Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheit im Internet

Empfehlungen zum Schutz von IP-Netzen und -Diensten

Inhaltsverzeichnis

Unsere Gesellschaft auf dem Daten-Highway 3

Das BSI im Dienst der Öffentlichkeit 4

1 Sicherheit im Internet 7

2 Gefährdungen bei der Nutzung des Internet 9

2.1 Abhören von vertraulichen Daten 9
2.2 Computer-Sabotage (Verändern, Täuschen, Betrügen, Fälschen) 9
2.3 Ausfall des E-Mail-Servers durch Spam-E-Mails 10

3 Grundprinzipien der Internet-Sicherheit 12

3.1 Funktionstrennung 12
3.2 Minimalität 12
3.3 Need-to-Know-Prinzip 12
3.4 Whitelisting 12
3.5 Beschränkung des Verbindungsaufbaus 13
3.6 Aktualität 13

4 BSI-Standards zur Internet-Sicherheit (ISi-Reihe) 15

4.1 Sichere Anbindung an das Internet 16
4.2 Absicherung eines Servers 20
4.3 Absicherung eines Arbeitsplatz-PCs 21
4.4 Sichere Nutzung von Web-Angeboten 22
4.5 Sicheres Bereitstellen von Web-Angeboten 23
4.6 Sichere Nutzung von E-Mail 24
4.7 Sicherer Betrieb von E-Mail-Servern 25
4.8 Sicherer Fernzugriff auf das interne Netz 26
4.9 Sichere Internet-Telefonie 27
4.10 Sicheres WLAN 28
4.11 Sicheres VPN 29

Unsere Gesellschaft auf dem Daten-Highway

Wir befinden uns heute in einer globalen Informationsgesellschaft. Immer komplexere, schnellere und weltweit vernetzte informationstechnische Systeme übernehmen zunehmend weitreichendere Aufgaben.

Die Informationstechnik (IT) hat inzwischen alle gesellschaftlichen Bereiche erfasst und ist ein selbstverständlicher und teilweise unsichtbarer Bestandteil des Alltags geworden.

Die Funktionsweise von informationstechnischen Produkten und Systemen ist aber für weite Kreise der Anwender nicht sofort und ohne fundiertes Fachwissen durchschaubar. Vertrauen in die Informationstechnik kann aber nur dann entstehen, wenn sich die Nutzer auf ihre Anwendung verlassen können. Das gilt insbesondere für die Sicherheit von Daten im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität.

Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, entsprechend der jeweiligen Gefährdungslage, Sicherheitsstandards zu entwickeln und einzuhalten.

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.

Mit seinen derzeit rund 550 Mitarbeiterinnen und Mitarbeitern und 62 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Infomationstechnik (IT) durchdringt alle Lebensbereiche: Telekommunikation, Börsen, Versicherungen, Behörden, Produktionsprozesse, Unterhaltungsindustrie. Wo Millionen Informationen und Daten verarbeitet werden, müssen Schutzmechanismen vorhanden sein, damit für das Funktionieren der Gesellschaft wichtige Systeme nicht versagen oder durch Angriffe von außen gestört werden.

Diese Broschüre beschreibt nachfolgend welche Gefährdungen bei der Nutzung des Internet entstehen und welche Schutzmechanismen es u.a. gibt, um Angriffe abzuwehren.

1 Sicherheit im Internet

1 Sicherheit im Internet

Das Internet ist heute aus Verwaltung und Wirtschaft kaum noch wegzudenken. Die Möglichkeiten erstrecken sich von der Informationsbeschaffung, über das Versenden und Empfangen von E-Mails bis zur Erledigung von Geschäften wie Online-Banking oder der Abgabe der Steuererklärung. Ebenso hat die Vernetzung verschiedener Standorte deutlich zugenommen. Jedoch stellt das Internet für die angeschlossenen IT-Systeme und die davon abhängigen Informationsverarbeitungsprozesse auch eine erhebliche zusätzliche Gefahr dar. Fast täglich wird in der Presse über Angriffe auf die Vertraulichkeit, Verfügbarkeit und Integrität von Daten berichtet.

Um sich vor Angriffen zu schützen, ist es erforderlich verschiedene Maßnahmen zu ergreifen. Nur wenn Sicherheit neben Funktionalität und Leistungsfähigkeit als gleichrangiges Ziel bei der Entwicklung und beim Erwerb von Rechnersystemen anerkannt wird, kann eine sichere Internet-Nutzung ermöglicht werden.

Dazu gehört neben dem Schutz der eigenen Infrastruktur auch der Schutz der Nutzer. So sollte z. B. ein Anbieter von Web-Seiten, seine Dienste im Internet so konzipieren, dass die potenziellen Nutzer diese in Anspruch nehmen können, ohne die eigenen Sicherheitsmaßnahmen aufzuweichen.

2 Gefährdungen bei der Nutzung des Internet

2 Gefährdungen bei der Nutzung des Internet

Mit der Anbindung eines lokalen Netzes (LAN) an ein nicht vertrauenswürdiges Netz (z. B. das Internet) wird das LAN zusätzlichen Gefährdungen ausgesetzt. Es werden unter anderem folgende Arten von Angriffen möglich:

2.1 Abhören von vertraulichen Daten

Beispiel: Ein Außendienstmitarbeiter kommuniziert unverschlüsselt mit seinem Unternehmen. Ein Angreifer, der diese Kommunikation aufzeichnet, kann vertrauliche Daten ausspähen.

Beispiel: Per E-Mail werden einem an Antiquitäten interessierten Mitarbeiter Links zu Angeboten zugeschickt. Beim Betrachten der Angebote im Browser wird im Hintergrund mithilfe Aktiver Inhalte ein Trojanisches Pferd installiert, das fortan alle Eingaben auf der Tastatur aufzeichnet und an den Angreifer sendet.

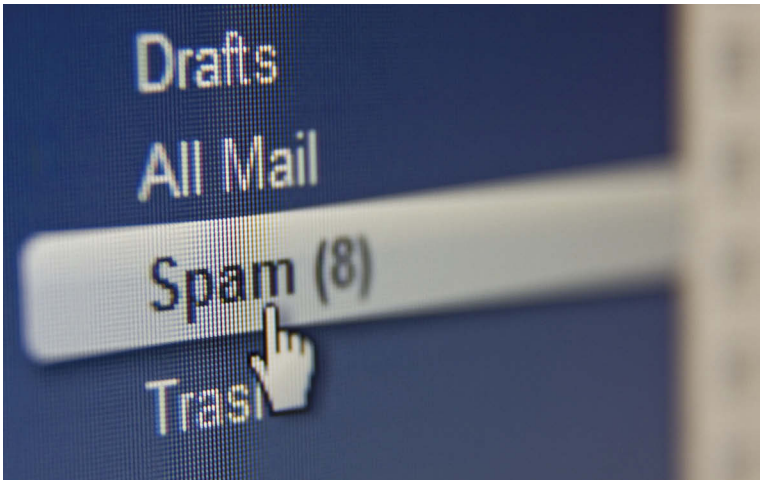
2.2 Computer-Sabotage (Verändern, Täuschen, Betrügen, Fälschen)

Beispiel: Ein Angreifer versucht, die Einträge auf einem DNS-Server zu manipulieren (DNS-Spoofing) mit dem Ziel, Anwender auf seine Webseite umzulenken. So kann er zum Beispiel seinen Angriffsrechner als ein Portal für Online-Banking ausgeben. Gelingt der Angriff, so kann der Angreifer Bank-Transaktionen entgegennehmen, die darin enthaltenen Zugangs-Passwörter, PINs und TANs ausspähen und versuchen, mit diesen Informationen das Konto des Opfers zu plündern.

2.3 Ausfall des E-Mail-Servers durch Spam-E-Mails

Beispiel: Ein Angreifer versendet in großem Umfang Spam-E-Mails an eine Institution. Der empfangende E-Mail-Server wird durch diese Flut so überlastet, dass er keine weitere E-Mails mehr annehmen kann. Die Institution ist so vom E-Mail-Verkehr abgeschnitten.

Um entsprechende Lasten zu generieren, basieren solche Angriffe meist auf einem ferngesteuerten, koordinierten Angriff auf den Zielrechner, ausgehend von einer sehr großen Zahl von Angriffsrechnern; man spricht in diesem Falle von verteilten Denial-of-Service-Angriffen (Distributed DoS, DDoS).



Umfassende Information über bestehende Bedrohungen und Gefährdungen sowie über Gegenmaßnahmen sind für einen hinreichenden Schutz unerläßlich.

3 Grundprinzipien der Internet-Sicherheit

3 Grundprinzipien der Internet-Sicherheit

Beim Anschluss eines LAN an ein nicht vertrauenswürdiges Netz (z. B. das Internet) ist es wichtig, bei Aufbau, Konfiguration und Betrieb u. a. folgende Grundprinzipien zu berücksichtigen:

3.1 Funktionstrennung

Unabhängige Funktionen sollten getrennt voneinander realisiert werden („Ein Server – ein Dienst!"). Dies gilt insbesondere für sicherheitsrelevante Funktionen. Die Funktionstrennung reduziert die Komplexität der Gerätekonfiguration und minimiert so die Angriffsfläche und die Last der einzelnen Komponenten.

3.2 Minimalität

Alle Systemkomponenten – insbesondere die Komponenten des Sicherheits-Gateways sowie die über das Internet erreichbaren Server – sollten minimal konfiguriert sein. Überflüssige Software sollte entfernt, nicht benötigte Funktionen sollten deaktiviert werden.

3.3 Need-to-Know-Prinzip

Systemkomponenten, Anwendungen und Dienste dürfen nur solche Informationen über das LAN und seine Benutzer preisgeben, die für den ordnungsgemäßen Betrieb und die Nutzung der IT-Infrastruktur unverzichtbar sind. Das zugängliche Informationsangebot sollte je nach Rolle und Zugriffsrechten des Benutzers individuell zugeschnitten werden.

3.4 Whitelisting

Alle Filterregeln in Paketfiltern sollten so formuliert sein, dass Anfragen, die nicht ausdrücklich zugelassen sind, automatisch abgewiesen werden.

3.5 Beschränkung des Verbindungsaufbaus

Verbindungen in und aus dem Internet müssen immer über das Sicherheits-Gateway laufen.

3.6 Aktualität

Die eingesetzte Betriebssystem- und Anwendungs-Software sollte immer auf dem neuesten Stand gehalten werden. Verfügbare Patches sollten unverzüglich eingepflegt werden.

Darüber hinaus gelten u. a. folgende grundlegende Empfehlungen für den sicheren Betrieb von vernetzten IT-Systemen:

» Entwicklung und Fortschreibung eines IT-Sicherheitskonzeptes,

» regelmäßige Datensicherung,

» regelmäßige Überprüfung der Wiederherstellbarkeit von Sicherungskopien,

» die kontinuierliche Überwachung der Logdaten und Fehlermeldungen mit Fehlerbeseitigung und Anpassung der Schwellenwerte für Alarmierungen,

» die periodische Überprüfung und Erprobung der Notfallpläne,

» die Aktualisierung der Systemdokumentation nach jeder Änderung,

» Durchführung von Revisionen.

Detaillierte Auskünfte, welche Maßnahmen im Einzelfall not wendig oder sinnvoll sind und wie diese am besten umgesetzt werden können, sind in den BSI-Standards zur Internet-Sicherheit (ISi-Reihe) zu finden.

4 BSI-Standards zur Internet-Sicherheit (ISi-Reihe)

4 BSI-Standards zur Internet-Sicherheit (ISi-Reihe)

Die ISi-Reihe macht dem Leser in jedem Modul einen konkreten Vorschlag für eine Architektur, die den sicheren Umgang mit dem jeweiligen Thema ermöglicht. Diese Architektur kann mit zahlreichen Varianten an die eigenen Bedürfnisse angepasst werden. Dadurch wird eine große Flexibilität bei der Anpassung an individuelle Begebenheiten erreicht. Dieser Ansatz deckt sowohl den normalen, als auch den hoher Schutzbedarf umfassend ab. Ein besonderes Gewicht liegt hierbei auf der Konzeption von sicheren IP-Netzen und -Diensten. Die ISi-Reihe ergänzt die IT-Grundschutzkataloge um konkrete Umsetzungsvorschläge zum Thema „Internet-Sicherheit".

Die BSI-Standards zur Internet-Sicherheit sind modular aufgebaut. Jedes Modul beschäftigt sich detailliert mit einem Bereich der Internet-Sicherheit. Es besteht aus einer Leitlinie, einer Studie und Checklisten. Die Leitlinie (ISi-L) richtet sich primär an Führungskräfte und IT-Koordinatoren, die Studie (ISi-S) an alle IT-Fachleute, die Checklisten (ISi-Check) speziell an Administratoren, Programmierer und Web-Entwickler sowie an Revisioren.

Im Folgenden wird kurz auf die bereits existierenden Module eingegangen.

4.1 Sichere Anbindung an das Internet

Soll ein lokales Netz (LAN) an ein nicht vertrauenswürdiges Netz (z. B. das Internet) angeschlossen werden, so muss dieses gegen die zusätzlichen Gefährdungen aus dem Internet abgesichert werden.

Angreifer können Schwachstellen der grundlegenden Internet-Protokolle, -Dienste und -Komponenten ausnutzen und so Datenverkehr abhören („Sniffing"), Systeme mit gefälschten Absenderangaben zu unerwünschtem Verhalten bringen („Spoofing") oder in das interne Netz eindringen („Hacking").

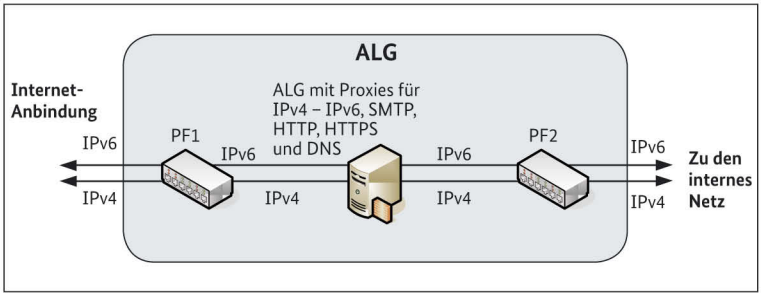
Um sich vor solchen Gefährdungen zu schützen, hilft das Modul der ISi-Reihe „Sichere Anbindung von lokalen Netzen an das Internet" dem Anwender bei der Konzeption des Netzaufbaus, bei der Beschaffung der Komponenten sowie bei der Realisierung und dem Betrieb des Netzes.

Hierbei wurde nicht nur das Protokoll IPv4 betrachtet, sondern das Modul gibt auch Empfehlungen für die Einführung von IPv6, das auch neue Gefährdungen berücksichtigt. Nicht alle am Markt erhältlichen Netzwerk-Komponenten unterstützen IPv6 im selben Umfang wir IPv4. Daher kann es bei der Umstellung auf IPv6 und gerade in der Übergangszeit mit einem parallelen Betrieb von IPv4 und IPv6 zu Mehraufwänden, Stolpersteinen und inkonsistenten Konfigurationen kommen.

In der Studie wird ein Vorschlag für eine Grundarchitektur gemacht, die vornehmlich die Netzzugangsschicht, die Internet-Schicht und die Transportschicht absichert. Es wird auf verschiedene Szenarien eingegangen, wie z. B. der Parallelbetrieb von IPv4 und IPv6. Im Mittelpunkt der Grundarchitektur steht das Sicherheits-Gateway (oft auch Firewall genannt).

Ein Sicherheits-Gateway gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation.

Ein solches Gateway besteht in der Regel aus einem äußeren Paketfilter, einem Application-Level Gateway in der Mitte und einem inneren Paketfilter (s. folgende Abbildung).



Hierbei muss u. a. Folgendes beachtet werden:

» Das Sicherheits-Gateway darf nicht umgangen werden, jeglicher Datenaustausch zwischen Internet und internem Netz muss das Sicherheits-Gateway passieren,

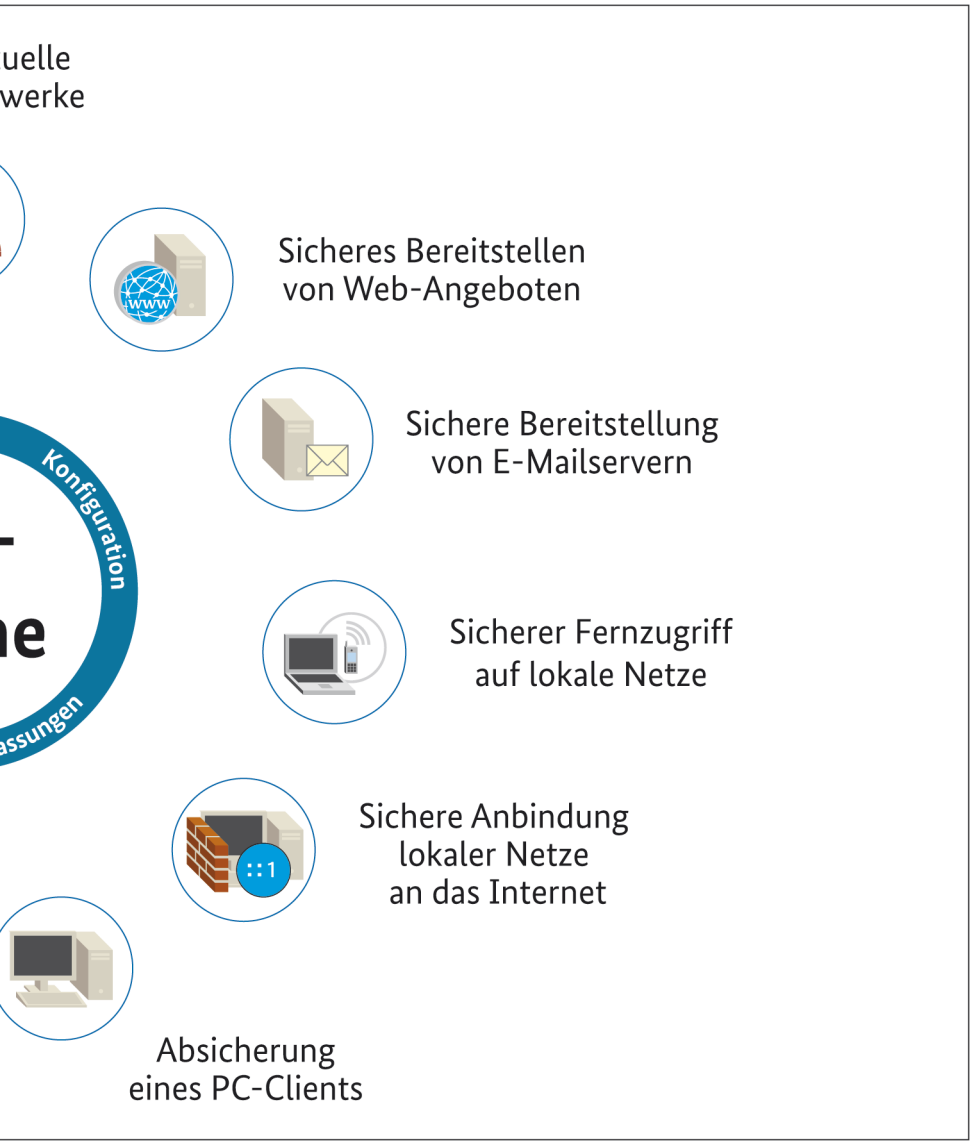
» Verschlüsselte Verbindungen dürfen das Sicherheits-Gateway nicht ungeprüft durchtunneln,

» Zugriffe von außen auf die angebotenen Internet-Dienste werden auf einem Server in einer DMZ (Demilitarisierter Zone) des Sicherheits-Gateways terminiert, um das interne Netz vor Zugriffen zu schützen.

» Bei der Verwendung von IPv6 bekommt das ALG im Sicherheits-Gateway zusätzlich noch die Aufgabe der Adressübersetzung von IPv4 nach IPv6 und umgekehrt.

Die im Folgenden beschriebenen Module der ISi-Reihe bauen auf dieser Grundarchitektur auf und ergänzen diese um die für die Absicherung der jeweiligen Anwendung notwendigen Komponenten und Dienste.


Sichere Virt
Private Netz
Sichere Nutzung
von Web-Angeboten
Sichere Nutzung
von E-Mail
Sicheres
Wireless LAN
Sichere
Internet-Telefonie
Absicherung
eines Servers
Grundarchitektur
ISi-
Reih
individuelle Anp


uelle
werke
Konfiguration
ne
assungen
Sicheres Bereitstellen
von Web-Angeboten
Sichere Bereitstellung
von E-Mailservern
Sicherer Fernzugriff
auf lokale Netze
Sichere Anbindung
lokaler Netze
an das Internet
Absicherung
eines PC-Clients

4.2 Absicherung eines Servers

Institutionen sind von der verlässlichen Nutzung der IT, insbesondere des Internets und des Intranets zunehmend abhängig geworden. Bedingt durch Schwachstellen in den Betriebssystemen und den Programmen, aber auch durch fehlerhafte Konfigurationen von Servern sind vernetzte IT-Systeme erheblichen Gefährdungen ausgesetzt. Sobald ein Server an ein Netz (Internet oder Intranet) angeschlossen wird, besteht die Gefahr, dass Angreifer versuchen Schwachstellen im Betriebssystem oder in Diensten auszunutzen, um deren Verfügbarkeit zu stören, vertrauliche Informationen zu entwenden oder mutwillig Daten zu ändern bzw. zu löschen.

Das Modul „ISi-Server“ empfiehlt eine sichere Grundarchitektur, die auf dem Minimalprinzip beruht. Dies bedeutet, dass nur die für den Betrieb notwendigen Funktionen installiert bzw. aktiviert sind, um so die Angriffsfläche möglichst gering zu halten.

Serversysteme sind von vielen weiteren Systemen abhängig und müssen Schnittstellen für Monitoring, Datensicherung, Patch- und Update-Management, Protokollierung, Benutzerverwaltung und Zeitsynchronisation bieten. Je nach Anwendungsfall kann die Anbindung an ein Speichernetz (NAS, SAN) sinnvoll sein oder die Erweiterung um zusätzliche Komponenten, wie Integritätsprüfung oder Virenschutzprogramm.

Darüber hinaus ist im Serverumfeld Virtualisierung eine weit verbreitete Technik. Auf einem Virtualisierungsserver kann eine Vielzahl von Systemen parallel betrieben werden, welche unterschiedliche Dienste anbieten. Beim Einsatz von Virtualisierung sind zusätzliche Sicherheitsaspekte zwischen den Schnittstellen, wie z. B. zwischen Host- und Gastbetriebssystem oder unterschiedlichen Netzsegmenten, zu berücksichtigen. Die

Studie geht auf die Gefährdungen ein, denen virtuelle Systeme ausgesetzt sind und beschreibt Maßnahmen, die diese Gefährdungen auf ein akzeptables Restrisiko reduzieren.

4.3 Absicherung eines Arbeitsplatz-PCs

Auch mit einem zentralen Sicherheits-Gateway kann nicht auf einen Schutz der Arbeitsplatz-PCs (APCs) im internen Netz verzichtet werden. Schadprogramme können unter Umständen am zentralen Gateway nicht erkannt oder mit USB-Sticks direkt ins interne Netz gebracht werden. Um eine Infektion und ggf. deren Ausbreitung im internen Netz zu verhindern, sind APCs mit Schutzkomponenten, wie einem Virenschutzprogramm, einer Personal Firewall sowie einem Programm zur Integritätsprüfung auszustatten.

Einsatz von Schutzkomponenten sind auch die korrekte Installation und Konfiguration des APCs sowie der korrekte Umgang mit Benutzerrechten von entscheidender Bedeutung.

Benutzer dürfen keine administrative Kontrolle über den APC haben und sollten zentral über einen Verzeichnisdienst verwaltet werden. Die Konfiguration der Schutzkomponenten sowie das Einspielen von Updates/Patches sollte ebenfalls zentral erfolgen, um die Administration zu vereinfachen und Fehlkonfigurationen zu vermeiden.

Das Modul „ISi-Client“ beschränkt sich auf die Absicherung des APCs auf Ebene des Betriebssystems. Der korrekte Umgang mit Anwendungen, wie E-Mail-Clients und Browsern, wird in eigenen ISi-Modulen behandelt.

4.4 Sichere Nutzung von Web-Angeboten

Sowohl Unternehmen und Behörden als auch Privatpersonen können immer mehr Aufgaben und Tätigkeiten über das Web abwickeln. Der Zugang zum Web ermöglicht nicht nur Zugriff auf Informationen aus der ganzen Welt, sondern kann auch die Effizienz in Geschäftsprozessen erheblich steigern. Die Nutzung von Web-Angeboten bringt jedoch zahlreiche Gefährdungen mit sich, wie z. B. Phishing-Attacken, aber auch den Missbrauch von Aktiven Inhalten oder das Ausnutzen von Software-Schwachstellen in Browsern. Das Modul „Sichere Nutzung von Web-Angeboten“ gibt Empfehlungen, wie diesen Gefährdungen bei normalem Schutzbedarf zu begegnen ist: durch eine robuste Architektur des Netzes, eine geeignete Auswahl der Komponenten, sichere Konfigurationseinstellungen sowie systematische Kontrollmechanismen im Betrieb. Zudem werden Varianten aufgezeigt, die auch hohen Schutzbedarf abdecken können.

Zu den grundlegenden Maßnahmen gehören:

» Verzicht auf Aktive Inhalte im internen Netz,

» Einsatz einer separaten Internet-PC-Zone für Aktive Inhalte,

» Einsatz von Virenschutzprogrammen und Personal Firewalls zum Schutz der Clients,

» Erstellung einer Benutzerrichtlinie.

4.5 Sicheres Bereitstellen von Web-Angeboten

Das Modul „Sicheres Bereitstellen von Web-Angeboten“ behandelt die stetig wachsenden Gefährdungen, die bei Bereitstellung von Web-Angeboten, z. B. Internet-Banking und Online-Shops, beachtet werden müssen.

Ein Beispiel für eine solche Gefährdung ist die Manipulation der Inhalte eines Web-Auftritts, die unter Umständen zu einem schweren Ansehensverlust führen kann. Um Web-Angebote ausreichend sicher zur Verfügung stellen zu können, wird eine konkrete Architektur für den normalen Schutzbedarf empfohlen. Hierbei müssen u. a. folgende Grundprinzipien beachtet werden:

» Verzicht auf Aktive Inhalte,

» Sichere Datenübertragung (Verschlüsselung der Datenübertragung zwischen Client und Web-Server z. B. mit SSL),

» Sichere Authentisierung von Benutzern,

» Sicheres Session-Management,

» Kontextsensitive Filterung von Benutzereingaben, Datei-Uploads und Ausgaben,

» Aktualität durch Patch-Management.

4.6 Sichere Nutzung von E-Mail

Besonders Spam und Phishing, aber auch Schadprogramme wie Viren, Würmer und Trojanische Pferde, lassen sich mit der Nutzung von E-Mail in Verbindung bringen. Das Modul „Sichere Nutzung von E-Mail“ beschreibt geeignete Maßnahmen gegen bestehende Gefährdungen. Diese Maßnahmen beziehen sich auf eine sichere Architektur des E-Mail-Clients, eine geschützte Anbindung an den E-Mail-Server und einen sicheren Austausch von Informationen zwischen den Kommunikationspartnern. Es wird u. a. empfohlen:

» Ergänzung der eigentlichen E-Mail-Client-Software durch weitere Komponenten für verschiedene Sicherheitsüberprüfungen, wie ein Virenschutzprogramm, eine Anti-Spam-Software, eine Anti-Phishing-Software und eine Personal Firewall,

» Anbindung der E-Mail-Clients an den E-Mail-Server mittels SSL/TLS sowie zusätzlicher Authentisierung und Verschlüsselung,

» Erstellung einer E-Mail-Richtlinie, die beschreibt, wie sich Benutzer bei der Nutzung von E-Mail zu verhalten haben.

4.7 Sicherer Betrieb von E-Mail-Servern

E-Mail ist als Kommunikationsmittel aus Institutionen heute kaum noch wegzudenken. Bei der Nutzung von E-Mails über das Internet besteht jedoch eine Reihe von Gefährdungen. Ein Angreifer, der Zugriff auf den Netzverkehr hat, kann sämtliche unverschlüsselte E-Mails mitlesen. Dabei kann er auch in den Besitz sensibler Informationen gelangen.

Diese Daten können durch eine Verschlüsselung der E-Mail-Kommunikation geschützt werden. Gegen das unbemerkte Verändern von E-Mails oder die Erstellung von neuen Nachrichten unter falschem Namen können digitale Signaturen helfen. Eine weitere Gefährdung stellen unerwünschte E-Mails (sog. Spam) dar. Sie können einen E-Mail-Server überlasten und damit zum Verlust der Verfügbarkeit des E-Mail-Dienstes führen.

Das Modul ISi-Mail-Server stellt eine sichere E-Mail-Architektur vor. Diese Architektur besteht aus einem Proxy-Server, einem Content-Filter, dem E-Mail-Server an sich und optional noch aus einer virtuellen Poststelle.

4.8 Sicherer Fernzugriff auf das interne Netz

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

Dies ist jedoch mit zahlreichen Risiken verbunden. Das interne Netz muss dazu noch weiter nach außen hin geöffnet werden. 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. Das Modul „Sicherer Fernzugriff auf das interne Netz“ gibt Empfehlungen, wie diesen Gefährdungen bei normalem Schutzbedarf zu begegnen ist.

Zu den wichtigsten Empfehlungen 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.

Zusätzlich wird eine Anwenderrichtlinie empfohlen, in der der Benutzer auf seine Sorgfaltspflichten hingewiesen wird, um so die Risiken durch Nachlässigkeit zu reduzieren.

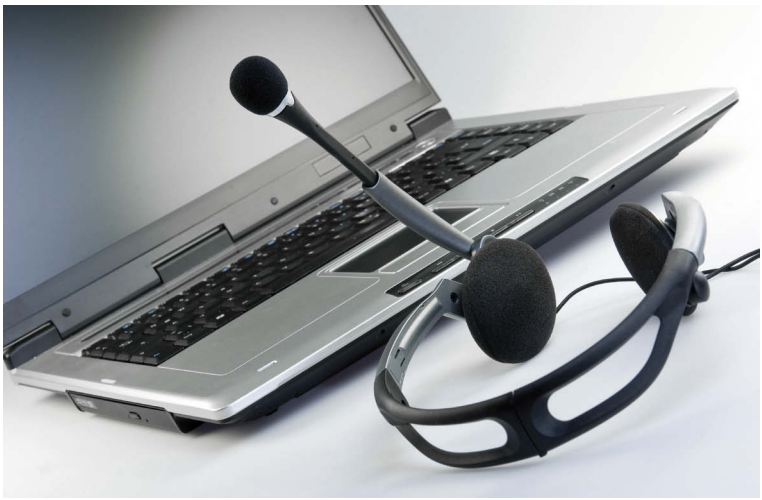
4.9 Sichere Internet-Telefonie

Neben dem Surfen im Internet und dem Kommunizieren über E-Mails stellt das Telefonieren über das Internet eine weitere wichtige Anwendung in den Datennetzen dar. Zusätzlich zu den aus der herkömmlichen Telefonie bekannten Gefährdungen entstehen dadurch zahlreiche neue Risiken. Mögliche Angriffsszenarien sind z. B. das Abhören von Gesprächen, das Stören oder Verhindern von Telefongesprächen oder Gebührenbetrug. Um den netztypischen Gefährdungen zu begegnen, werden in der ISi-Leitlinie „Sichere Internet-Telefonie“ sowie in der BSI-Studie „Voice over IP, Sichere Umstellung der Sprachkommunikation auf IP-Technologie“ umfassende Sicherheitsmaßnahmen beschrieben. Hierzu gehören u. a.:

» Einsatz eines Voice-over-IP-fähigen Sicherheits-Gateways,

» Verschlüsselung der Sprach- und Signalisierungsdaten,

» Absicherung der einzelnen Komponenten auf Internet- und Transportschicht (s. hierzu auch „Sichere Anbindung an das Internet“).



4.10 Sicheres WLAN

Lokale Funknetze (engl. Wireless Local Area Network, WLAN) sind inzwischen weit verbreitet. Ein WLAN lässt sich einfach und kostengünstig installieren und ermöglicht u. a. die arbeitsplatzungebundene Nutzung des Firmennetzes. Über öffentliche Zugangspunkte (Hotspots) ist der Internet-Zugang auch unterwegs möglich.

Jedoch bringt der Einsatz von WLANs zahlreiche Gefährdungen mit sich. So kann beispielsweise die Kommunikation auch noch außerhalb des geplanten Wirkungsbereichs mitgehört werden, was die Vertraulichkeit der übermittelten Daten bedroht. Des Weiteren sind Funkverbindungen sehr anfällig für Störungen, was zu Leistungseinbußen und im schlimmsten Fall sogar zum Verlust der Verfügbarkeit des WLAN führen kann.

In der Leitlinie „ISi-L WLAN“ sowie in weiteren Veröffentlichungen des BSI zu diesem Thema (insbesondere „Technische Richtlinie Sicheres WLAN“) werden Maßnahmen beschrieben, um diesen Gefährdungen zu begegnen. Welche Maßnahmen geeignet sind, ist dabei vom jeweiligen Anwendungsfall abhängig. Für ein WLAN, das zur Erweiterung des LAN verwendet wird, sollten insbesondere folgende Empfehlungen umgesetzt werden:

» Verschlüsselung der Kommunikation,

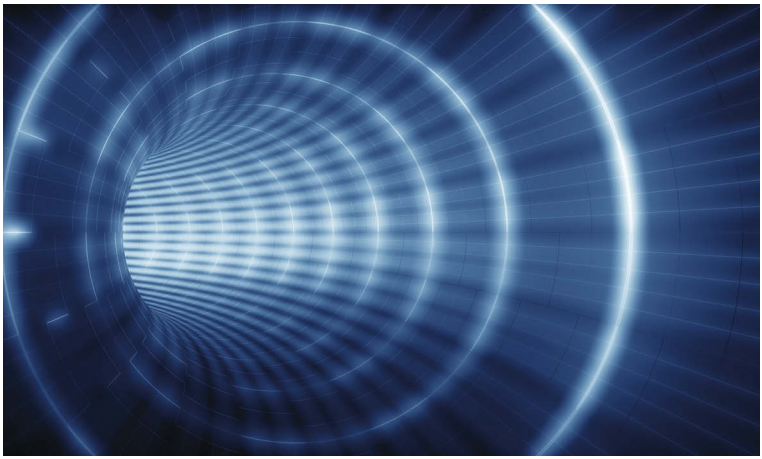
» Gegenseitige Authentisierung zwischen den Endgeräten und der WLAN-Infrastruktur,

» Anpassung und Umsetzung der hauseigenen Sicherheitsrichtlinien.

4.11 Sicheres VPN

Der mobile Zugriff auf Daten des internen Netzes oder die Zusammenarbeit an verschiedenen Standorten erfordern eine gesicherte Verbindung zwischen den Kommunikationspartnern. Virtuelle Private Netzwerke (engl. Virtual Private Network, VPN) bieten hier den notwendigen Rahmen zur Absicherung der Verbindung.

Da das Internet prinzipiell als unsicher betrachtet werden muss, sind Sicherheitsmaßnahmen zu treffen, die gewährleisten, dass sich Unbefugte keinen Zugang über das Internet zum internen Netz verschaffen und die Daten auf dem Weg durch das Internet nicht mitgelesen werden können. In der ISi-Leitlinie „Sicheres VPN“ sowie in der Veröffentlichung des BSI zum Aufbau von Virtual Private Networks werden die wichtigsten Verfahren, u.a. Authentisierung und Verschlüsselung, vorgestellt.



Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de · www.facebook.com/bsi.fuer.buerger

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: isi@bsi.bund.de
Internet: www.isi-reihe.de
Telefon +49 (0) 22899 9582 - 0
Telefax +49 (0) 22899 9582 - 5400

Stand
Januar 2014

Druck
WM Druck + Verlag
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-Bro14/313

www.bsi.bund.de