Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheit im Internet

www.bsi.bund.de
www.bsi-fuer-buerger.de

Sicherheit im Internet

Das Internet bietet eine Vielzahl von Diensten, die von Anbietern bereitgestellt werden. Dazu zählt ein umfangreiches Informationsangebot sowie E-Mail, Chat, Voice over IP u. a.. Jedoch stellt das Internet mit seinen vielen Millionen Benutzern und seiner weltweiten Verfügbarkeit auch eine große Quelle für Angriffe auf die Vertraulichkeit, Verfügbarkeit und Integrität dar. Um sich vor den Bedrohungen und Angriffen zu schützen, stehen eine Reihe von Maßnahmen zur Verfügung. 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. Ganz wichtig ist außerdem, dass Anbieter ihre Dienste im Internet so konzipieren, dass potentielle Nutzer diese in Anspruch nehmen können, ohne die eigenen Sicherheitsmaßnahmen aufzuweichen.

Sichere Anbindung an das Internet

Bei den im Internet angebotenen Diensten müssen sowohl dem Anbieter als auch dem Anwender neben den Funktionen auch die Risiken bewusst sein. Hier liegt besonders bei den Dienste-Anbietern eine große Verantwortung. Denn wenn der Anbieter aktiv etwas gegen mögliche Bedrohungen unternimmt, wird auch auf Nutzerseite das Schadensrisiko minimiert, z. B. durch Verzicht auf Aktive Inhalte bei der Gestaltung von Web-Seiten.

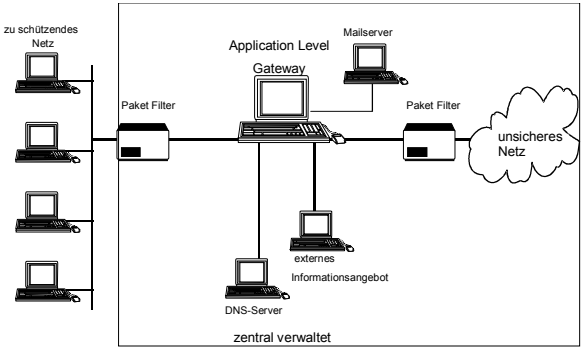
Eine wichtige Standardmaßnahme zum Schutz von Netzen oder Internet-Diensten beim Anschluss an das Internet ist dabei das Sicherheits-Gateway (oft auch Firewall genannt).

Die Hardware-Anordnung und die Default-Einstellung der Filterregeln des Sicherheits-Gateways müssen gewährleisten, dass alle Verbindungen verhindert werden, die nicht explizit erlaubt worden sind. Grundsätzlich sollten keine Verbindungsaufbauten aus dem Internet ins lokale Netz zugelassen werden. Falls Ausnahmen unvermeidbar sind, müssen sie durch geeignete Maßnahmen (z. B. Filterung auf der Anwendungsschicht) besonders abgesichert werden.

Sicherheits-Gateways bestehen zumeist aus:

- Paketfilter: Diese filtern auf der IP- und TCP/UDP-Protokollschicht, also z. B. nach Rechneradresse und Dienst. Sie sollten mindestens:
  - einen TCP/UDP-Verbindungsaufbau erkennen,
  - getrennte Filterregeln für jedes Interface und für kommende und gehende Pakete zulassen sowie
  - eine Protokollierung der Verbindungsdaten und Regelverletzungen zulassen.
- Application Level Gateways (ALG)/Proxys: Diese filtern auf der Anwendungsschicht, also z. B. einzelne Protokollbefehle in Abhängigkeit von der Parametrisierung der Befehle, der Zeit und des Benutzers. ALGs haben u. a. folgende Eigenschaften:
  - benutzerspezifische Filterung,
  - Verdecken der internen Netzstruktur,
  - Filterung der Datenflussrichtung und
  - umfangreiche Protokollierung.

Eine sinnvolle, 3-stufige Anordnungsmöglichkeit für ein Sicherheits-Gateway ist in der Abbildung dargestellt.



Der symmetrische Aufbau bietet auch einen Schutz gegen Angreifer aus dem internen Netz. Der Anschluss der DNS (Domain Name Service, s. Glossar)-, Mail- und Webserver in der DMZ (Demilitarisierte Zone, s. Glossar) an ein zusätzliches Interface sorgt für einen sehr guten Schutz dieser Server gegen Angriffe.

Darüber hinaus ist es wichtig, dass ein Sicherheitskonzept folgende Punkte regelt:

- Was soll geschützt werden?
- Welche Dienste sind erforderlich?
- Welche Benutzer werden zugelassen?
- Wer administriert das Sicherheits-Gateway?
- Welche Daten werden protokolliert und wer wertet diese Daten aus? (Datenschutz!)
- Welcher Datendurchsatz ist zu erwarten? Unzureichende Leistungsfähigkeit kann schnell dazu führen, dass Benutzer versuchen, das Sicherheits-Gateway zu umgehen.

Gefährdungen bei der Nutzung des Internet

Die Basis für einen erfolgreichen Schutz gegen Angriffe ist die umfassende Information über bestehende Bedrohungen und Gefährdungen. Diese betrachtet man allgemein im Hinblick auf die Sicherheits-Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit:

- **Verlust der Vertraulichkeit:** Im Internet werden in der Basiskonfiguration alle Informationen unverschlüsselt übertragen, sodass sie von jedem, der Zugang zu einer an der Übertragung beteiligten Netzkomponente hat, mitgelesen werden können.
- **Verlust der Integrität:** Im Internet werden in der Basiskonfiguration alle Daten ohne einen Schutz gegen Veränderungen übertragen, so dass jeder, der Zugang zu einer an der Übertragung beteiligten Netzkomponenten hat, die Daten manipulieren kann. Des Weiteren können durch Ausnutzen von Sicherheitslücken Angreifer Inhalte auf Servern verändern.
- **Verlust der Verfügbarkeit:** An die Verfügbarkeit des Zugangs zum Internet oder der angebotenen Dienste werden häufig hohe Anforderungen gestellt. Durch technische Defekte, Beeinträchtigung der Infrastruktur aufgrund höherer Gewalt (z. B. Brand oder Hochwasser) oder gezielte Angriffe (DDoS-Angriffe) können wichtige Systeme außer Betrieb gesetzt werden.

Angreifer nutzen bei ihrer Aktivität Schwachstellen (Sicherheitslücken, Verwundbarkeiten) aus, die sie in den Systemen vorfinden. Typische Schwachstellen sind:

- **Programmierfehler**: Durch die mangelhafte Prüfung im Hinblick auf Fehler, die für einen Missbrauch eines Rechnersystems ausgenutzt werden können (z. B. eine fehlende Eingabe-Validierung beim Aufrufen einer Unterroutine), entstehen bei der Erstellung von Software viele schwer wiegenden Sicherheitslücken.
- **Konfigurationsfehler**: Konfigurationsfehler entstehen durch eine falsche oder nicht vollständige Einstellung der Parameter und Optionen, mit denen ein Programm gestartet wird. In diese Gruppe fallen z. B. falsch gesetzte Zugriffsrechte für Dateien.
- **Konzeptionsfehler**: Häufig werden Programme ausgeführt, die zum Betrieb nicht notwendig sind und daher Angreifern unnötig zusätzliche Sicherheitslücken zum Ausnutzen „anbieten“. Des Weiteren kann die Netzarchitektur Konstruktionsfehler aufweisen, z. B. wenn Daten an einem vorhandenen Sicherheits-Gateway vorbei transportiert werden können.

Trifft eine Bedrohung auf eine offene Schwachstelle, entsteht eine Gefährdung. Angriffe wie die im Folgenden beschriebenen werden möglich:

- **Missbrauch von Informationen:** Häufig werden Informationen (z. B. Benutzernamen, Rechnernamen, Namen und Version des verwendeten Betriebssystems), die missbraucht werden können, ungewollt potentiellen Angreifern zur Verfügung gestellt.
- **Passwörter:** Die gebräuchlichste Art der Authentisierung gegenüber einem Rechner beruht auf Passwörtern. Sind diese leicht zu erraten oder anderweitig durch Dritte in Erfahrung zu bringen (Social Engineering), ist ein Missbrauch möglich.
- **Spoofing:** Hierunter wird das Vortäuschen z. B. falscher IP-Adressen (IP-Spoofing) oder falscher Rechnernamen (DNS-Spoofing) verstanden. Rechte, die nur aufgrund dieser Angaben vergeben werden, sind so oft leicht zu missbrauchen.
- **Schadprogramme (Trojanische Pferde, Viren, Würmer):** Programme oder Programmteile mit Schadfunktion können Daten verändern, an Unberechtigte weitergeben, zerstören oder infizierte Rechner unbemerkt zur Teilnahme an einem Bot-Netz zwingen. Schadprogramme werden oft über bösartige Aktive Inhalte in Informationsangeboten oder über E-Mail verteilt.
  Weitere Informationen hierzu siehe:
  http://www.bsi.bund.de/av/index.htm
- **DDoS-Angriff:** Hierbei handelt es sich um einen verteilten Angriff auf die Verfügbar-

keit von Diensten. So können Verzögerungen oder sogar Ausfälle bei der E-Mail-Zustellung mit einer entsprechend großen Flut von Spam-Mails erreicht werden. Auch Informations-Server können durch massenhafte Anfragen überlastet werden und sind dann nur noch eingeschränkt oder gar nicht mehr erreichbar. Für derartige Angriffe werden oft Bot-Netze eingesetzt.

- **Cross-Site-Scripting (XSS):** Dieser Angriff wird oft durch Schwachstellen in dynamisch erstellten Webseiten ermöglicht. Diese Schwachstellen entstehen meistens durch eine mangelhafte Überprüfung der Benutzereingaben. Hiermit können unter anderem vertrauliche Daten von Anwendern (z. B. Kreditkarten-Informationen) gestohlen werden („Phishing"). Oft treten diese XSS-Schwachstellen im Zusammenhang mit der Verwendung von Aktiven Inhalten auf. Dies ist ein wichtiger Grund für die generelle Empfehlung, wenn immer möglich, auf Aktive Inhalte zu verzichten (siehe hierzu):

  http://www.ohne-aktive-inhalte.de

Schutzmöglichkeiten

Vor dem Anschluss an das Internet sollten, neben der Installation eines Sicherheits-Gateways, folgende Maßnahmen ergriffen werden:

Organisatorische Maßnahmen:

1. Beschaffung von Informationen über alle Prozesse, die eine Internet-Verbindung aufbauen können.

   Dies können entweder bereits beim Booten gestartete Prozesse sein oder Prozesse, die erst bei Bedarf von anderen Programmen gestartet werden (z. B. Java-Applets mit Hilfe des Browsers oder unter Unix Daemon-Prozesse mit Hilfe des inetd). Wichtig sind besonders die folgenden Punkte:

   - Welche Informationen können durch diesen Prozess ins Internet gelangen?
   - Bietet der Prozess einem Angreifer die Möglichkeit, Daten auf dem lokalen System oder dem lokalen Netz zu lesen bzw. zu verändern, sich auf dem lokalen System einzuloggen oder auf anderem Wege Informationen über das System zu erlangen?
   - Welche Konfigurationsdateien werden von dem Prozess benutzt? Werden systemweite Konfigurationsdateien verändert?
   - Welche Protokollinformationen werden erzeugt und wie werden diese gespeichert?
   - Besteht die Möglichkeit, dass der Prozess eine Schadfunktion (z. B. Trojanisches Pferd) enthält?

2. Auswahl der benötigten Dienste.

   Auf einem Rechner, der mit einem unsicheren Netz verbunden ist, sollten nicht benötigte und besonders gefährdete Dienste deaktiviert werden.

3. Abschalten und eventuelles Löschen der ungenutzten Programme.

   Um das Starten der Prozesse beim Booten zu verhindern, müssen sie auch aus den Startup-Dateien gelöscht werden. Damit sie nicht indirekt über andere Prozesse starten, müssen die Konfigurationsdateien geändert werden. Hier ist es besonders wichtig, alle Konfigurationsdateien zu berücksichtigen.

4. Beachtung möglicher Schwachstellen der verbliebenen Programme.

   Besonders wichtig sind die Fragen:

   - Gibt es Konzeptionsfehler im Programm oder in den benutzten Netzprotokollen? Die offene Übertragung von Informationen bei TCP/IP kann zu Vertraulichkeitsverlust der übertragenen Daten führen. Dem sollte durch Verschlüsselung begegnet werden.
   - Laufen die Programme in einer geschützten Umgebung und mit eingeschränkten Rechten?
   - Werden sicherheitskritische Bestandteile des Betriebssystems benutzt? Zum Beispiel lassen sich Bibliotheksfunktionen missbrauchen, die bei ihrem Aufruf nicht in einer gesicherten Umgebung ablaufen.
   - Gibt es Hinweise über Schwachstellen im Internet oder beim Hersteller?
   - Gibt es neuere Programmversionen?
   - Gibt es sicherheitskritische Optionen oder Konfigurationsmöglichkeiten?

Technische Maßnahmen:

1. Regelmäßiger Einsatz von Programmen, die Integritätsverletzungen an Programmen und Dateien feststellen können (z. B. unter Unix tripwire).
2. Bei hohen Anforderungen an die Verfügbarkeit des Netzübergangs redundante Auslegung der wichtigsten Komponenten des Netzübergangs.
3. Einsatz von Programmen zur Erkennung von Angriffen auf ein IT-System. Dies kann ein Intrusion Detection System (IDS) sein oder ein anderes zur Frühwarnung taugliches Netzüberwachungssysteme. Ziel ist es, Angriffe so früh wie möglich zu entdecken und gemäß Notfallvorsorgekonzept Gegenmaßnahmen einzuleiten.

4. Einsatz aller Sicherheitsmaßnahmen des Betriebssystems. Hierbei leisten die IT-Grundschutz-Kataloge des BSI oder Prüfprogramme (unter Unix z. B. Nessus) Unterstützung. Wichtig sind folgende Punkte:
   - ► Benutzung „guter“ Passwörter,
   - ► Benutzung aller vorhandenen Protokollmechanismen,
   - ► richtige Vergabe von Rechten,
   - ► regelmäßige Backups sowie
   - ► Einsatz von mitgelieferter Sicherheits-Software (z. B. iptables, ipfw, Windows-Firewall).
5. Abschalten der Ausführung Aktiver Inhalte im verwendeten Browser und zusätzliche Filterung durch das Sicherheits-Gateway.
6. Einsatz von Anti-Viren-Programmen mit aktuellen Virensignaturen.
7. Einsatz von Verschlüsselung und Signaturen zum Schutz der Vertraulichkeit und/oder der Integrität.

Glossar

Aktive Inhalte: Bei Aktiven Inhalten handelt es sich um zusätzlichen Programmcode (wie JavaScript, Java-Applets, ActiveX, Flash etc.), der im Webbrowser auf Seiten des Anwenders ausgeführt wird. Webseiten, die ohne Aktive Inhalte nur teilweise oder gar nicht funktionieren, verführen den Anwender dazu, die Sicherheitseinstellungen in seinem Browser zu lockern. Hierdurch kann es zu ganz unterschiedlichen Gefährdungen kommen. Näheres hierzu siehe:

http://www.bsi.bund.de/fachthem/sinet/index.htm

Bot-Netz: Gruppe von Rechnern, die unter zentraler Kontrolle eines Angreifers stehen und von ihm z. B. für (DDoS-)Angriffe auf andere Rechner oder zum Spam-Versand benutzt werden. Dies geschieht ohne Wissen der Benutzer.

DDoS (Distributed Denial of Service): Verteilter Angriff auf die Verfügbarkeit von Diensten, den viele im Internet verteilte Rechner zusammen ausführen. Häufig kommen Bot-Netze zum Einsatz.

DMZ (Demilitarisierte Zone): Server, die Daten zum Abruf bereitstellen, werden häufig in einer speziellen Sicherheitszone, der DMZ, aufgestellt, um sie vor Angriffen zu schützen. Alle Zugriffe in diese Zone werden vom Sicherheits-Gateway kontrolliert.

DNS (Domain Name Service): Dienst zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt.

IP (Internet Protocol): Verbindungsloses Protokoll entsprechend der Schicht 3 des ISO/OSI-Modells. Ein IP-Header enthält u. a. die IP-Adressen der kommunizierenden Rechner.

Java: Java ist eine Programmiersprache. Häufig wird Java in Form von Java-Applets auf Web-Seiten genutzt. Damit Java-Programme funktionieren, muss auf dem betreffenden Rechner oder im Browser das „Java Runtime Environment“ (JRE) installiert sein. Das Ausführen von Java-Applets bringt nicht unerhebliche Sicherheitsrisiken mit sich.

Phishing: Versuch von Betrügern, IT-Anwender irrezuführen und zur Herausgabe von Authentisierungsmitteln zu bewegen. Dies wird oft bei Internet-Banking-Verfahren eingesetzt.

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.

Spam: Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail

TCP (Transmission Control Protocol): Verbindungsorientiertes Protokoll der Transportschicht, welches auf IP aufsetzt.

UDP (User Datagram Protocol): Verbindungsloses Protokoll der Transportschicht, welches auf IP aufsetzt.

Informationsquellen

Unter der WWW-Adresse

http://www.bsi.bund.de/fachthem/sinet/

finden Sie vertiefende Informationen zum Thema Internet-Sicherheit, darunter z. B. Studien zu folgenden Themen:

- ► Konzeption von Sicherheits-Gateways
- ► Anforderung an Module von Sicherheits-Gateways (Firewalls)
- ► Einführung von Intrusion-Detection-Systemen
- ► Anti-Spam-Strategien
- ► E-Government ohne Aktive Inhalte
- ► Integration und IT-Revision von Netzübergängen
- ► IT-Grundschutz-Kataloge
- ► Sicherheit von Voice over Internet Protocol

Weitere Informationen zum Thema „IT-Sicherheit“ erhalten Sie unter:

WWW: http://www.bsi.bund.de/
WWW: http://www.bsi-fuer-buerger.de/
WWW: http://www.cert-fuer-buerger.de/