entstehen, wenn sicherheitstechnische Anforderungen bei der Beschaffung von Informationstechnik nicht berücksichtigt werden.
- Wenn benötigtes Verbrauchsmaterial nicht zeitgerecht zur Verfügung gestellt wird, können die davon abhängigen IT-Verfahren ins Stocken geraten.
- Es können Schwachstellen entstehen, wenn bei der Planung eines IT-Verfahrens ungeeignete Übertragungsprotokolle ausgewählt werden.

Die Informationstechnik und das gesamte Umfeld einer Behörde bzw. eines Unternehmens ändern sich ständig. Sei es, dass Mitarbeiter ausscheiden oder hinzukommen, neue Hard- oder Software beschafft wird oder ein Zulieferbetrieb Konkurs anmeldet. Werden die dadurch notwendigen organisatorischen und technischen Anpassungen nicht oder nur ungenügend berücksichtigt, können sich Gefährdungen ergeben.

Beispiele:

- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Da die Mitarbeiter nicht ausreichend unterrichtet wurden, kann das Gebäude nicht in der erforderlichen Zeit geräumt werden.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, ein für die Empfängerseite lesbares Datenformat zu benutzen.

G 0.19 Offenlegung schützenswerter Informationen

Vertrauliche Daten und Informationen dürfen nur den zur Kenntnisnahme berechtigten Personen zugänglich sein. Neben der Integrität und der Verfügbarkeit gehört die Vertraulichkeit zu den Grundwerten der Informationssicherheit. Für vertrauliche Informationen (wie Passwörter, personenbezogene Daten, Firmen- oder Amtsgeheimnisse, Entwicklungsdaten) besteht die inhärente Gefahr, dass diese durch technisches Versagen, Unachtsamkeit oder auch durch vorsätzliche Handlungen offengelegt werden.

Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (USB-Sticks, CDs oder DVDs),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie Informationen offengelegt werden, kann sehr unterschiedlich sein, zum Beispiel:

- unbefugtes Auslesen von Dateien,
- unbedachte Weitergabe, z. B. im Zuge von Reparaturaufträgen,
- unzureichende Löschung oder Vernichtung von Datenträgern,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen,
- Infektion von IT-Systemen mit Schadprogrammen,
- Mitlesen am Bildschirm oder Abhören von Gesprächen.

Werden schützenswerte Informationen offengelegt, kann dies schwerwiegende Folgen für eine Institution haben. Unter anderem kann der Verlust der Vertraulichkeit zu folgenden negativen Auswirkungen für eine Institution führen:

- Verstoß gegen Gesetze, zum Beispiel Datenschutz, Bankgeheimnis,
- Negative Innenwirkung, zum Beispiel Demoralisierung der Mitarbeiter,
- Negative Außenwirkung, zum Beispiel Beeinträchtigung der Beziehungen zu Geschäftspartnern, verlorenes Vertrauen von Kunden,
- Finanzielle Auswirkungen, zum Beispiel Schadensersatzansprüche, Bußgelder, Prozesskosten,
- Beeinträchtigung des informationellen Selbstbestimmungsrechtes.

Ein Verlust der Vertraulichkeit wird nicht immer sofort bemerkt. Oft stellt sich erst später heraus, z. B. durch Presseanfragen, dass Unbefugte sich Zugang zu vertraulichen Informationen verschafft haben.

Beispiel:

- Käufer von gebrauchten Rechnern, Festplatten, Mobiltelefonen oder ähnlichen Geräten finden darauf immer wieder höchst vertrauliche Informationen wie Patientendaten oder Kontonummern.

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Wenn Informationen, Software oder Geräte verwendet werden, die aus unzuverlässigen Quellen stammen oder deren Herkunft und Korrektheit nicht ausreichend geprüft wurden, kann der Einsatz hohe Gefahren mit sich bringen. Dies kann unter anderem dazu führen, dass geschäftsrelevante Informationen auf einer falschen Datenbasis beruhen, dass Berechnungen falsche Ergebnisse liefern oder dass falsche Entscheidungen getroffen werden. Ebenso können aber auch Integrität und Verfügbarkeit von IT-Systemen beeinträchtigt werden.

Beispiele:

- Ein Empfänger kann durch E-Mails, deren Herkunft er nicht geprüft hat, dazu verleitet werden, bestimmte Aktionen durchzuführen, die sich für ihn oder andere nachteilig auswirken. Beispielsweise kann die E-Mail interessante Anhänge oder Links enthalten, die beim Anklicken dazu führen, dass Schadsoftware beim Empfänger installiert wird. Der Absender der E-Mail kann dabei gefälscht oder dem eines bekannten Kommunikationspartners nachgeahmt sein.
- Die Annahme, dass eine Angabe wahr ist, weil es "in der Zeitung steht" oder "im TV ausgestrahlt wurde", ist nicht immer gerechtfertigt. Dadurch können falsche Aussagen in geschäftskritische Berichte eingearbeitet werden.
- Die Zuverlässigkeit von Informationen, die über das Internet verbreitet werden, ist sehr unterschiedlich. Wenn Ausführungen ohne weitere Quellenprüfungen aus dem Internet übernommen werden, können daraus Fehlentscheidungen resultieren.
- Wenn Updates oder Patches aus nicht vertrauenswürdigen Quellen eingespielt werden, kann dies zu unerwünschten Nebenwirkungen führen. Wenn die Herkunft von Software nicht überprüft wird, besteht ein erhöhtes Risiko, dass IT-Systeme mit schädlichem Code infiziert werden.

G 0.21 Manipulation von Hard- oder Software

Als Manipulation wird jede Form von gezielten, aber heimlichen Eingriffen bezeichnet, um Zielobjekte aller Art unbemerkt zu verändern. Manipulationen an Hard- oder Software können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden. Im Fokus können dabei Geräte aller Art, Zubehör, Datenträger (z. B. DVDs, USB-Sticks), Applikationen, Datenbanken oder ähnliches stehen.

Manipulationen an Hard- und Software führen nicht immer zu einem unmittelbaren Schaden. Wenn jedoch die damit verarbeiteten Informationen beeinträchtigt werden, kann dies alle Arten von Sicherheitsauswirkungen nach sich ziehen (Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit). Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse der Täter sind und je tiefgreifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen. Manipulationen können dadurch auch erhebliche Ausfallzeiten nach sich ziehen.

Beispiele:

- In einem Schweizer Finanzunternehmen hatte ein Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Dadurch war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Durch Manipulationen an Geldausgabeautomaten ist es Angreifern mehrfach gelungen, die auf Zahlungskarten gespeicherten Daten unerlaubt auszulesen. In Verbindung mit ausgespähten PINs wurden diese Daten dann später missbraucht, um Geld zulasten der Karteninhaber abzuheben.

G 0.22 Manipulation von Informationen

Informationen können auf vielfältige Weise manipuliert werden, z. B. durch fehlerhaftes oder vorsätzlich falsches Erfassen von Daten, inhaltliche Änderung von Datenbank-Feldern oder von Schriftverkehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

Archivierte Dokumente stellen meist schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.

Beispiel:

- Eine Mitarbeiterin hat sich über die Beförderung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.

G 0.23 Unbefugtes Eindringen in IT-Systeme

Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass darüber unbefugt auf das IT-System zugegriffen wird.

Beispiele:

- Wenn eine Benutzerkennung und das zugehörige Passwort ausgespäht werden, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.
- Über unzureichend gesicherte Fernwartungszugänge könnten Hacker unerlaubt auf IT-Systeme zugreifen.
- Bei unzureichend gesicherten Schnittstellen von aktiven Netzkomponenten ist es denkbar, dass Angreifer einen unberechtigten Zugang zur Netzkomponente erlangen. Wenn es ihnen außerdem gelingt, die lokalen Sicherheitsmechanismen zu überwinden, also z.B. an administrative Berechtigungen gelangt sind, könnten sie alle Administrationstätigkeiten ausüben.
- Viele IT-Systeme haben Schnittstellen für den Einsatz austauschbarer Datenspeicher, wie z. B. Zusatzspeicherkarten oder USB-Speichermedien. Bei einem unbeaufsichtigten IT-System mit der entsprechenden Hard- und Software besteht die Gefahr, dass hierüber große Datenmengen unbefugt ausgelesen oder Schadprogramme eingeschleust werden können.

G 0.24 Zerstörung von Geräten oder Datenträgern

Durch Fahrlässigkeit, unsachgemäße Verwendung aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Datenträgern kommen, die den Betrieb des IT-Systems empfindlich stören können.

Es besteht außerdem die Gefahr, dass durch die Zerstörung wichtige Informationen verloren gehen, die nicht oder nur mit großem Aufwand rekonstruiert werden können.

Beispiele:

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server versteckt aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt, und der Server fiel für mehrere Tage aus.
- Ein Mitarbeiter hatte sich über das wiederholte Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Hierbei wurde die Festplatte durch Fußtritte gegen den Rechner so stark beschädigt, dass sie unbrauchbar wurde. Die hier gespeicherten Daten konnten nur teilweise wieder durch ein Backup vom Vortag rekonstruiert werden.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen.

G 0.25 Ausfall von Geräten oder Systemen

Werden auf einem IT-System zeitkritische Anwendungen betrieben, sind die Folgeschäden nach einem Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider (ISP) führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Als Folge waren mehrere vom ISP betriebene Webserver tagelang nicht erreichbar.

G 0.26 Fehlfunktion von Geräten oder Systemen

Geräte und Systeme, die der Informationsverarbeitung dienen, haben heute häufig viele Funktionen und sind deshalb entsprechend komplex aufgebaut. Grundsätzlich betrifft dies sowohl Hardware- als auch Software-Komponenten. Durch die Komplexität gibt es in solchen Komponenten viele unterschiedliche Fehlerquellen. Als Folge kommt es immer wieder dazu, dass Geräte und Systeme nicht wie vorgesehen funktionieren und dadurch Sicherheitsprobleme entstehen.

Ursachen für Fehlfunktionen gibt es viele, zum Beispiel Materialermüdung, Fertigungstoleranzen, konzeptionelle Schwächen, Überschreitung von Grenzwerten, nicht vorgesehene Einsatzbedingungen oder fehlende Wartung. Da es keine perfekten Geräte und Systeme gibt, muss eine gewisse Restwahrscheinlichkeit für Fehlfunktionen ohnehin immer akzeptiert werden.

Durch Fehlfunktionen von Geräten oder Systemen können alle Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) beeinträchtigt werden. Hinzu kommt, dass Fehlfunktionen unter Umständen auch über einen längeren Zeitraum unbemerkt bleiben können. Dadurch kann es beispielsweise passieren, dass Berechnungsergebnisse verfälscht und nicht rechtzeitig korrigiert werden.

Beispiele:

- Aufgrund eines verstopften Lüftungsgitters kommt es zur Überhitzung eines Speichersystems, das daraufhin nicht komplett ausfällt, sondern nur sporadische Fehlfunktionen aufweist. Erst einige Wochen später wird bemerkt, dass die gespeicherten Informationen unvollständig sind.
- Eine wissenschaftliche Standard-Anwendung wird genutzt, um eine statistische Analyse für einen vorab erhobenen Datenbestand durchzuführen, der in einer Datenbank gespeichert ist. Laut Dokumentation ist die Anwendung jedoch für das eingesetzte Datenbank-Produkt nicht freigegeben. Die Analyse scheint zwar zu funktionieren, durch Stichproben stellt sich allerdings heraus, dass die berechneten Ergebnisse falsch sind. Als Ursache wurden Kompatibilitätsprobleme zwischen der Anwendung und der Datenbank identifiziert.

G 0.27 Ressourcenmangel

Wenn die vorhandenen Ressourcen in einem Bereich unzureichend sind, kann es zu Engpässen in der Versorgung mit diesen Ressourcen bis hin zu Überlastungen und Ausfällen kommen. Je nach Art der betroffenen Ressourcen können durch ein kleines Ereignis, dessen Eintritt zudem vorhersehbar war, im Endeffekt eine Vielzahl von Geschäftsprozessen beeinträchtigt werden. Ressourcenmangel kann im IT-Betrieb und bei Kommunikationsverbindungen auftreten, aber auch in anderen Bereichen einer Institution. Werden für bestimmte Aufgaben nur unzureichende personelle, zeitliche und finanzielle Ressourcen zur Verfügung gestellt, kann das vielfältige negative Auswirkungen haben. Es kann beispielsweise passieren, dass die in Projekten notwendigen Rollen nicht mit geeigneten Personen besetzt werden. Wenn Betriebsmittel wie Hard- oder Software nicht mehr ausreichen, um den Anforderungen gerecht zu werden, können Fachaufgaben unter Umständen nicht erfolgreich bearbeitet werden.

Häufig können personelle, zeitliche, finanzielle, technische und sonstige Mängel im Regelbetrieb für einen begrenzten Zeitraum noch ausgeglichen werden. Unter hohem Zeitdruck werden sie jedoch, beispielsweise in Notfall-Situationen, umso deutlicher.

Ressourcen können auch absichtlich überlastet werden, wenn jemand einen intensiven Bedarf an einem Betriebsmittel vorsätzlich generiert und dadurch eine intensive und dauerhafte Störung des Betriebsmittels provoziert, siehe auch G 0.40 Verhinderung von Diensten (Denial of Service).

Beispiele:

- Überlastete Elektroleitungen erhitzen sich, dies kann bei ungünstiger Verlegung zu einem Schwelbrand führen.
- Werden neue Anwendungen mit einem höheren als zum Planungszeitpunkt berücksichtigten Bandbreitenbedarf auf dem Netz betrieben, kann dies zu einem Verlust der Verfügbarkeit des gesamten Netzes führen, wenn die Netzinfrastruktur nicht ausreichend skaliert werden kann.
- Wenn die Administratoren wegen Überlastung die Protokoll-Dateien der von ihnen betreuten IT nur sporadisch kontrollieren, werden eventuell Angriffe nicht zeitnah erkannt.
- Webserver können durch eine hohe Menge zeitgleich eintreffender Anfragen so überlastet werden, dass ein geregelter Zugriff auf Daten fast unmöglich wird.
- Wenn sich ein Unternehmen in einem Insolvenzverfahren befindet, kann es passieren, dass kein Geld für dringend benötigte Ersatzteile vorhanden ist oder dass wichtige Dienstleister nicht bezahlt werden können.

G 0.28 Software-Schwachstellen oder -Fehler

Für jede Software gilt: je komplexer sie ist, desto häufiger treten Fehler auf. Auch bei intensiven Tests werden meist nicht alle Fehler vor der Auslieferung an die Kunden entdeckt. Werden Software-Fehler nicht rechtzeitig erkannt, können die bei der Anwendung entstehenden Abstürze oder Fehler zu weitreichenden Folgen führen. Beispiele hierfür sind falsche Berechnungsergebnisse, Fehlentscheidungen der Leitungsebene und Verzögerungen beim Ablauf der Geschäftsprozesse.

Durch Software-Schwachstellen oder -Fehler kann es zu schwerwiegenden Sicherheitslücken in einer Anwendung, einem IT-System oder allen damit vernetzten IT-Systemen kommen. Solche Sicherheitslücken können unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

Beispiele:

- Die meisten Warnmeldungen der Computer Emergency Response Teams (CERTs) in den letzten Jahren bezogen sich auf sicherheitsrelevante Programmierfehler. Dies sind Fehler, die bei der Erstellung von Software entstehen und dazu führen, dass diese Software von Angreifern missbraucht werden kann. Ein großer Teil dieser Fehler wurde durch Speicherüberläufe (Buffer Overflow) hervorgerufen.
- Internet-Browser sind heute eine wichtige Software-Komponente auf Clients. Browser werden häufig nicht nur zum Zugriff auf das Internet, sondern auch für interne Web-Anwendungen in Unternehmen und Behörden genutzt. Software-Schwachstellen oder -Fehler in Browsern können deshalb die Informationssicherheit insgesamt besonders stark beeinträchtigen.

G 0.29 Verstoß gegen Gesetze oder Regelungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme einer Institution unzureichend abgesichert sind (beispielsweise durch ein unzureichendes Sicherheitsmanagement), kann dies zu Verstößen gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern führen. Welche Gesetze jeweils zu beachten sind, hängt von der Art der Institution bzw. ihrer Geschäftsprozesse und Dienstleistungen ab. Je nachdem, wo sich die Standorte einer Institution befinden, können auch verschiedene nationale Vorschriften zu beachten sein. Folgende Beispiele verdeutlichen dies:

- Der Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt. Dazu gehören das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl bereichsspezifischer Regelungen.
- Die Geschäftsführung eines Unternehmens ist dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. In Deutschland gelten verschiedene Rechtsvorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder AktG (Aktiengesetz), aus denen sich zu Risikomanagement und Informationssicherheit entsprechende Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.
- Die ordnungsmäßige Verarbeitung von buchungsrelevanten Daten ist in verschiedenen Gesetzen und Vorschriften geregelt. In Deutschland sind dies unter anderem das Handelsgesetzbuch (z. B. HGB §§ 238 ff.) und die Abgabenordnung (AO). Die ordnungsmäßige Verarbeitung von Informationen umfasst natürlich deren sichere Verarbeitung. Beides muss in vielen Ländern regelmäßig nachgewiesen werden, beispielsweise durch Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses. Falls hierbei gravierende Sicherheitsmängel festgestellt werden, kann kein positiver Prüfungsbericht erstellt werden.
- In vielen Branchen (z.B. der Automobil-Industrie) ist es üblich, dass Hersteller ihre Zulieferer zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an die Informationssicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen nach sich ziehen.

Nur wenige Sicherheitsanforderungen ergeben sich unmittelbar aus Gesetzen. Die Gesetzgebung orientiert sich jedoch im Allgemeinen am Stand der Technik als allgemeine Bewertungsgrundlage für den Grad der erreichbaren Sicherheit. Stehen bei einer Institution die vorhandenen Sicherheitsmaßnahmen in keinem gesunden Verhältnis zu den zu schützenden Werten und dem Stand der Technik, kann dies gravierende Folgen haben.

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Ohne geeignete Mechanismen zur Zutritts-, Zugriffs- und Zugangskontrolle kann eine unberechtigte Nutzung von Geräten und Systemen praktisch nicht verhindert oder erkannt werden. Bei IT-Systemen ist der grundlegende Mechanismus die Identifikation und Authentisierung von Benutzern. Aber selbst bei IT-Systemen mit einer starken Identifikations- und Authentisierungsfunktion ist eine unberechtigte Nutzung denkbar, wenn die entsprechenden Sicherheitsmerkmale (Passwörter, Chipkarten, Token etc.) in falsche Hände gelangen. Auch bei der Vergabe und Pflege von Berechtigungen können viele Fehler gemacht werden, beispielsweise wenn Berechtigungen zu weitreichend oder an unautorisierte Personen vergeben oder nicht zeitnah aktualisiert werden.

Unbefugte können durch die unberechtigte Nutzung von Geräten und Systemen an vertrauliche Informationen gelangen, Manipulationen vornehmen oder Störungen verursachen.

Ein besonders wichtiger Spezialfall der unberechtigten Nutzung ist die unberechtigte Administration. Wenn Unbefugte die Konfiguration oder die Betriebsparameter von Hardware- oder Software-Komponenten ändern, können daraus schwere Schäden resultieren.

Beispiel:

- Bei der Kontrolle von Protokollierungsdaten stieß ein Netzadministrator auf zunächst unerklärliche Ereignisse, die an verschiedenen Tagen, aber häufig am frühen Morgen und am Nachmittag aufgetreten sind. Bei näherer Untersuchung stellte sich heraus, dass ein WLAN-Router unsicher konfiguriert war. Wartende Personen an der Bushaltestelle vor dem Firmengebäude haben diesen Zugang genutzt, um während der Wartezeit mit ihren mobilen Endgeräten im Internet zu surfen.

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann deren Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. Dies führt häufig zu Störungen oder Ausfällen. Je nachdem, welche Arten von Geräten oder Systemen falsch genutzt werden, können aber auch Vertraulichkeit und Integrität von Informationen verletzt werden.

Ein besonders wichtiger Spezialfall der fehlerhaften Nutzung ist die fehlerhafte Administration. Fehler bei der Installation, Konfiguration, Wartung und Pflege von Hardware- oder Software-Komponenten können schwere Schäden nach sich ziehen.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu Sicherheitsvorfällen führen.

Gleichermaßen können durch die fehlerhafte Bedienung von IT-Systemen oder Anwendungen auch Daten versehentlich gelöscht oder verändert werden. Dadurch könnten aber auch vertrauliche Informationen an die Öffentlichkeit gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

Wenn Strom- oder Netzkabel ungeschützt verlegt werden, können sie unbeabsichtigt beschädigt werden, wodurch Verbindungen ausfallen können. Geräteanschlussleitungen können herausgerissen werden, wenn Mitarbeiter oder Besucher darüber stolpern.

G 0.32 Missbrauch von Berechtigungen

Abhängig von ihren Rollen und Aufgaben erhalten Personen entsprechende Zutritts-, Zugangs- und Zugriffsberechtigungen. Auf diese Weise soll einerseits der Zugang zu Informationen gesteuert und kontrolliert werden, und andererseits soll es den Personen ermöglicht werden, bestimmte Aufgaben zu erledigen. Beispielsweise benötigen Personen oder Gruppen bestimmte Berechtigungen, um Anwendungen ausführen zu können oder Informationen bearbeiten zu können.

Eine missbräuchliche Nutzung von Berechtigungen liegt vor, wenn vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten außerhalb des vorgesehenen Rahmens genutzt werden. Ziel dabei ist häufig, sich persönliche Vorteile zu verschaffen oder einer Institution oder bestimmten Personen zu schaden.

In nicht wenigen Fällen verfügen Personen aus historischen, systemtechnischen oder anderen Gründen über höhere oder umfangreichere Zutritts-, Zugangs- oder Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können unter Umständen für Angriffe missbraucht werden.

Beispiele:

- Je feingranularer die Zugriffsrechte auf Informationen gestaltet werden, desto größer ist oft auch der Pflegeaufwand, um diese Berechtigungen auf dem aktuellen Stand zu halten. Es besteht deshalb die Gefahr, dass bei der Vergabe der Zugriffsrechte zu wenig zwischen den unterschiedlichen Rollen differenziert wird und dadurch der Missbrauch der Berechtigungen erleichtert wird.
- Bei verschiedenen Anwendungen werden Zugriffsberechtigungen oder Passwörter in Systembereichen gespeichert, auf die auch andere Benutzer zugreifen können. Dadurch könnten Angreifer die Berechtigungen ändern oder Passwörter auslesen.
- Personen mit zu großzügig vergebenen Berechtigungen könnten versucht sein, auf fremde Dateien zuzugreifen, beispielsweise eine fremde E-Mail einzusehen, weil bestimmte Informationen dringend benötigt werden.

G 0.33 Personalausfall

Der Ausfall von Personal kann erhebliche Auswirkungen auf eine Institution und deren Geschäftsprozesse haben. Personal kann beispielsweise durch Krankheit, Unfall, Tod oder Streik unvorhergesehen ausfallen. Des weiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird. Ein Personalausfall kann auch durch einen internen Wechsel des Arbeitsplatzes verursacht werden.

Beispiele:

- Aufgrund längerer Krankheit blieb der Netzadministrator einer Firma vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben, da es nur diesen in den Netzbetrieb eingearbeiteten Administrator gab. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs eines Administrators musste in einer Institution auf die Backup-Medien im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kurz zuvor geändert und war nur diesem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Administrator nicht eher im Urlaub erreichbar war.
- Im Falle eine Pandemie fällt nach und nach längerfristig immer mehr Personal aus, sei es durch die Krankheit selbst, durch die notwendige Pflege von Angehörigen oder durch die Betreuung von Kindern. Auch aus Angst vor Ansteckung in öffentlichen Verkehrsmitteln oder in der Institution bleiben einige Mitarbeiter vom Dienst fern. Als Folge können nur noch die notwendigsten Arbeiten erledigt werden. Die erforderliche Wartung der Systeme, sei es der zentrale Server oder die Klimaanlage im Rechenzentrum, ist nicht mehr zu leisten. Nach und nach fallen dadurch immer mehr Systeme aus.

G 0.34 Anschlag

Durch einen Anschlag kann eine Institution, bestimmte Bereiche der Institution oder einzelne Personen bedroht werden. Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung. Ob und in welchem Umfang eine Institution der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von ihren Aufgaben und vom politisch-sozialen Klima ab. Unternehmen und Behörden, die in politisch kontrovers diskutierten Bereichen agieren, sind stärker bedroht als andere. Institutionen in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Orten. Für die Einschätzung der Gefährdung oder bei Verdacht auf Bedrohungen durch politisch motivierte Anschläge können in Deutschland die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

Beispiele:

- In den 1980er-Jahren wurde ein Sprengstoffanschlag auf das Rechenzentrum einer großen Bundesbehörde in Köln verübt. Durch die große Durchschlagskraft des Sprengkörpers wurden nicht nur Fenster und Wände, sondern auch viele IT-Systeme im Rechenzentrum zerstört.
- Bei dem Anschlag auf das World-Trade-Center in New York am 11. September 2001 wurden nicht nur viele Menschen getötet, sondern es wurden auch zahlreiche IT-Einrichtungen zerstört. Als Folge hatten mehrere Unternehmen erhebliche Schwierigkeiten, ihre Geschäftstätigkeiten fortzusetzen.

G 0.35 Nötigung, Erpressung oder Korruption

Nötigung, Erpressung oder Korruption können dazu führen, dass die Sicherheit von Informationen oder Geschäftsprozessen beeinträchtigt wird. Durch Androhung von Gewalt oder anderen Nachteilen kann ein Angreifer beispielsweise versuchen, das Opfer zur Missachtung von Sicherheitsrichtlinien oder zur Umgehung von Sicherheitsmaßnahmen zu bringen (Nötigung).

Anstatt zu drohen, können Angreifer auch gezielt Geld oder andere Vorteile anbieten, um Mitarbeiter oder andere Personen zum Instrument für Sicherheitsverletzungen zu machen (Korruption). Beispielsweise besteht die Gefahr, dass ein bestechlicher Mitarbeiter vertrauliche Dokumente an Unbefugte weiterleitet.

Durch Nötigung oder Korruption können grundsätzlich alle Grundwerte der Informationssicherheit beeinträchtigt werden. Angriffe können unter anderem darauf abzielen, vertrauliche Informationen an Unbefugte zu leiten, geschäftskritische Informationen zu manipulieren oder den reibungslosen Ablauf von Geschäftsprozessen zu stören.

Besondere Gefahr besteht, wenn sich solche Angriffe gegen hochrangige Führungskräfte oder Personen in besonderen Vertrauensstellungen richten.

G 0.36 Identitätsdiebstahl

Beim Identitätsdiebstahl täuscht ein Angreifer eine falsche Identität vor, er benutzt also Informationen über eine andere Person, um in deren Namen aufzutreten. Hierfür werden Daten wie beispielsweise Geburtsdatum, Anschrift, Kreditkarten- oder Kontonummern benutzt, um sich beispielsweise auf fremde Kosten bei einem Internet-Dienstleister anzumelden oder sich auf andere Weise zu bereichern. Identitätsdiebstahl führt häufig auch direkt oder indirekt zur Rufschädigung, aber verursacht auch einen hohen Zeitaufwand, um die Ursachen aufzuklären und negative Folgen für die Betroffenen abzuwenden. Einige Formen des Identitätsbetrugs werden auch als Maskerade bezeichnet.

Identitätsdiebstahl tritt besonders dort häufig auf, wo die Identitätsprüfung zu nachlässig gehandhabt wird, vor allem, wenn hierauf teure Dienstleistungen basieren.

Eine Person, die über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.

Beispiele:

- Bei verschiedenen E-Mail-Providern und Auktionsplattformen im Internet reichte es zur Anmeldung anfangs, sich einen Phantasienamen auszudenken und diesen mit einer passenden Adresse aus dem Telefonbuch zu unterlegen. Zunächst konnten sich Angreifer auch unter erkennbar ausgedachten Namen anmelden, beispielsweise von Comicfiguren. Als dann schärfere Plausibilitätstests eingeführt wurden, sind hierfür auch Namen, Adressen und Kontonummern von echten Personen verwendet worden. Die Betroffenen haben hiervon erst erfahren, als die ersten Zahlungsaufforderungen bei ihnen eintrafen.
- Die Absender-Adressen von E-Mails lassen sich leicht fälschen. Es passiert immer wieder, dass Anwendern auf diese Weise vorgetäuscht wird, dass eine E-Mail von einem vertrauenswürdigen Kommunikationspartner stammt. Ähnliche Angriffe sind durch die Manipulation der Rufnummernanzeige bei Sprachverbindungen oder durch die Manipulation der Absenderkennung bei Faxverbindungen möglich.
- Ein Angreifer kann durch eine Maskerade versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde.

G 0.37 Abstreiten von Handlungen

Personen können aus verschiedenen Gründen abstreiten, bestimmte Handlungen begangen zu haben, beispielsweise weil diese Handlungen gegen Anweisungen, Sicherheitsvorgaben oder sogar Gesetze verstoßen. Sie könnten aber auch leugnen, eine Benachrichtigung erhalten zu haben, zum Beispiel weil sie einen Termin vergessen haben. Im Bereich der Informationssicherheit wird daher häufig die Verbindlichkeit hervorgehoben, eine Eigenschaft, über die sichergestellt werden soll, dass erfolgte Handlungen nicht unberechtigt abgestritten werden können. Im englischen Sprachraum wird dafür der Begriff Non-Repudiation (Nichtabstreitbarkeit) verwendet.

Bei Kommunikation wird zusätzlich unterschieden, ob ein Kommunikationsteilnehmer den Nachrichtenempfang ableugnet (Repudiation of Receipt) oder den Versand (Repudiation of Origin). Den Nachrichtenempfang abzuleugnen kann unter anderem bei finanziellen Transaktionen von Bedeutung sein, z. B. wenn jemand bestreitet, eine Rechnung fristgemäß erhalten zu haben. Ebenso kann es passieren, dass ein Kommunikationsteilnehmer den Nachrichtenversand ableugnet, z.B. also eine getätigte Bestellung abstreitet. Nachrichtenversand oder -empfang kann beim Postversand ebenso abgeleugnet werden wie bei Fax- oder E-Mail-Nutzung.

Beispiel:

- Ein dringend benötigtes Ersatzteil wird elektronisch bestellt. Nach einer Woche wird das Fehlen reklamiert, inzwischen sind durch den Produktionsausfall hohe Kosten entstanden. Der Lieferant leugnet, je eine Bestellung erhalten zu haben.

G 0.38 Missbrauch personenbezogener Daten

Personenbezogene Daten sind fast immer besonders schützenswerte Informationen. Typische Beispiele sind Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Wenn der Schutz personenbezogener Daten nicht ausreichend gewährleistet ist, besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Ein Missbrauch personenbezogener Daten kann beispielsweise vorliegen, wenn eine Institution zu viele personenbezogene Daten sammelt, sie ohne Rechtsgrundlage oder Einwilligung erhoben hat, sie zu einem anderen als dem bei der Erhebung zulässigen Zweck nutzt, personenbezogene Daten zu spät löscht oder unberechtigt weitergibt.

Beispiele:

- Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben oder erstmals gespeichert worden sind. Es ist daher unzulässig, Protokolldateien, in denen die An- und Abmeldung von Benutzern an IT-Systemen ausschließlich für die Zugriffskontrolle festgehalten werden, zur Anwesenheits- und Verhaltenskontrolle zu nutzen.
- Personen, die Zugriff auf personenbezogene Daten haben, könnten diese unbefugt weitergeben. Beispielsweise könnte ein Mitarbeiter am Empfang eines Hotels die Anmeldedaten von Gästen an Werbefirmen verkaufen.

G 0.39 Schadprogramme

Ein Schadprogramm ist eine Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Zu den typischen Arten von Schadprogrammen gehören unter anderem Viren, Würmer und Trojanische Pferde. Schadprogramme werden meist heimlich, ohne Wissen und Einwilligung des Benutzers aktiv.

Schadprogramme bieten heutzutage einem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Unter anderem können Schadprogramme gezielt Passwörter ausforschen, Systeme fernsteuern, Schutzsoftware deaktivieren und Daten ausspionieren.

Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Informationen oder Anwendungen von größter Tragweite. Aber auch der Imageverlust und der finanzielle Schaden, der durch Schadprogramme entstehen kann, sind von großer Bedeutung.

Beispiele:

- In der Vergangenheit verbreitete sich das Schadprogramm W32/Bugbear auf zwei Wegen: Es suchte in lokalen Netzen nach Computern mit Freigaben, auf die schreibender Zugriff möglich war, und kopierte sich darauf. Zudem schickte es sich selbst als HTML-E-Mail an Empfänger im E-Mail-Adressbuch von befallenen Computern. Durch einen Fehler in der HTML-Routine bestimmter E-Mail-Programme wurde das Schadprogramm dort beim Öffnen der Nachricht ohne weiteres Zutun des Empfängers ausgeführt.
- Das Schadprogramm W32/Klez verbreitete sich in verschiedenen Varianten. Befallene Computer schickten den Virus an alle Empfänger im E-Mail-Adressbuch des Computers. Hatte dieser Virus einen Computer befallen, verhinderte er durch fortlaufende Manipulationen am Betriebssystem die Installation von Viren-Schutzprogrammen verbreiteter Hersteller und erschwerte so die Desinfektion der befallenen Computer erheblich.

G 0.40 Verhinderung von Diensten (Denial of Service)

Es gibt eine Vielzahl verschiedener Angriffsformen, die darauf abzielen, die vorgesehene Nutzung bestimmter Dienstleistungen, Funktionen oder Geräte zu verhindern. Der Oberbegriff für solche Angriffe ist "Verhinderung von Diensten" (englisch: "Denial of Service"). Häufig wird auch die Bezeichnung "DoS-Angriff" verwendet.

Solche Angriffe können unter anderem von verärgerten Mitarbeitern oder Kunden, aber auch von Mitbewerbern, Erpressern oder politisch motivierten Tätern ausgehen. Das Ziel der Angriffe können geschäftsrelevante Werte aller Art sein. Typische Ausprägungen von DoS-Angriffen sind

- Störungen von Geschäftsprozessen, z. B. durch Überflutung der Auftragsannahme mit fehlerhaften Bestellungen,
- Beeinträchtigungen der Infrastruktur, z. B. durch Blockieren der Türen der Institution,
- Herbeiführen von IT-Ausfällen, indem z. B. Dienste eines Servers im Netz gezielt überlastet werden.

Diese Art von Angriffen steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass sie den eigentlichen Nutzern nicht mehr zur Verfügung stehen. Bei IT-basierten Angriffen können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Arbeitsspeicher, Plattenplatz, Übertragungskapazität.

Beispiel:

- Im Frühjahr 2007 fanden über einen längeren Zeitraum starke DoS-Angriffe auf zahlreiche Internet-Angebote in Estland statt. Dadurch kam es in Estland zu erheblichen Beeinträchtigungen bei der Nutzung von Informationsangeboten und Dienstleistungen im Internet.

G 0.41 Sabotage

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen oder Prozessen mit dem Ziel, dem Opfer dadurch Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter, punktuell manipuliert werden, um Betriebsstörungen hervorzurufen. Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

Beispiele:

- In einem großen Rechenzentrum führte die Manipulation an der USV zu einem vorübergehenden Totalausfall. Der Täter hatte wiederholt die USV von Hand auf Bypass geschaltet und dann die Hauptstromversorgung des Gebäudes manipuliert. Insgesamt fanden in drei Jahren vier Ausfälle statt. Teilweise kam es sogar zu Hardware-Schäden. Die Betriebsunterbrechungen dauerten zwischen 40 und 130 Minuten.
- Innerhalb eines Rechenzentrums waren auch sanitäre Einrichtungen untergebracht. Durch Verstopfen der Abflüsse und gleichzeitiges Öffnen der Wasserzufuhr drang Wasser in zentrale Technikkomponenten ein. Die auf diese Weise verursachten Schäden führten zu Betriebsunterbrechungen des Produktivsystems.
- Für elektronische Archive stellt Sabotage ein besonderes Risiko dar, da hier meist auf kleinem Raum viele schützenswerte Dokumente verwahrt werden. Dadurch kann unter Umständen durch gezielte, wenig aufwendige Manipulationen ein großer Schaden verursacht werden.

G 0.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Wenn sich Angreifer unerlaubt Passwörter oder andere Authentisierungsmerkmale verschaffen, beispielsweise mit Hilfe von Social Engineering, wird dies häufig auch als "Phishing" (Kunstwort aus "Password" und "Fishing") bezeichnet.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

G 0.43 Einspielen von Nachrichten

Angreifer senden bei dieser Angriffsform speziell vorbereitete Nachrichten an Systeme oder Personen mit dem Ziel, für sich selbst einen Vorteil oder einen Schaden für das Opfer zu erreichen. Um die Nachrichten geeignet zu konstruieren, nutzen die Angreifer beispielsweise Schnittstellenbeschreibungen, Protokollspezifikationen oder Aufzeichnungen über das Kommunikationsverhalten in der Vergangenheit.

Es gibt zwei in der Praxis wichtige Spezialfälle des Einspielens von Nachrichten:

- Bei einer "Replay-Attacke" (Wiedereinspielen von Nachrichten) zeichnen Angreifer gültige Nachrichten auf und spielen diese Information zu einem späteren Zeitpunkt (nahezu) unverändert wieder ein. Es kann auch ausreichen, nur Teile einer Nachricht, wie beispielsweise ein Passwort, zu benutzen, um unbefugt in ein IT-System einzudringen.
- Bei einer "Man-in-the-Middle-Attacke" nimmt der Angreifer unbemerkt eine Vermittlungsposition in der Kommunikation zwischen verschiedenen Teilnehmern ein. In der Regel täuscht er hierzu dem Absender einer Nachricht vor, der eigentliche Empfänger zu sein, und er täuscht dem Empfänger vor, der eigentliche Absender zu sein. Wenn dies gelingt, kann der Angreifer dadurch Nachrichten, die nicht für ihn bestimmt sind, entgegennehmen und vor der Weiterleitung an den eigentlichen Empfänger auswerten und gezielt manipulieren.

Eine Verschlüsselung der Kommunikation bietet keinen Schutz vor Man-in-the-Middle-Attacken, wenn keine sichere Authentisierung der Kommunikationspartner stattfindet.

Beispiele:

- Ein Angreifer zeichnet die Authentisierungsdaten (z. B. Benutzerkennung und Passwort) während des Anmeldevorgangs eines Benutzers auf und verwendet diese Informationen, um sich Zugang zu einem System zu verschaffen. Bei rein statischen Authentisierungsprotokollen kann damit auch ein verschlüsselt übertragenes Passwort benutzt werden, um unbefugt auf ein fremdes System zuzugreifen.
- Um finanziellen Schaden beim Arbeitgeber (Unternehmen oder Behörde) zu verursachen, gibt ein Mitarbeiter eine genehmigte Bestellung mehrmals auf.

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Wenn Unbefugte in ein Gebäude oder einzelne Räumlichkeiten eindringen, kann dies verschiedene andere Gefahren nach sich ziehen. Dazu gehören beispielsweise Diebstahl oder Manipulation von Informationen oder IT-Systemen. Bei qualifizierten Angriffen ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können.

Häufig wollen die Täter wertvolle IT-Komponenten oder andere Waren, die leicht veräußert werden können, stehlen. Ziel eines Einbruchs kann es jedoch unter anderem auch sein, an vertrauliche Informationen zu gelangen, Manipulationen vorzunehmen oder Geschäftsprozesse zu stören.

Durch das unbefugte Eindringen in Räumlichkeiten können somit mehrere Arten von Schäden entstehen:

- Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und/oder Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.
- Entwendete, beschädigte oder zerstörte Geräte oder Komponenten müssen repariert oder ersetzt werden.
- Es können Schäden durch die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder Anwendungen entstehen.

Beispiele:

- Vandalismus
- Bei einem Einbruch in ein Unternehmen an einem Wochenende wurde nur Bagatellschaden durch Aufhebeln eines Fensters angerichtet, lediglich eine Kaffeekasse und kleinere Einrichtungsgegenstände wurden entwendet. Bei einer Routinekontrolle wurde jedoch später festgestellt, dass ein zentraler Server genau zum Zeitpunkt des Einbruchs geschickt manipuliert wurde.

G 0.45 Datenverlust

Ein Datenverlust ist ein Ereignis, das dazu führt, dass ein Datenbestand nicht mehr wie erforderlich genutzt werden kann (Verlust der Verfügbarkeit). Eine häufige Form des Datenverlustes ist, dass Daten unbeabsichtigt oder unerlaubt gelöscht werden, zum Beispiel durch Fehlbedienung, Fehlfunktionen, Stromausfälle, Verschmutzung oder Schadsoftware.

Ein Datenverlust kann jedoch auch durch Beschädigung, Verlust oder Diebstahl von Geräten oder Datenträgern entstehen. Dieses Risiko ist bei mobilen Endgeräten und mobilen Datenträgern häufig besonders hoch.

Weiterhin ist zu beachten, dass viele mobile IT-Systeme nicht immer online sind. Die auf diesen Systemen gespeicherten Daten befinden sich daher nicht immer auf dem aktuellsten Stand. Wenn Datenbestände zwischen mobilen IT-Systemen und stationären IT-Systemen synchronisiert werden, kann es durch Unachtsamkeit oder Fehlfunktion zu Datenverlusten kommen.

Beispiele:

- Der PDA fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Mobiltelefon wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Solche und ähnliche Ereignisse sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Es gibt Schadprogramme, die gezielt Daten auf infizierten IT-Systemen löschen. Bei einigen Schädlingen wird die Löschfunktion nicht sofort bei der Infektion ausgeführt, sondern erst, wenn ein definiertes Ereignis eintritt, zum Beispiel wenn die Systemuhr ein bestimmtes Datum erreicht.
- Viele Internet-Dienste können genutzt werden, um online Informationen zu speichern. Wenn das Passwort vergessen wird und nicht hinterlegt ist, kann es passieren, dass auf die gespeicherten Informationen nicht mehr zugegriffen werden kann, sofern der Dienstleister kein geeignetes Verfahren zum Zurücksetzen des Passwortes anbietet.
- Festplatten und andere Massenspeichermedien haben nur eine begrenzte Lebensdauer. Wenn keine geeigneten Redundanzmaßnahmen getroffen sind, kann es durch technische Defekte zu Datenverlusten kommen.

G 0.46 Integritätsverlust schützenswerter Informationen

Die Integrität von Informationen kann durch verschiedene Ursachen beeinträchtigt werden, z. B. durch Manipulationen, Fehlverhalten von Personen, Fehlbedienung von Anwendungen, Fehlfunktionen von Software oder Übermittlungsfehler.

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Übertragungsfehler: Bei der Datenübertragung kann es zu Übertragungsfehlern kommen.
- Schadprogramme: Durch Schadprogramme können ganze Datenbestände verändert oder zerstört werden.
- Fehleingaben: Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die häufig lange Zeit nicht bemerkt werden.
- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

Wenn Informationen nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Informationen können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.
- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren (hier reicht die Änderung eines Bits), können sie unter Umständen nicht mehr entschlüsselt bzw. entpackt werden.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.
- Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

IT-gestützte Angriffe können Auswirkungen haben, die

- von den Tätern nicht beabsichtigt sind oder
- nicht die unmittelbar angegriffenen Zielobjekte betreffen oder
- unbeteiligte Dritte schädigen.

Ursächlich hierfür sind die hohe Komplexität und Vernetzung moderner Informationstechnik sowie die Tatsache, dass die Abhängigkeiten der angegriffenen Zielobjekte und der zugehörigen Prozesse in der Regel nicht offenkundig sind.

Dadurch kann es unter anderem dazu kommen, dass der tatsächliche Schutzbedarf von Zielobjekten falsch eingeschätzt wird oder dass die Verantwortlichen für die Zielobjekte kein Eigeninteresse an der Behebung von Mängeln dieser Zielobjekte haben.

Beispiele:

- Auf IT-Systemen installierte Bots, mit denen die Täter verteilte Denial-of-Service-Angriffe (DDoS-Angriffe) durchführen können, stellen für die infizierten IT-Systeme selbst oft keine direkte Gefahr dar, weil sich die DDoS-Angriffe in der Regel gegen IT-Systeme Dritter richten.
- Schwachstellen von IoT-Geräten in WLANs können von Tätern als Einfallstor genutzt werden, um andere wichtigere Geräte im gleichen WLAN anzugreifen. Deshalb müssen solche IoT-Geräte auch dann geschützt werden, wenn sie selbst nur einen geringen Schutzbedarf haben.
- Ransomware-Angriffe auf IT-Systeme können unter Umständen Kettenreaktionen auslösen und damit auch Kritische Infrastrukturen treffen. Dies wiederum könnte zu Versorgungsengpässen der Bevölkerung führen, auch wenn die Täter dies möglicherweise gar nicht beabsichtigt haben.