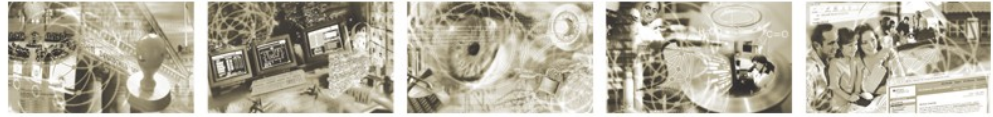




Bundesamt
für Sicherheit in der
Informationstechnik



Sicherer Fernzugriff auf das interne Netz (ISi-Fern)

BSI-Leitlinie zur Internet-Sicherheit (ISi-L)

Vervielfältigung und Verbreitung

Bitte beachten Sie, dass das Werk einschließlich aller Teile urheberrechtlich geschützt ist.

Erlaubt sind die Vervielfältigung und Verbreitung zu nicht-kommerziellen Zwecken, insbesondere zu Zwecken der Ausbildung, Schulung, Information oder hausinternen Bekanntmachung, sofern sie unter Hinweis auf die ISi-Reihe des BSI als Quelle erfolgen.

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

<https://www.bsi.bund.de> oder <http://www.isi-reihe.de>

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: <http://www.bsi.bund.de>
© Bundesamt für Sicherheit in der Informationstechnik 2010

Inhaltsverzeichnis

1 Leitlinie zum sicheren Fernzugriff.....	4
1.1 Management Summary.....	4
1.2 Einführung und Überblick	5
1.2.1 Endgeräte	5
1.2.2 Netzzugang der Endgeräte.....	5
1.2.3 Komponenten des Fernzugriffs im Netz der Institution.....	6
1.2.4 Typische Anwendungen beim Fernzugriff.....	6
1.3 Wesentliche Ergebnisse der Gefährdungsanalyse.....	7
1.3.1 Verlust des Endgerätes.....	7
1.3.2 Gefährdungen durch Schadprogramme.....	7
1.3.3 Ausfall des Fernzugriffs.....	8
1.3.4 Manipulation des Fernzugriffs.....	8
1.4 Wesentliche Empfehlungen.....	8
1.4.1 Grundarchitektur.....	9
1.4.2 Grundlegende Sicherheitsmerkmale	11
1.5 Fazit.....	13
2 Glossar.....	14
3 Stichwort- und Abkürzungsverzeichnis.....	20

1 Leitlinie zum sicheren Fernzugriff

Der Fernzugriff ermöglicht externen Mitarbeitern einer Institution den Zugang zum Netz der Institution. So sind für sie bestimmte Anwendungen auch außerhalb der Institution nutzbar und sie können unabhängig von einem bestimmten Standort tätig sein. Die bisherigen Unterschiede des Arbeitens innerhalb und außerhalb des Netzes der Institution verschwinden. Das Modul ISi-Fern vermittelt die grundlegenden Sicherheitsempfehlungen zu den Basistechniken, die für den Fernzugriff auf das Netz einer Institution erforderlich sind.

Die vorliegende Leitlinie baut auf der BSI-Studie „Sicherer Fernzugriff (ISi-Fern)“ auf, die thematisch an die BSI-Studie „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)“ anschließt. Im Folgenden wird ein Überblick über den Fernzugriff, die wesentlichen Gefährdungen, die grundlegenden Architekturelemente und die entsprechenden Empfehlungen gegeben.

1.1 Management Summary

In Verwaltung, Wirtschaft und anderen Bereichen wächst die Notwendigkeit, auf Daten und Anwendungen einer Institution unabhängig vom Standort dieser Institution zuzugreifen. Mitarbeiter sollen z. B. sowohl am Heimarbeitsplatz als auch bei Fortbildungen und anderen Geschäftsreisen stets erreichbar sein und auf Daten und Anwendungen zugreifen können. Firmen und Behörden müssen daher Fernzugriffsmöglichkeiten auf ihre zentralen EDV-Systeme einrichten.

Diese Fernzugriffsmöglichkeiten können mit unterschiedlichen Endgeräten (Desktop, Laptop, Smartphone) realisiert werden. Die Verbindung zwischen dem Endgerät und der Zentrale führt in der Regel über das Internet, auf das wiederum über DSL-Anschlussleitungen, UMTS, WLAN, Wi-Max oder öffentliche Telefonnetze zugegriffen werden kann.

Der Fernzugriff auf zentrale EDV-Systeme und deren Daten birgt aber auch Risiken. Die Endgeräte befinden sich außerhalb der geschützten Gebäude der Institution und können gestohlen oder einfach vergessen werden. Diebe bzw. Finder dieser Endgeräte haben die Möglichkeit, vertrauliche Daten aus den Endgeräten zu lesen und zu missbrauchen. Im Extremfall reicht den Dieben der alleinige Besitz des Endgeräts, um in das zentrale Netz der zugehörigen Institution einzudringen und dort Spionage oder Sabotage zu betreiben. Die Daten können sogar ohne einen physischen Zugriff ausgespäht werden, indem der Angreifer z. B. unbemerkt hinter dem Benutzer steht und so über dessen Schulter blickend die Eingaben des Benutzers mitverfolgt (Shoulder Surfing). Des Weiteren können Schadprogramme aus dem Internet dazu führen, dass Angreifer die Kontrolle über das Endgerät gewinnen und Schaden verursachen.

Diesen Risiken begegnet die in der Studie „ISi-Fern“ vorgestellte Grundarchitektur für den normalen Schutzbedarf. Zusätzlich ermöglichen die Varianten sowohl für den normalen als auch für den hohen Schutzbedarf die Anpassung an individuelle Gegebenheiten.

Zu den wichtigsten Maßnahmen der Grundarchitektur gehören:

- eine erfolgreiche Authentifizierung des Benutzers gegenüber seinem Endgerät und dem Netz der Institution
- Verschlüsselung der Daten auf dem Endgerät und eine regelmäßige Sicherung der Daten im Netz der Institution, um die auf dem Endgerät gespeicherten Daten vor Verlust und gegen Vertraulichkeitsverletzungen zu schützen
- Einsatz eines kryptografisch gesicherten VPN, um die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution vor unbefugtem Mitlesen zu schützen.

Wurde ein Endgerät entwendet oder gestohlen, lässt sich der Fernzugriff des betroffenen Benutzers durch die Institution kurzfristig sperren. Zusätzlich weist eine Anwenderrichtlinie den Benutzer auf seine Sorgfaltspflichten hin, um so die Risiken durch Nachlässigkeit zu reduzieren. Die Maßnahmen der ISi-Fern-Grundarchitektur und ihrer Varianten zum Fernzugriff können Gefährdungen nicht völlig ausschließen, führen aber zu einem akzeptablen Restrisiko.

1.2 Einführung und Überblick

Der Fernzugriff ermöglicht Mitarbeitern einer Institution den Zugang zu deren internem Netz, so dass sie – etwa im Außendienst - notwendige Anwendungen und Daten auch außerhalb der Institution nutzen können. Mitarbeiter, die den Fernzugriff nutzen, werden nachfolgend einfach als Benutzer bezeichnet.

Für den Fernzugriff steht ihnen ein entsprechend ausgestattetes Endgerät zur Verfügung. Es muss für den Zugriff auf Anwendungen und Daten im Netz der Institution eine Kommunikationsbeziehung über einen Netzzugang (etwa DSL, WLAN, WiMax oder Mobilfunk) und über ein Transfernetz (wie das Internet) zum Netz der Institution aufbauen können.

1.2.1 Endgeräte

Für den Fernzugriff sind die Endgerätetypen Desktop, Laptop und Smartphone geeignet. Die unterschiedliche Bauform und Leistungsfähigkeit der Endgeräte beeinflussen die über Fernzugriff nutzbaren Anwendungen im Prinzip nicht. Dies gilt auch für Smartphones, die gegenwärtig bevorzugt für den Fernzugriff auf E-Mails (mobile E-Mail-Synchronisation) und Web-Inhalte eingesetzt werden. Die gerätetypischen Einschränkungen eines Smartphones hinsichtlich Display-Größe und Performance lassen sich durch geeignete technische Maßnahmen umgehen. Dazu zählt Middleware, die eine für kleine Smartphone-Displays aufbereitete Darstellung von Anwendungsinhalten bereitstellt. Als weitere Maßnahme bietet sich der Einsatz eines Terminal-Servers an, der auf wenig performanten Smartphones nur den Betrieb eines entsprechenden Clients erfordert. Die Clients der eigentlichen Anwendungen laufen auf dem ausreichend leistungsfähigen Terminal-Server.

Mit den Endgeräten lassen sich die Zugriffsarten „Vollzugriff“ und „Eingeschränkter Zugriff“ realisieren. Sie unterscheiden sich im Umfang der Anwendungen und Berechtigungen, die dem Benutzer über den Fernzugriff bereitgestellt werden. Diese können denen beim Zugriff aus dem internen Netz heraus gleichen (Vollzugriff) oder ihnen gegenüber eingeschränkt sein (Eingeschränkter Zugriff). Es ist auch möglich, dass Benutzern bestimmte Anwendungen nur über Fernzugriff zur Verfügung stehen.

1.2.2 Netzzugang der Endgeräte

Für den Fernzugriff am Heimarbeitsplatz ist DSL eine weit verbreitete Netzzugangstechnik. Alternativen zum kabelgebundenen DSL stellen die Mobilfunktechniken UMTS und WiMax dar, über die zunehmend in städtischen Räumen ein breitbandiger, kabelloser Internet-Zugang möglich ist. Ein Internet-Zugang über eine direkte Ethernet-Verbindung lässt sich von anderen Institution aus oder vermehrt auch in Hotels nutzen.

An vielen von Geschäftsreisenden frequentierten Orten werden Internetzugänge über das kabellose WLAN angeboten. Entsprechende WLAN Access Points (sogenannte Hotspots) finden sich oft in Flughäfen, Hotels, Messen oder Tagungsräumen.

Soll der Netzzugang möglichst unabhängig von bestimmten Orten erfolgen können, ist der Zugang über Mobilfunk die am besten geeignete Alternative. UMTS und HSPA, die sich immer stärker verbreiten, bieten einen breitbandigen Internet-Zugang. Das ältere GPRS wie auch EDGE sind aufgrund der geringen Datenübertragungsrate, vergleichbar mit der eines Analog-/ISDN-Modems, weniger geeignet, stehen aber momentan in Deutschland fast flächendeckend zur Verfügung.

1.2.3 Komponenten des Fernzugriffs im Netz der Institution

Um den Fernzugriff zu ermöglichen, müssen im Netz der Institution einige zusätzliche Komponenten betrieben werden. Dies sind das VPN-Gateway und der Authentisierungs-Server (AAA-Server). Weitere Server bieten zusätzliche Sicherheitsmerkmale oder erlauben spezielle Anwendungen für den Fernzugriff.

VPN-Gateway

Die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution erfolgt beim Fernzugriff durch einen verschlüsselten VPN-Tunnel. Im Netz der Institution endet der VPN-Tunnel auf dem VPN-Gateway. Das VPN-Gateway sorgt mit Hilfe nachgelagerter Authentisierungsserver – auch AAA-Server genannt – dafür, dass nur erfolgreich authentifizierte Benutzer und/ oder Endgeräte VPN-Tunnel aufbauen können.

AAA-Server

Der Fernzugriff ist so gestaltet, dass nur befugte Benutzer auf zulässige Anwendungen und Daten im Netz der Institution zugreifen können. Die hierfür erforderlichen Aufgaben realisiert ein AAA-Server im Netz der Institution. Zu den Aufgaben zählen die Überprüfung der behaupteten Identität des Benutzers (Authentisierung), die Verwaltung und Bereitstellung möglicher Daten zu Beschränkungen des Fernzugriffs (Autorisierung) und das Erfassen definierter Daten zum Fernzugriff (Accounting).

Weitere Server

Weitere Server, die für den Fernzugriff im Netz der Institution betrieben werden, dienen der Umsetzung von bestimmten Qualitäts- und Sicherheitsmerkmalen sowie von speziellen Anwendungen des Fernzugriffs. So ist es mit einem Terminal-Server möglich, beim Fernzugriff Daten nur zentral im Netz der Institution vorzuhalten. Auf den Endgeräten selbst müssen keine Daten gespeichert werden. Die Möglichkeiten des Datenverlusts und der Datenspionage werden auf diese Weise drastisch reduziert. Mittels eines Proxy-Servers lassen sich die Datenströme des Fernzugriffs auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten. Spezielle E-Mail-Synchronisationsserver können eingesetzt werden, um die mobile Nutzung von E-Mail zu optimieren.

1.2.4 Typische Anwendungen beim Fernzugriff

Zu den Anwendungen, die besonders oft mit einem Fernzugriff in Verbindung gebracht werden, zählen Web-Zugriff, E-Mail und Zugriff auf Netzlaufwerke. Über den Fernzugriff auf Netzlaufwerke kann der Benutzer unterwegs auf Dateien der Institution zugreifen und diese auf sein Endgerät laden oder umgekehrt in das Netz der Institution übertragen.

Über den Fernzugriff auf Web-Anwendungen hat ein Benutzer unterwegs die Möglichkeit, Web-basierte Workflows wie Arbeitszeiterfassung oder Projektplanung, eCommerce-Anwendungen wie Fahrkartenkauf und Hotelbuchung oder Recherchen im Internet oder im Intranet der Institution durchzuführen.

Der Fernzugriff auf das dienstliche E-Mail-Postfach erlaubt die E-Mail-Kommunikation auch außerhalb eines Standortes der Institution. Dabei werden die E-Mails auf dem Endgerät mit denen im Netz der Institution synchronisiert. In der Regel schließt dies auch die Synchronisation von PIM-Daten (Personal Information Management) ein, zu denen persönliche Daten wie Kalender, Adressbuch und Aufgabenplanung gehören. Als Endgerät kommt häufig ein Smartphone zum Einsatz, auf das neue E-Mails im Netz der Institution automatisch weitergeleitet werden.

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Ein Endgerät für den Fernzugriff ist ein attraktives Angriffsziel, wenn ein Angreifer auf dem Endgerät selbst oder im Netz der Institution Daten vermutet, die einen Wert für ihn darstellen. Die wesentlichsten Gefährdungen, die für eine Institution bei der Nutzung des Fernzugriffs entstehen können, sind:

1. Verlust des Endgerätes
2. Gefährdungen durch Schadprogramme
3. Ausfall des Fernzugriffs
4. Manipulation des Fernzugriffs

Diese werden im Folgenden genauer beschrieben:

1.3.1 Verlust des Endgerätes

Wenn sich der Benutzer unachtsam verhält oder wenn das Endgerät schlecht gesichert aufbewahrt wird, etwa in einem Hotelzimmer oder während einer Reise, besteht die Gefahr, dass das Endgerät entwendet oder vergessen wird. Auch Endgeräte des Typs Desktop an einem Heimarbeitsplatz sind möglicher Gegenstand eines Einbruchdiebstahls.

Hierbei ist nicht nur der materielle Schaden von Bedeutung, sondern vor allen Dingen der Verlust der Vertraulichkeit der Daten, die auf dem Endgerät gespeichert sind. Bei diesen Daten kann es sich um die E-Mail-Korrespondenz, die Kontakte des Benutzers oder gespeicherte Dokumente handeln, die z.B. Informationen zu aktuellen Vertragsverhandlungen, zur Finanzsituation, zur Strategie der Institution oder zum Bereich Forschung und Entwicklung beinhalten.

Insbesondere bei einem gezielten Diebstahl, z. B. zum Zwecke der Spionage, versucht der Angreifer nicht nur die Daten des Endgeräts selber, sondern zusätzlich zum Endgerät, auch in den Besitz von Passwörtern, PINs, SmartCards und anderen Mitteln zu gelangen, die für die Anmeldung am Netz der Institution notwendig sind. Ist der Angreifer erst einmal in den Besitz dieser Authentisierungsmittel gekommen, kann er sowohl auf die geschützten Daten des Endgeräts als auch auf die Daten im Netz der Institution zugreifen, diese verfälschen oder sogar löschen.

1.3.2 Gefährdungen durch Schadprogramme

Endgeräte für den Fernzugriff sind besonders anfällig für Schadprogramme, da die schützenden Software-Aktualisierungen von Betriebssystem und/oder Anwendung nicht immer rechtzeitig ein-

gespielt werden können. Verschärfend kommt hinzu, dass es beim Fernzugriff eine Vielzahl möglicher Übertragungswege von Schadprogrammen auf ein Endgerät gibt, etwa der ungeschützte Zugang zu Web-Inhalten, schlecht gesicherte Netzzugänge oder der Datenaustausch über infizierte mobile Datenträger von Dritten. Ein einmal infiziertes Endgerät kann Schadprogramme bei einem Fernzugriff leicht in das Netz der Institution und auf dessen IT-Systeme übertragen. Zu den bevorzugten Zielen der Schadprogramme gehören die heimliche Spionage vertraulicher Daten der Institution, deren Manipulation oder Löschung.

1.3.3 Ausfall des Fernzugriffs

Für den Fernzugriff ist ein Netzzugang und ein Transfernetz notwendig, über die eine Kommunikationsverbindung vom Endgerät zum Netz der Institution aufgebaut werden kann. In der Regel unterliegen weder Netzzugang noch Transfernetz der Kontrolle der Institution, so dass diese kein definiertes Sicherheitsniveau durchsetzen kann. Daher kann es zu Verzögerungen bis hin zum Ausfall des Fernzugriffs kommen. Aber auch im Netz der Institution können Probleme auftreten. Verzögerungen könnten z. B. dadurch entstehen, dass die Internet-Anbindung des Netzes der Institution die Mindestdatenübertragungsrate für den Fernzugriff nicht bereitstellt und überlastet wird. Wollen dann zu viele Anwender gleichzeitig einen Fernzugriff durchführen, kommt der Fernzugriff nicht oder nur verzögert zustande. Der komplette Verlust der Verfügbarkeit eines Fernzugangs kann durch den Ausfall des VPN-Gateways oder anderer wichtiger Komponenten bzw. des Endgerätes selbst zustande kommen. Eine Nutzung des Fernzugangs ist dann nicht mehr möglich.

1.3.4 Manipulation des Fernzugriffs

Die jeweiligen Betreiber von Netzzugang und Transfernetz haben aufgrund ihrer Rolle prinzipiell Zugang zu den übertragenen Daten. Diese Zugangsmöglichkeit kann auch für andere Mitbenutzer des Netzzugangs bestehen, wie bei einem schlecht gesicherten WLAN-Internet-Zugang. Bei unzureichender Verschlüsselung, können die beim Fernzugriff übertragenen Daten unbemerkt ausspioniert und verändert werden. Unbefugte haben die Möglichkeit, Einblick in Geheimnisse der Institution zu erlangen, vertrauliche E-Mail-Kommunikation eines Mitarbeiters während dessen Fernzugriff mitzuverfolgen oder deren Inhalte zu verändern. Auch Passwörter, die für die Anmeldung zum Fernzugriff erforderlich sind, lassen sich so ermitteln. Mit diesen Anmeldeinformationen kann der Angriff auf das Netz der Institution ausgeweitet werden, um auch dort Informationen auszuspähen, zu verfälschen oder Daten zu löschen.

1.4 Wesentliche Empfehlungen

Den dargestellten Gefährdungen des Fernzugriffs begegnet die im folgenden beschriebene Grundarchitektur mit ihren Sicherheitsmerkmalen, um das mit dem Fernzugriff verbundene Risiko auf ein akzeptables Maß zu reduzieren.

Die Grundarchitektur ist so gestaltet, dass sie folgende Anforderungen erfüllt:

- Es dürfen nur Endgeräte eingesetzt werden, die unter der Kontrolle der Institution stehen, in dessen Netz der Fernzugriff erfolgt.
- Die für das Endgerät gewählte Netzzugangstechnik muss zu der typischen Arbeitsumgebung des Benutzers passen. Im Fall des Fernzugriffs am Heimarbeitsplatz ist in der Regel DSL geeignet. Im Fall eines Fernzugriffs unabhängig von einem bestimmten Ort bietet sich Mobilfunk an.

- Die Datenübertragungsrate muss ausreichend dimensioniert sein. Die geforderten Leistungswerte bemessen sich letztlich am Datenaufkommen, das über den Fernzugriff übertragen werden soll.
- Für die Kommunikationsverbindung zwischen dem Endgerät und dem Netz der Institution ist ein kryptografisch gesichertes VPN einzusetzen.
- Insbesondere hoch interaktive Anwendungen dürfen nicht durch zu lange Verzögerungen (Latenzzeit) beeinträchtigt werden.
- Der Verlust eines Endgeräts darf nicht dazu führen, dass wichtige Anwenderdaten nicht mehr verfügbar sind oder Unbefugte vertrauliche Anwenderdaten einsehen können. Daraus folgt, dass die Daten auf dem Endgerät verschlüsselt und regelmäßig gesichert werden müssen.
- Unbefugte dürfen ein Endgerät nicht für den Fernzugriff auf das Netz der Institution einsetzen können. Deshalb wird dem Anwender der Zugriff auf das interne Netz der Institution erst nach einer erfolgreichen Authentisierung und Autorisierung gegenüber dem Endgerät und dem Netz gestattet.
- Bei der Umsetzung von IT-Sicherheitsfunktionen sollte der Bedienkomfort nicht außer Acht gelassen werden, da Benutzer dazu neigen, Sicherheitsfunktionen aus Bequemlichkeit zu umgehen und die Gefährdungen damit zu erhöhen.
- Der Internetzugriff von Endgeräten darf nur über das Sicherheits-Gateway der Institution erfolgen. Die Sicherheitsfunktionen des Sicherheits-Gateways schützen das Endgerät vor Angriffen aus dem Internet (z. B. Schadprogramme, Spam, unerlaubte E-Mail-Dateianhänge). Zusätzlich wird auch das interne Netz der Institution geschützt, damit sich bei einem Fernzugriff durch ein infiziertes Endgerät keine Schadprogramme verbreiten können.

1.4.1 Grundarchitektur

Basis für die nachfolgend abgebildete Grundarchitektur für den Fernzugriff sind die Anforderungen an die Funktionsfähigkeit und das angestrebte Sicherheitsniveau. Die Abbildung 1.1 zeigt die beim Fernzugriff beteiligten Teilnetze. Zur Grundarchitektur des Netzes der Institution (wie in ISi-LANA beschrieben) kommt eine Fernzugriffszone für den Betrieb der erforderlichen IT-Systeme hinzu.

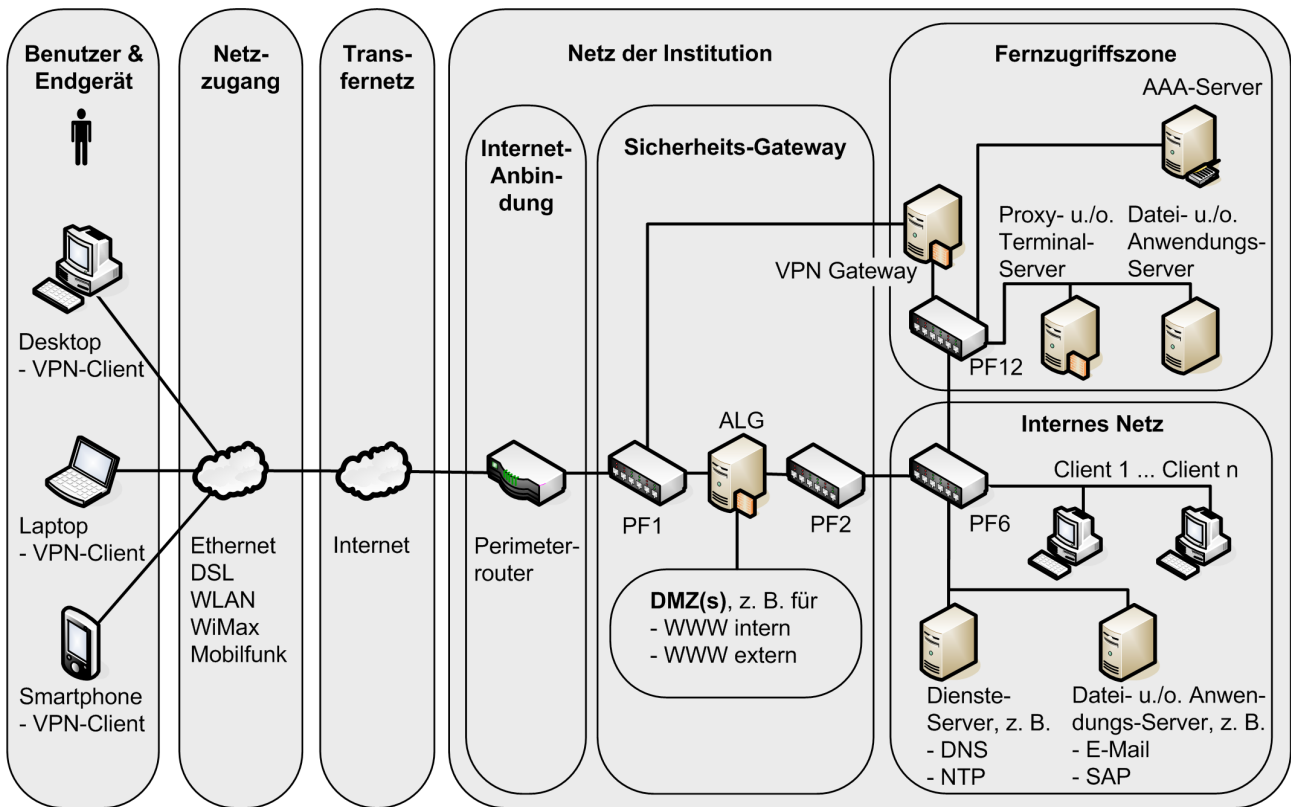


Abbildung 1.1: Grundarchitektur zum sicheren Fernzugriff auf das interne Netz

Damit ein Fernzugriff überhaupt möglich ist, muss der Benutzer über ein Endgerät verfügen und sich erfolgreich am Endgerät anmelden können.

Für den Fernzugriff baut das Endgerät über einen Netzzugang eine Verbindung zum Internet auf. Der Netzzugang lässt sich kabelgebunden, z. B. über DSL oder Ethernet, oder kabellos, z. B. über WLAN, WiMax oder Mobilfunk, gestalten. Alternativ zum Internet können auch das IP-Netz eines Netzbetreibers oder das öffentliche leitungsgebundene Telefonnetz eingesetzt werden.

An den Aufbau des Netzzugangs schließt sich der Aufbau des kryptografisch gesicherten VPNs zwischen dem Endgerät und dem VPN-Gateway im Netz der Institution an. Am VPN-Aufbau ist der AAA-Server im Netz der Institution maßgeblich beteiligt. Er führt die Authentifizierung der Benutzer durch und unterstützt deren Autorisierung, so dass nur befugte Benutzer auf die für sie zulässigen Anwendungen und Daten im Netz der Institution zugreifen können.

Das VPN-Gateway, der AAA-Server und andere unterstützende IT-Systeme für den Fernzugriff werden in einer speziellen Fernzugriffszone betrieben. Dieser Bereich des Netzes der Institution ist über Paketfilter von den anderen Netzbereichen separiert. Zur Fernzugriffszone können auch Proxy- und/oder Terminal-Server gehören, durch die sich spezielle Sicherheits- und Qualitätsmerkmale zum Fernzugriff durchsetzen lassen.

Die Fernzugriffszone lässt sich im Fall der mobilen E-Mail-Synchronisation um ein weiteres IT-System ergänzen, das die Synchronisation der E-Mails zwischen dem Netz der Institution und dem Endgerät realisiert. Hierbei kann es sich um ein IT-System handeln, das einen offenen herstellerunabhängigen Standard wie SyncML zur Datensynchronisation unterstützt.

1.4.2 Grundlegende Sicherheitsmerkmale

Die Grundarchitektur zeichnet sich durch die folgenden Sicherheitsmerkmale aus. Sie betreffen die Verbindung zwischen einem Endgerät und dem Netz der Institution sowie das Endgerät und das Netz der Institution selbst. Sie sind sowohl technischer als auch organisatorischer Art.

Endgerät unter Kontrolle der Institution

Es dürfen nur Endgeräte für den Fernzugriff eingesetzt werden, deren Betriebssystem und Anwendungssoftware unter der Kontrolle der Institution stehen, in dessen Netz der Fernzugriff erfolgt. Dies lässt sich auf verschiedene Weise umsetzen. Die Institution kann den Benutzern entsprechende Endgeräte bereitstellen und den Einsatz fremder Endgeräte untersagen. Als eine Variante der Grundarchitektur besteht die Möglichkeit, den Einsatz privater Endgeräte zuzulassen und technisch durchzusetzen, sodass der Fernzugriff nur in einer definierten, von der Institution kontrollierten Betriebssystemumgebung erfolgen kann. Hierfür lässt sich eine sogenannte Live-CD¹ einsetzen. Bei Einsatz einer Live-CD ist zu beachten, dass die technischen Rahmenbedingungen für den Einsatz einer solchen CD nicht überall gegeben sind.

Datenverschlüsselung des Endgeräts

Die Daten des Benutzers dürfen auf einem ausgeschalteten Endgerät nur in verschlüsselter Form vorliegen. Die Entschlüsselung muss an die erfolgreiche Authentisierung des Benutzers am Endgerät gekoppelt sein. Bei den Endgerätetypen Desktop und Laptop kann dies durch ein geeignetes Festplattenverschlüsselungsprogramm erfolgen. Die Entschlüsselung sollte auch durch einen Administrator der Institution möglich sein, falls der Benutzer die notwendigen Authentisierungsgeheimnisse vergessen hat.

Authentisierung gegenüber Endgerät und Netz der Institution

Der Benutzer darf ein Endgerät nur dann nutzen, wenn er sich zuvor erfolgreich gegenüber dem Endgerät authentisiert hat. Ergänzend müssen sich der Benutzer oder das Endgerät vor einem Fernzugriff erfolgreich gegenüber dem Netz der Institution authentisieren. Nach einer definierten Anzahl von Fehlversuchen müssen das Endgerät bzw. das VPN-Gateway weitere Authentisierungsversuche durch den Benutzer oder das Endgerät verwerfen oder zeitlich verzögern.

Virenschutz des Endgeräts

Auf einem Endgerät dürfen Dateien nur nach erfolgreicher Überprüfung durch ein Virenschutzprogramm bearbeitet werden. Dies kann auf speziellen IT-Systemen im Netz der Institution erfolgen oder auf dem Endgerät selbst, wenn die Daten nicht über das Netz der Institution auf das Endgerät gelangen.

Regelmäßige Datensicherung des Endgeräts

Daten des Benutzers, die nur lokal auf dem Endgerät vorliegen, müssen in regelmäßigen Zeitabständen auf ein IT-System im Netz der Institution gesichert werden. Die Zeitabstände der Sicherung sollten sich an den voraussichtlichen Schadensauswirkungen orientieren, die ein Verlust noch unge-

¹ Bei einer Live-CD handelt es sich um ein Betriebssystem, das unabhängig von einer im System vorhandenen Festplatte gestartet werden kann. Dieses Betriebssystem kann sich auf einer CD-ROM, einer DVD, einem USB-Stick oder einem anderen bootfähigen Speicher befinden. Dadurch wird das Arbeiten auf einem Computer ermöglicht, ohne auf dessen Festplatte oder installiertem Betriebssystem zuzugreifen.

sicherter Daten des Endgeräts nach sich ziehen würde. Die Schadensauswirkungen sollten begrenzt und überschaubar sein.

Eingeschränkte Verbindungsaufbauten zum/vom Endgerät (Personal Firewall)

Mögliche Verbindungsaufbauten vom und zum Endgerät müssen eingeschränkt werden. Dies kann durch eine Personal Firewall auf dem Endgerät erfolgen. Für den Fernzugriff sollte die Personal Firewall des Endgeräts ausgehende Verbindungsaufbauten nur an das VPN-Gateway des Netzes der Institution zulassen. Verbindungsaufbauten zum Endgerät müssen blockiert werden. Eine mögliche Ausnahme bilden Verbindungsaufbauten zu Administrationszwecken.

Fernadministration von mobilen Endgeräten

Insbesondere bei mobilen Endgeräten sollte eine Fernadministration durch einen Administrator im Netz der Institution möglich sein, beispielsweise um Benutzerdaten zu löschen, Passwörter neu zu setzen oder Softwareaktualisierungen einzuspielen.

VPN

Ein Fernzugriff darf nur über ein kryptografisch gesichertes VPN erfolgen, das die Vertraulichkeit und die Integrität der übertragenen Daten schützt. Die Endpunkte des VPN müssen das Endgerät und ein IT-System im Netz der Institution, ein sogenanntes VPN-Gateway, sein.

Internet-Zugang des Endgeräts nur über das Netz der Institution

Der Zugriff auf Web-Inhalte soll ausdrücklich nur über Fernzugriff, d. h. über das Netz der Institution, erfolgen und nicht direkt über einen möglicherweise bestehenden Netzzugang zum Internet außerhalb der Institution. Dadurch lassen sich auch während des Fernzugriffs technische Sicherheitsmaßnahmen wie Filterung oder Blockade schädlicher Aktiver Inhalte, die für den Zugang zu Web-Inhalten gelten, durchsetzen.

Möglichkeit der Sperrung von Fernzugängen

Die Institution muss den Fernzugriff eines bestimmten Benutzers oder eines bestimmten Endgeräts sperren können. Typische Gründe dafür sind der Verlust des Endgeräts oder von Authentisierungsmitteln. Die Benutzer sind anzuhalten, den Verlust ihres Endgeräts oder andere kritische Vorfälle zeitnah zu melden. Die Institution muss in der Lage sein, die meldenden Benutzer sicher zu identifizieren, die Meldungen zeitnah entgegenzunehmen und Sperrungen rasch durchsetzen zu können.

Beschränkung des Fernzugriffs auf das fachlich Notwendige

Ein Benutzer sollte den Fernzugriff nur nutzen können, wenn dies zur Ausübung seiner fachlichen Aufgaben innerhalb der Institution notwendig ist. Über den Fernzugriff sollte er nur auf die Anwendungen und Daten im Netz der Institution zugreifen können, die zur Aufgabenerledigung erforderlich sind.

Minimalkonfiguration

Alle Komponenten des Fernzugriffs (Endgeräte, VPN-Gateway, Server), insbesondere die aus dem Internet erreichbaren, müssen minimal konfiguriert werden. Überflüssige Software ist zu entfernen, unnötige Dienste sind zu deaktivieren.

Nicht für den Fernzugriff benötigte Kommunikationsschnittstellen des Endgeräts, wie z. B. Bluetooth oder Infrarot, müssen deaktiviert sein.

Anwenderrichtlinie

Der Nutzer des Fernzugriffs muss auf eine Anwenderrichtlinie verpflichtet werden, die die benutzerrelevanten Aspekte des Fernzugriffs regelt und darüber hinaus über den richtigen Umgang informiert. Hierzu zählen insbesondere der sachgerechte Umgang mit dem Endgerät und den Authentisierungsmitteln.

1.5 Fazit

Der Fernzugriff erfüllt den wachsenden Bedarf der Mitarbeiter vieler Institutionen, auch unabhängig vom Standort der Institution auf Daten und Anwendungen zugreifen zu können. Mit dem Gewinn an Flexibilität sind Risiken verbunden, die vor allen Dingen die Möglichkeit der Spionage und des Verlusts von Daten sowie der Sabotage der IT-Systeme der Institution betreffen. Gegen diese Risiken sind die Sicherheitsmaßnahmen der Grundarchitektur gerichtet. Zu den wichtigsten Maßnahmen zählen die Absicherung der Kommunikationsverbindung des Fernzugriffs, die Einschränkung des Fernzugriffs auf befugte Benutzer und der Schutz der Daten vor Verlust und Spionage durch regelmäßige Datensicherung und zusätzliche Verschlüsselung. Durch diese Grundarchitektur wird ein sicherer Fernzugriff auf das Netz der Institution realisiert. Nicht zu unterschätzen ist die Notwendigkeit der Sensibilisierung der Benutzer für den achtsamen Umgang mit ihren Endgeräten und Anmelde Mitteln, wie PIN, Passwort oder SmartCard. Nur in Verbindung mit achtsamen Benutzern reduzieren die technischen und organisatorischen Sicherheitsmaßnahmen der Grundarchitektur das mit dem Fernzugriff verbundene Risiko auf ein tragbares Maß.

2 Glossar

AAA-Server

Auf einem Authentisierungsserver läuft ein Dienst zur Authentifizierung von Benutzern und/oder IT-Systemen. Gängige Authentisierungsserver unterstützen auch zusätzlich die Funktionen Autorisierung und Accounting. Dem entsprechend werden sie auch als AAA-Server bezeichnet.

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computer-Netze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzer-Kennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff (engl. attack)

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Anwendungsschicht (engl. application layer)

Die Anwendungsschicht ist die oberste Schicht im TCP/IP-Referenzmodell. Sie umfasst alle Protokolle, die von Anwendungsprogrammen, z. B. Browser oder E-Mail-Client, verarbeitet und für den Austausch anwendungsspezifischer Daten genutzt werden. Beispiele für Protokolle der Anwendungsschicht sind das Hypertext Transfer Protocol (HTTP) oder das Simple Mail Transfer Protocol (SMTP).

Authentifizierung (engl. authentication)

Unter einer Authentifizierung versteht man die Prüfung einer Authentisierung, d. h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter Anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Authentisierung (engl. authentication)

Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Autorisierung (engl. authorization)

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Betriebssystem (engl. operating system)

Das Betriebssystem ist ein Steuerungsprogramm, das es dem Benutzer ermöglicht, seine Dateien zu verwalten, angeschlossene Geräte (z. B. Drucker, Festplatte) zu kontrollieren oder Programme zu starten. Weit verbreitet sind z. B. Windows, Linux oder MacOS.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (engl. Federal Office for Information Security)

Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern.

CD (Corporate Design [engl.])

Gestaltung eines durchgängigen Erscheinungsbildes. Im Corporate Design werden Logos, Farben und Schriften sowie Gestaltungsprinzipien für deren Verwendung definiert.

Client [engl.]

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

Datensicherung (engl. backup)

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren. Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustands von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

Gefährdung

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. So sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen. Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenbefallene Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Typ Computer-Virus ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Hacking [engl.]

Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls - bei unethischem Hacking - zu übernehmen.

Integrität (engl. integrity)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist ein Grundwert der IT-Sicherheit.

Intranet (engl. intranet)

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netze (wie dem Internet) durch ein Sicherheits-Gateway verhindert oder nur aufgrund spezieller Regeln zugelassen.

IP (Internet Protocol [engl.])

Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u. a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

Kryptografie

Mathematisches Fachgebiet, das sich mit Methoden zum Schutz von Informationen befasst (u. a. mit Vertraulichkeit, Integrität und Authentizität von Daten).

Middleware [engl.]

Je nach Architektur einer IT-Anwendung ist es sinnvoll, Funktionalitäten aus dem Frontend oder Backend in eine oder mehrere Zwischenschichten zu verlagern. Dabei handelt es sich i. d. R. um zwischengeschaltete Server, die bspw. die Zugriffsberechtigungen auf die Daten kontrollieren. Hierdurch lassen sich sowohl die Performance als auch die Sicherheit der IT-Anwendung erhöhen.

Paketfilter (engl. packet filter)

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Passwort

Geheimes Kennwort, das Daten, Rechner, Programme u. a. vor unerlaubtem Zugriff schützt.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Restrisiko (engl. residual risk)

Risiko, das grundsätzlich bleibt, auch wenn Maßnahmen zum Schutz des IT-Einsatzes ergriffen worden sind.

Risiko (engl. risk)

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Schutzbedarf (engl. protection requirements)

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Server [engl.]

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheits-Gateway

Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

Sicherheitsmaßnahme (engl. safeguard control)

Mit Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und entgegenzuwirken. Dies schließt organisatorische, personelle, technische und infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt.

Spam [engl.]

Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail.

SyncML

Die SyncML-Protokoll-Familie ist ein herstellerunabhängiger Standard der Open Mobile Alliance (OMA). Er dient der Synchronisation von Daten und der Verwaltung von Einstellungen von Endgeräten (Device Management). Ein mögliches SyncML-Einsatzszenario im Zusammenhang mit dem Fernzugriff ist die mobile E-Mail-Synchronisation zwischen einem mobilen Endgerät wie einem Smartphone und einem Mailserver im Netz einer Institution.

Verfügbarkeit (engl. availability)

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist ein Grundwert der IT-Sicherheit.

Verschlüsselung (engl. encryption)

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die Schlüssel genannt wird, in einen zugehörigen Geheimtext (Chiffre), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartexts aus dem Geheimtext - wird Entschlüsselung genannt.

Vertraulichkeit (engl. confidentiality)

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.

Virenschutzprogramm

Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Vollzugriff

Vollzugriff auf die Daten des internen Netzes bedeutet, dass der Nutzer mit dem entsprechenden Endgerät über die selben Berechtigungen verfügt, die er als Teil des internen Netzes hat oder hätte. Einschränkungen bei der Nutzung von Applikationen und minimale Beschneidungen der Berechtigungen können aber technisch bedingt notwendig sein.

VPN (Virtual Private Network [engl.])

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft dem Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des

Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

VPN-Gateway

Ein VPN-Gateway terminiert die durch das VPN realisierte verschlüsselte Verbindung, auch VPN-Tunnel genannt. Die nunmehr unverschlüsselten Daten leitet das VPN-Gateway an das adressierte interne Netz weiter.

WLAN (Wireless Local Area Network [engl.])

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

3 Stichwort- und Abkürzungsverzeichnis

AAA-Server.....	7, 11, 15
Administrator.....	12, 13, 15
ALG (Application-Level Gateway).....	18
Anwendungsschicht.....	7, 15
Authentifizierung.....	5, 11, 15
Authentisierung.....	7, 8, 10, 12-15
Authentizität.....	17
Autorisierung.....	7, 10, 11, 15
Backend.....	17
Bedrohung.....	16
Benutzer-Kennung.....	15
Betriebssystem.....	8, 12, 15, 16
Biometrie.....	15
Bit (Binary Digit).....	17
Bluetooth.....	14
BMI (Bundesministerium des Innern).....	16
CD (Compact Disk).....	12
CD (Corporate Design).....	16
Chiffre.....	19
Chipkarte.....	15
Dateianhang.....	10
Datensicherung.....	12, 14, 16
DSL (Digital Subscriber Line).....	5, 6, 9, 11
E-Mail (Electronic Mail).....	2, 6-11, 15, 18, 19
EDGE (Enhanced Data Rates for Global Evolution).....	7
EDV (Elektronische Datenverarbeitung).....	5
Ethernet.....	6, 11
Frontend.....	17
Gefährdung.....	5, 6, 8-10, 15, 16
Hacking.....	3, 17
Spam.....	10, 19
Gefährdungsanalyse.....	3, 8
GPRS (General Packet Radio Service).....	7
Grundarchitektur.....	3, 5, 6, 9, 10, 12, 14
Hacking.....	3, 17
Hardware.....	16, 18
HTTP (Hypertext Transfer Protocol).....	15
Hypertext.....	15
IEEE (Institute of Electrical and Electronics Engineers).....	20
IN (Intelligent Network).....	8
Informationssicherheit.....	17
INFOSEC (Information Security).....	16
Integrität.....	3, 13, 16, 17, 19
Internet-Schicht.....	17
Intranet.....	8, 17
IP (Internet Protocol).....	11, 15, 17, 18
IPv4 (Internet Protocol Version 4).....	17

ISDN (Integrated Services Digital Network).....	7
ISi (Internet-Sicherheit).....	
ISi-L (ISi-Leitfaden).....	1
ISi-Reihe.....	2
IT-Sicherheit.....	17, 19
Authentizität.....	17
Informationssicherheit.....	17
Integrität.....	3, 13, 16, 17, 19
Verfügbarkeit.....	3, 9, 16, 19
Vertraulichkeit.....	3, 8, 13, 17, 19
Kryptografie.....	5, 10, 11, 13, 17, 19
LAN (Local Area Network).....	20
MacOS (Macintosh Operating System).....	16
Middleware.....	6, 17
OMA (Object Management Architecture).....	19
Paketfilter.....	11, 17, 18
Passwort.....	8, 9, 13-15, 18
PIM (Personal Information Management).....	8
PIN (Persönliche Identifikationsnummer).....	14
Protokoll.....	
HTTP (Hypertext Transfer Protocol).....	15
IP (Internet Protocol).....	11, 15, 17, 18
IPv4 (Internet Protocol Version 4).....	17
SMTP (Simple Mail Transfer Protocol).....	15
TCP (Transmission Control Protocol).....	15, 17
Proxy.....	7, 11, 18
Restrisiko.....	6, 18
Risiko.....	5, 6, 9, 14, 18
Schadprogramm.....	5, 8-10, 16
Trojanisches Pferd.....	19
Virus.....	16, 19
Wurm.....	19
Schutzbedarf.....	5, 18
Schwachstelle.....	16
Sicherheits-Gateway.....	10, 17, 18
ALG (Application-Level Gateway).....	18
Paketfilter.....	11, 17, 18
Sicherheitsleitlinie.....	18
Sicherheitsmaßnahme.....	13, 14, 18
SMTP (Simple Mail Transfer Protocol).....	15
Spam.....	10, 19
SyncML.....	11, 19
TCP (Transmission Control Protocol).....	15, 17
TCP/IP-Referenzmodell.....	
Anwendungsschicht.....	7, 15
Internet-Schicht.....	17
Transportschicht.....	17
Transportschicht.....	17
Trojanisches Pferd.....	19
UMTS (Universal Mobile Telecommunications System).....	5-7

Verfügbarkeit.....	3, 9, 16, 19
Verschlüsselung.....	
Chiffre.....	19
Vertraulichkeit.....	3, 8, 13, 17, 19
Virenschutz.....	12
Virenschutzprogramm.....	12, 19
Virus.....	12, 16, 19
Vollzugriff.....	6, 19
VPN (Virtual Private Network).....	5, 7, 9-13, 19, 20
VPN-Gateway.....	7, 11-13, 20
Web-Anwendung.....	8
WLAN (Wireless Local Area Network).....	5, 6, 9, 11, 20
Wurm.....	19