Zusammenfassung

Motivation: Das Internet hat in den letzten Jahren zunehmend an Bedeutung gewonnen. Sowohl Unternehmen als auch Privatpersonen nutzen das Internet vermehrt als Kommunikationsmedium. Dabei ergibt sich das Problem, daß das Internet, aus seiner historischen Entwicklung heraus, nicht den Schutz von vertraulichen Daten berücksichtigt. Daher findet heute die Übertragung, selbst sensibelster Daten, häufig unverschlüsselt statt. Die Struktur des Internets ermöglicht dabei ganz besonders einfach das Belauschen und auch die Manipulation der übertragenen Daten. Diese Möglichkeit wird schon heute von vielen staatlichen Organisationen unterschiedlicher Herkunftsländer weltweit genutzt, jedoch stellt es auch für ambitionierte Unternehmen oder Privatpersonen mit dem nötigen technischen Fachwissen kein großes Problem dar, auf Daten, die im Internet übertragen werden, unberechtigt Zugriff zu nehmen. Die Gefahr, die durch diese Möglichkeit ausgeht, wird nur allzu häufig unterschätzt oder die Verantwortlichen sind sich ihrer noch nicht einmal bewußt.

„Sicherheit im Internet“: Unter Sicherheit im Internet ist maßgeblich Kommunikationssicherheit zu verstehen, da speziell dieser Punkt die Sicherheit im Internet von anderen Sicherheitsbegriffen der Informationstechnologie, wie physischer Schutz von Rechneranlagen oder Festlegung von Zugriffsrechten auf Ressourcen, unterscheidet.

Kommunikationssicherheit: Kommunikationssicherheit wird über eine Reihe von zu erfüllenden Kriterien definiert, diese sind:

- Vertraulichkeit – Schutz vertraulicher Informationen vor dem Einblick durch unberechtigte Dritte
- Datenintegrität – Schutz übertragener Daten vor Manipulation durch unberechtigte Dritte
- Verfügbarkeit – Sicherstellung der Verfügbarkeit von Diensten für den berechtigten Nutzer
- Berechtigung
  - Authentifikation – Nachweis der Identität eines Nutzer
  - Zugriffskontrolle – Beschränkung der Nutzungsberechtigung von Diensten
  - Sicherstellung der Zustellung – Beweisbarkeit des Empfangs elektronischer Informationen
- Wahrung der Anonymität – Möglichkeit der anonymen Kommunikation

Organisatorische Maßnahmen: Um ein Unternehmensnetz gegen Angriffe aus dem Internet auf seine Daten und die Kommunikationsinfrastruktur zu schützen, ist es notwendig, die *Sicherheitsanforderungen* zu bestimmen. Dies kann durch eine detaillierte *Risikoanalyse* erfolgen, die sich in vier Teilphasen gliedert:

- Bestandsaufnahme – Bestimmung aller gefährdeter Systeme im Unternehmen
- Bedrohungsanalyse – Untersuchung der Schwachstellen der gefährdeten Systeme
- Bestimmung der Eintrittswahrscheinlichkeit und der möglichen Schadenshöhe
  Risiko = Schadenshöhe × Eintrittswahrscheinlichkeit
- Risikobewertung –Abwägung zwischen tragbaren und nicht tragbaren Risiken

Aus den Ergebnissen der Ermittlung der Sicherheitsanforderungen ergibt sich das *Sicherheitskonzept*. In diesem werden die beschlossenen Maßnahmen zur Schließung der gefundenen Sicherheitslücken festgehalten. Das Sicherheitskonzept darf nicht statisch sein, sondern es muß ein Maßnahmenbündel zur regelmäßigen Anpassung der Anforderungen und zur Überarbeitung der Sicherheitsmaßnahmen enthalten.

Kryptographie: Es wird unterschieden zwischen *Verschlüsselung* und *Message Digest (Signaturen)*. Verschlüsselung dient dem Schutz vor unberechtigter Einsichtnahme und Manipulation. Es werden symmetrische und asymmetrische Verfahren unterschieden. Symmetrische Verfahren verwenden zur Ver- und Entschlüsselung einen identischen Schlüssel; typische Vertreter sind DES, IDEA und CAST. Asymmetrische Verfahren (Public-Key-Verfahren) verwenden zur Ver- und Entschlüsselung zwei

verschiedene Schlüssel, einen sogenannten privaten, geheimzuhaltenden und einen, vom privaten Schlüssel abgeleiteten, öffentlichen Schlüssel; typische Vertreter sind RSA und ElGamal. Message Digest Verfahren dienen der Berechnung eines Fingerabdruckes eines Dokumentes, der der Überprüfung der Authentizität dient. In Verbindung mit Verschlüsselungsverfahren ermöglichen Message Digest Verfahren den effizienten Schutz übertragener Daten vor Manipulation, ohne die Daten selbst verschlüsseln zu müssen.

Protokolle und ihre Sicherheitsprobleme: Die im Internet eingesetzten Protokolle IP, TCP, UDP, ICMP und ARP sind allesamt durch böswillige Dritte angreifbar. Dabei sind die sog. Spoofing-Angriffe, allen voran das *IP-Spoofing*, häufig anzutreffen. Im Rahmen dieser Angriffe werden die Absenderadressen der Datenpakete gefälscht, um den Absender zu verschleiern oder um Zugriff auf Dienste mittels einer vorgetäuschten Identität zu erlangen. Eine weitere Angriffsmöglichkeit, das sog. SYN-Flooding, zielt auf eine Schwachstelle im TCP-Verbindungsaufbau und hat die Nicht-Erreichbarkeit des angegriffenen Systems zum Ziel. Angriffe wie dieser werden Denial-of-Service-Attacken genannt.

Schutz offener Systeme – Firewalls: Unternehmensnetze können vor Angriffen aus dem Internet mittels sog. Firewalls geschützt werden. Diese ermöglichen einen fundamentalen Schutz des zu schützenden Netzes vor unkontrolliertem Datenverkehr zwischen diesem und dem Internet. Es werden zwei Typen von Firewalls unterschieden: Paketfilter und Proxy Gateways. Paketfilter beschränken den Datenverkehr anhand von statischen Informationen des Typs: erlaube / verbiete Datenverkehr zwischen Adresse X und Adresse Y. Paketfilter sind häufig schon in im Unternehmen bereits eingesetzten Routern integriert und sind i.d.R. sehr effizient. Proxy Gateways kontrollieren den Datenverkehr auf höheren Protokollschichten und beziehen dabei auch Informationen über die Art des verwendeten Dienstes bzw. den Typ der übertragenen Daten mit ein. Auch können sie eingesetzt werden, um die Netzwerkstruktur im Unternehmensnetz zu verbergen. Eine häufig in der Praxis eingesetzte Konfiguration beinhaltet den kombinierten Einsatz von Paketfiltern und Proxy Gateways in einem zweistufigen Sicherheitskonzept. Dabei wird zwischen dem außenliegenden Paketfilter und dem innenliegenden Proxy Gateway eine sog. „Demilitarisierte Zone“ geschaffen, in der die vom Internet aus zugänglichen Server (eMail, WWW, DNS etc.) installiert werden. Insgesamt wird durch diese Konfiguration ein hohes Maß an Schutz für die Rechner im Unternehmensnetz erreicht.

Dienste und ihre Sicherheitsprobleme: Die gängigen Dienste des Internet (WWW, FTP, DNS, eMail, Remote Access und Terminalbetrieb) haben allesamt starke Schwachstellen. Sehr häufig beruhen diese auf der unverschlüsselten Übertragung vertraulicher Informationen, wie z.B. Paßwörter. Das WWW, als einer der am häufigsten genutzten Dienste des Internet, besitzt überdies hinaus Schwachstellen bzgl. der Wahrung der Anonymität der Nutzer und der Verwendung aktiver Inhalte, wie beispielsweise Java-Applets. Dem Problem der unverschlüsselten Übertragung kann durch den Einsatz kryptographischer Protokollen, wie z.B. SSL oder S-HTTP, begegnet werden.

Ausblick: Es besteht die Notwendigkeit für die Sicherheitsproblematik des Internets ein breites Bewußtsein, insbesondere bei den Verantwortlichen, zu schaffen und neue Protokolle bereits unter dem Aspekt der Kommunikationssicherheit zu entwerfen.

Literaturempfehlungen:

Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg, 1998

Oppliger, Rolf: Internet and intranet security, Boston, 1997

Shaffer, Steven L.; Simon, Alan R.: Network Security, Boston, 1994

Schneier, Bruce: Applied Cryptography Second Edition – Protocols, Algorithms, and Source Code in C, New York, 1996