

Sicherheit im Netzwerk

1. Einleitung	2
2. Zusammenfassung	2
3. Markt	3
4. Vorgehensweise in Security Projekten	4
5. IT Grundschutz	5
6. Teilbereiche IT Security	6
6.1 Schwachstellenanalyse / Security Audit	6
6.2 Security Policies	7
6.3 Public Key Infrastrukturen (PKI)	7
6.3.1 Authentifizierung und Autorisierung	8
6.3.2 Verbindlichkeit	9
6.3.3 Vertraulichkeit	9
6.3.4 Integrität	9
6.4 Netzwerk	10
6.4.1 Firewalls	10
6.4.2 Vituelle Private Netze	10
6.4.3 Netzwerksicherheit	10
6.5 Mobile Business	11
6.5.1 WLAN	11
6.5.2 UMTS	11
6.6 Software	11
6.6.1 Betriebssystem	11
6.6.2 Middleware	12
6.6.3 Anwendungen	12
6.7 Content Security	12
6.7.1 Malicious Code (Viren, Würmer, Trojaner, Malware u.a.)	12
6.7.2 URL Filter und Content Scanner	13
6.8 Systemintegrität	13
6.8.1 Host basierendes Intrusion Detection	13
6.8.2 Netzwerk basierendes Intrusion Detection	13
6.9 Sonstige Aspekte	13
6.9.1 Juristische Grundlagen	13
6.9.2 Schulung	14
6.9.3 Managed Services	14
6.9.4 Verfügbarkeit	14
6.9.5 Management	14
6.9.6 Physische Sicherheit	14
7. Produktauswahl	14
8. Projektphasen und Services	15
8.1 Schwachstellenanalyse (Assessment)	15
8.2 Design	15
8.3 Implementierung	15
8.4 Betrieb	16

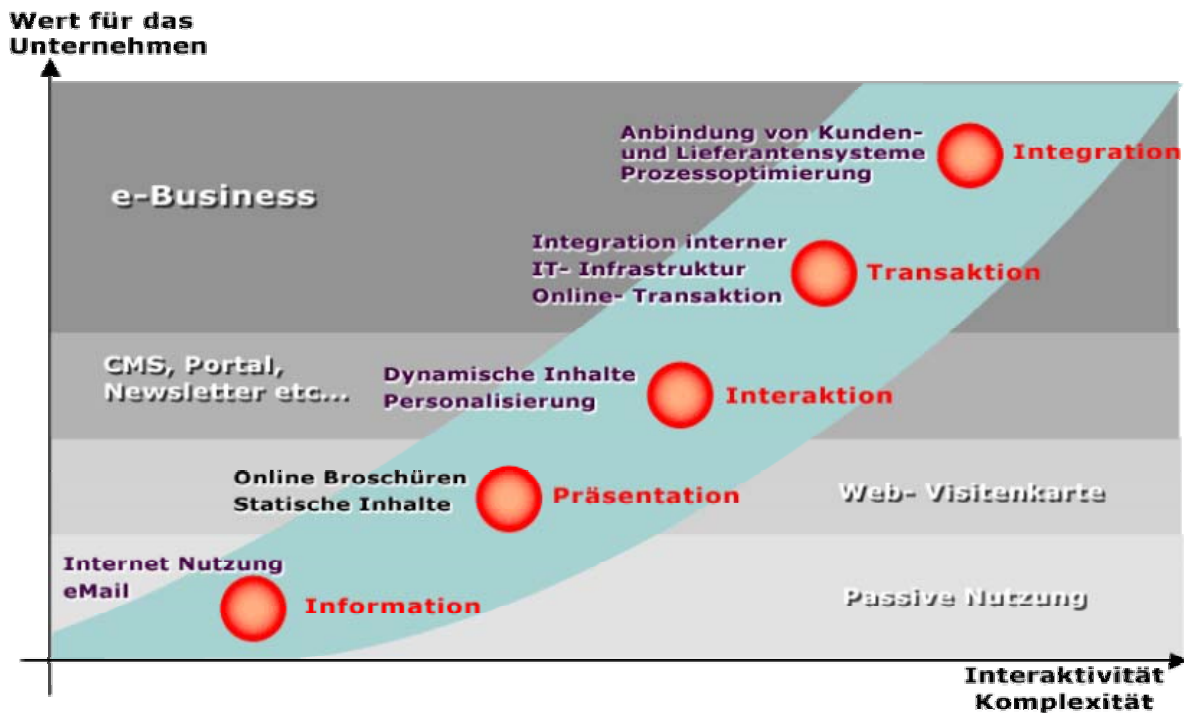
1. Einleitung

Netzwerktechnologien haben Geschäftsprozesse in den letzten 10 Jahren mehr umgestaltet als jede andere Technologie zuvor. Netzwerke durchdringen heute praktisch jedes Unternehmen und kommunizieren untereinander durch das Medium Internet. Angefangen mit der Präsentation von Produkten und Dienstleistungen bis zu Heimarbeitsplätzen, Einkaufsportalen, Kundenbetreuung und Marktplätzen auf Basis des Internets: Unternehmen machen sich und Ihre Leistungen weltweit bekannt, automatisieren Geschäftsprozesse mit ihren Partnern, verbessern die Kundennähe sowie -bindung und das alles bei gleichzeitiger Einsparung von Kosten.

Die einst allein durch physische Isolierung bereits sicheren Backend Prozesse und -daten von Unternehmen sind heute über das Internet weltweit mit praktisch jedem PC vernetzt. Da das Internet selbst keinerlei Funktionen für die Sicherstellung der Vertraulichkeit und Integrität von Daten und Nutzern bietet, sind die Unternehmen spätestens mit der Nutzung des Internets zu einem radikalen Umdenken in Sachen Sicherheit gezwungen.

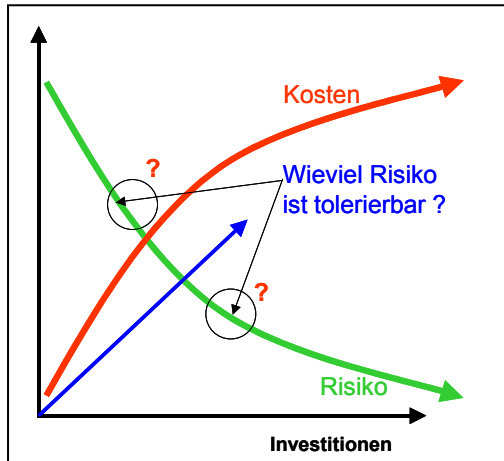
2. Zusammenfassung

In einem Punkt sind sich alle Experten einig; Vollständige Sicherheit gibt es nicht. So wie im „realen“ Leben sind Geschäftsprozesse auch in ihrem elektronischen Equivalent niemals absolut sicher. Effizienter Schutz kann das Sicherheitsrisiko jedoch drastisch reduzieren. Die Kosten für e-Security lassen sich daher nur sehr schwer mit den gängigen ROI¹ Metriken rechtfertigen sondern müssen eher als Versicherungstarif aufgefasst werden. Hierzu ist die Einschätzung des potentiellen Schadens essentiell. Derzeit gibt es jedoch noch keine allgemein anerkannten Methoden zur Umrechnung von Information und Transaktionen in monetäre Equivalente. Es erfordert daher einiges an Verständnis und Einfühlungsvermögen für Branche und Betrieb des Kunden um mit ihm eine gemeinsame Basis für die Beurteilung des Gefährdungspotentials zu finden.



Evolution des Internets: Die Externalisierung von Geschäftsprozessen

¹ ROI: Return of Investment – die Zeit nach der Amortisierung der Investition

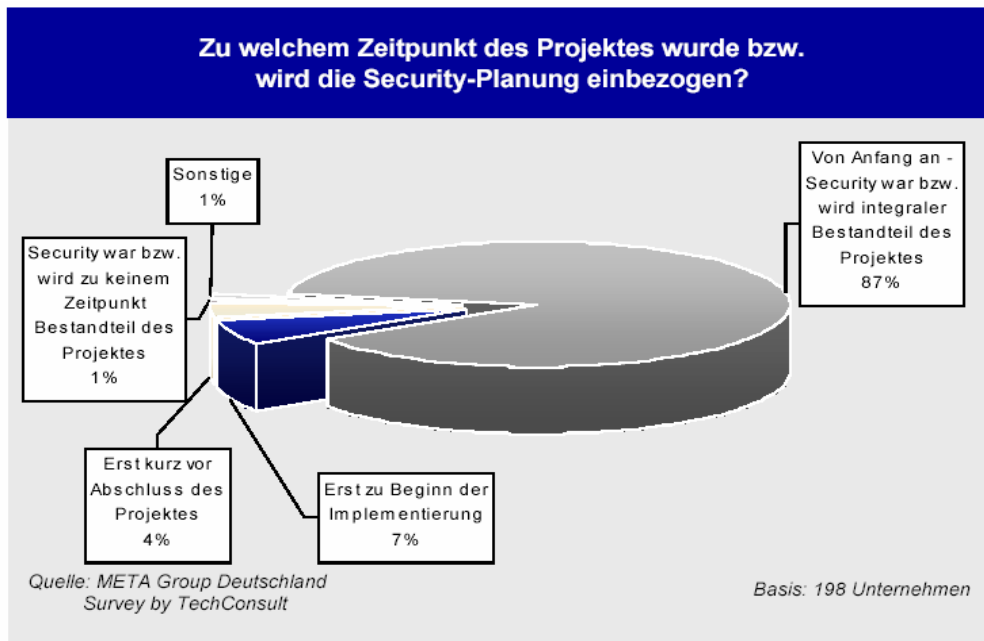


e-Security kann nicht auf die Ansammlung einzelner Produkte reduziert sondern muss als strukturierter, ganzheitlicher Prozess aufgefasst werden. e-Security umfasst das komplette Unternehmensnetzwerk, alle Schnittstellen zur Außenwelt, sämtliche Sicherheitsprozesse als auch die Aufbau- und Ablauforganisation sowie die Unternehmenskultur und damit jeden einzelnen Mitarbeiter und Prozess.

e-Security wird anhand eines definierten Regelwerks stetig überwacht und angepasst. Heutige Netzwerke sind hochgradig funktional und entsprechend komplex aufgebaut. Um diese Netzwerke möglichst effizient zu schützen ist umfangreiches Know-How aus praktisch allen IT-Fachbereichen erforderlich. Gepaart mit der kurzen Halbwertszeit des Security- Know-Hows wird die Entscheidung „Make or Buy“ insbesondere für kleinere Unternehmen immer schwieriger. Bereits in der konzeptionellen Phase wird daher häufig auf Dienstleistungsangebote im Markt zurückgegriffen. Externe Dienstleister spielen in allen e-Security Projektphasen eine zunehmend wichtige Rolle. Selbst der Betrieb sicherer Gateways ist für kleinere Unternehmen oft wirtschaftlicher mit Hilfe sog. *Managed Services* zu realisieren.

e-Security beginnt eine zunehmend strategische Rolle einzunehmen. Lt. Meta Group haben bereits 59% der Unternehmen, die heute e-Business Projekte planen, durchführen oder abgeschlossen haben eine eigene IT- Sicherheitsorganisation. Im Bereich e-Government steht e-Security an erster Stelle der Prioritätenliste. Für Dienstleister im e-Business Umfeld ist daher eine ausgeprägte Kompetenz in diesem Arbeitsfeld unverzichtbar.

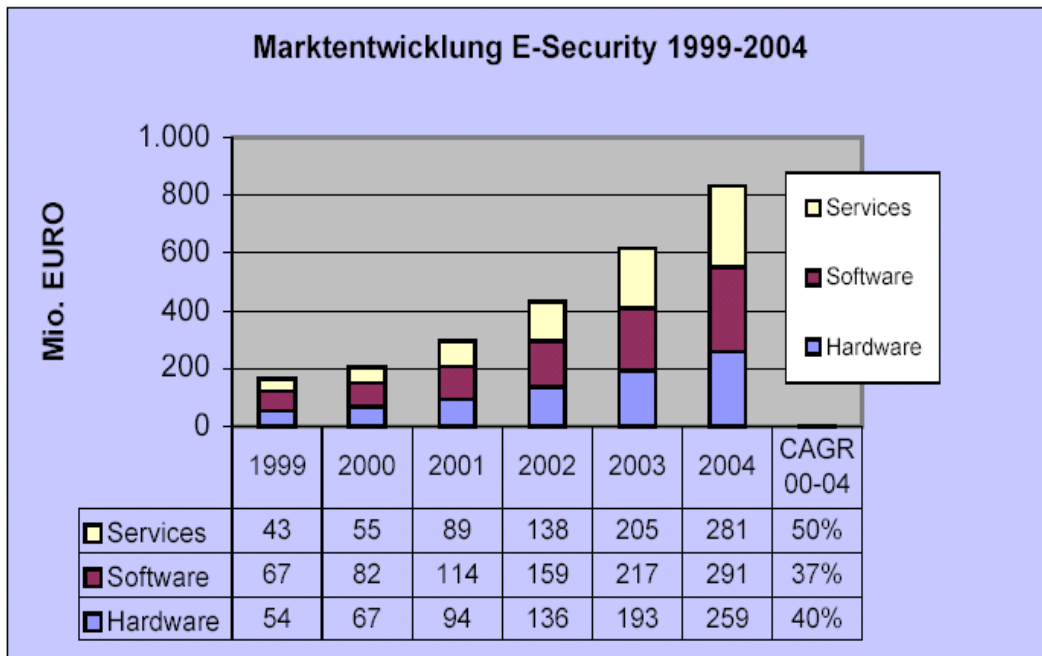
e-Security beginnt eine zunehmend strategische Rolle einzunehmen. Lt. Meta Group haben bereits 59% der Unternehmen, die heute e-Business Projekte planen, durchführen oder abgeschlossen haben eine eigene IT- Sicherheitsorganisation. Im Bereich e-Government steht e-Security an erster Stelle der Prioritätenliste. Für Dienstleister im e-Business Umfeld ist daher eine ausgeprägte Kompetenz in diesem Arbeitsfeld unverzichtbar.



3. Markt

Die Schreckensmeldungen der Virenfront à la *Code Red*, *Melissa*, *Nimda*, *I love you* etc. von denen allein letzterer für einen Gesamtschaden von mehreren Milliarden Dollar verantwortlich sein soll, stellen nur die Spitze des Eisberges dar. Der US-amerikanische CSI/FBI-Report geht von einer 300% Steigerung finanzieller Verluste aufgrund von Sicherheitsproblemen innerhalb von nur 2 Jahren auf fast 400 Millionen US\$ in 2001 aus. Mit dem Anstieg der Externalisierung von Geschäftsprozessen ist eine allgemeine Sensibilisierung der Anwender zu beobachten.

Meta Group erwartet für den e-Security Markt (Security in e-Business Projekten) in Deutschland ein Wachstum (CAGR) von ca. 42% auf 831 Millionen Euro in 2004. Für den e-Security Dienstleistungssektor werden gar 50% CAGR und ca. 280 Millionen Euro Marktvolumen in 2004 erwartet.



Quelle: META Group Deutschland

Das Wachstum für den Gesamtmarkt e-Security wird von 1,3 in 2000 auf 3 Milliarden Euro in 2004 geschätzt. Der Anteil des IT Budgets für Security wird lt. Meta Group voraussichtlich von ehemals 2,3% (1999) auf ca. 5,3% (2004) steigen. Im Bereich des E-Business schätzt Meta Group den Security Anteil auf durchschnittlich 15%. Unternehmen mit mehr als 1000 Mitarbeitern weisen deutlich höhere Ausgaben für IT-Security im E-Business Umfeld auf.

An erster Stelle des Maßnahmenkatalogs stehen bei den Kunden dabei derzeit die Themen **Authentifizierung** und **Autorisierung, Single-Sign-On, PKI** und **Management**. Seit des Inkrafttretens des Signaturgesetzes ist auch ein steigendes Interesse an **digitalen Signaturen** und **Smart Cards** zu beobachten.

Um diese prominenten Security Themen herum gruppieren sich vielfältige Teilbereiche, die sich u.a. mit Virenabwehr, Protokollsicherheit, Kontrolle der Netzwerkaktivitäten, Systemintegrität, aktiver und passiver Hackerabwehr, Kontrolle des Surfverhaltens etc. beschäftigen.

Im Servicebereich spielen **Beratung, Workshops, Risk Assessment, Penetration Testing**, und **Managed Services** eine zunehmend wichtigere Rolle. Heute verfügbare Produkte bedingen hohen Implementierungsaufwand, sind i.d.R. nicht hinsichtlich Interoperabilität designed, bedingen kontinuierliche Produktpflege² und haben oft deutlich negative Auswirkungen auf die Netzwerkleistung.

4. Vorgehensweise in Security Projekten

e-Security ist kein Produkt – sie kann als dynamische Versicherungspolice mit regelmäßigem Soll/Ist Abgleich verstanden werden. Vielen Unternehmen ist bis heute nicht bewusst, wie vielschichtig die Lösung der Aufgabe „Sicherheit“ ist und welche Aspekte es dabei zu beachten gilt. Untersuchungen von dem auf Security spezialisierten Unternehmen ISS³ haben gezeigt, dass Anspruch und Wirklich-

² z.B. regelmäßiges Einspielen von Patches und Updates

³ ISS: Internet Security Systems

keit in den meisten Unternehmen selten deckungsgleich sind. Während die Entscheider annehmen ein Maximum an Sicherheit bereits erreicht zu haben, sehen Security Verantwortliche großen Nachholbedarf und eine neutrale Sicherheitsanalyse ergibt schließlich das Bild eines löchrigen Schweizer Käses.

Eine Sensibilisierung kann über die Ermittlung des Wertes der zu schützenden Informationen und Systeme und einer Schwachstellenanalyse erfolgen, die durch nicht schädigende Angriffe⁴ ergänzt wird (Seit Ende 2001 soll die Nachfrage nach diesen „Security Checks“ lt. Aussagen aus Fachkreisen deutlich zugenommen haben).

Als Ergebnis von **Wertermittlung, Schwachstellenanalyse** und **Penetration Test** wird ein **Maßnahmenkatalog** mit Prioritäten erstellt. Dieser Maßnahmenkatalog ist wiederum Grundlage zur Erstellung einer **e-Security Policy**, die zur Definition der konkreten Security Projekte dient.

Die Ergebnisse werden im Rahmen eines Workshops mit dem Kunden diskutiert und Maßnahmen abgestimmt.

5. IT Grundschutz

Bundesinnenminister Otto Schily hat angesichts der gehäuften Hacker-Angriffe auf das Internet bereits Mitte Februar 2000 eine Task Force "Sicheres Internet" eingesetzt, die das Bedrohungspotential in Deutschland klären und Maßnahmen zur besseren Bekämpfung derartiger Angriffe vorschlagen und koordinieren soll.

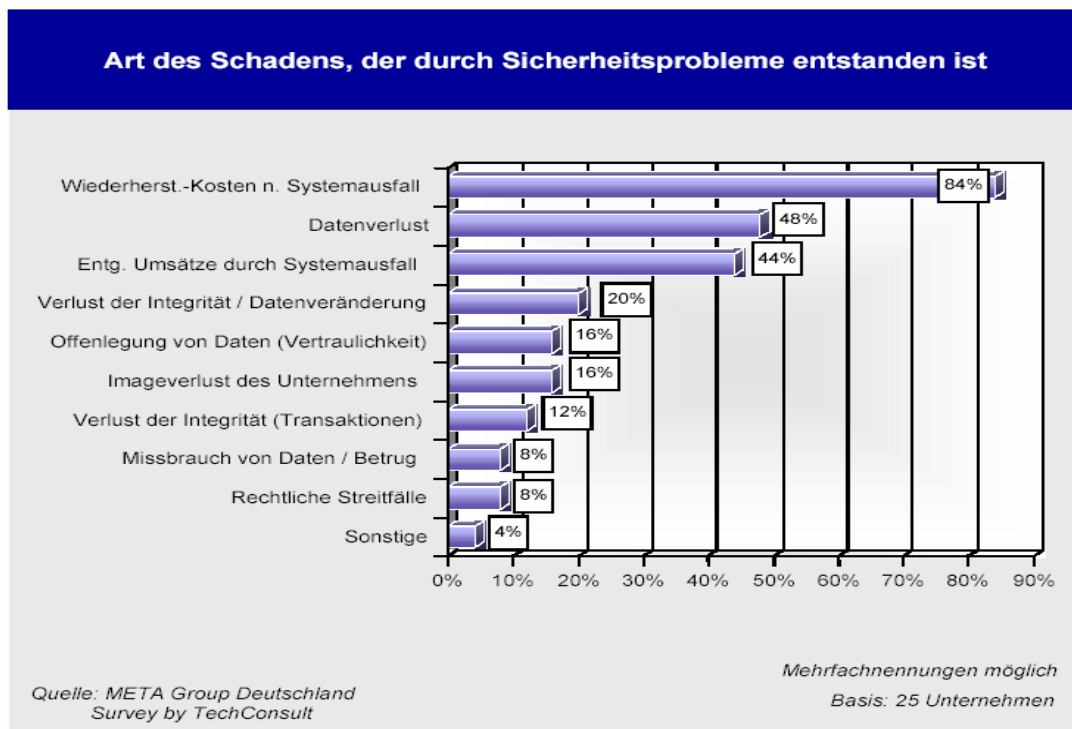
Minister Schily erklärte dazu am 14.02.2000: "Die Sicherheit in der Informationstechnik ist eine Schlüsselfrage für jede moderne Volkswirtschaft. Deshalb wird die Bundesregierung weiter alle Maßnahmen ergreifen, mit der diese Sicherheit auch in Zukunft gewährleistet wird. Sie wird dazu insbesondere den Internet-Providern und den Firmen Hinweise geben, mit welchen Sicherheitstechniken sie sich vor Hacker-Angriffen schützen können. Staat und Wirtschaft müssen gemeinsam daran arbeiten, dieser neuen Art von Angriffen auf die Sicherheit unsers Wirtschaftslebens einen Riegel vorzuschieben. Bei derartigen Angriffen handele es sich keineswegs um technische Spielereien, sondern um Taten, die mit allen Mitteln verhindert werden müssen. Die erheblichen zivilrechtlichen Konsequenzen, wie etwa die Leistung von Schadenersatz an die Geschädigten, sollten allen eine zusätzliche Warnung sein."

Mit dem IT- Grundschutzhandbuch stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) IT- Managern und IT- Sicherheitsbeauftragten einen Mindeststandard für die Informationssicherheit eines Unternehmens zur Verfügung. Darin enthalten sind Maßnahmen zur Betriebssicherheit sowie ein sog. Schutzstufenkonzept. Das Schutzstufenkonzept zeigt die Risiken jeder Schutzstufe sowie erforderliche Gegenmaßnahmen auf. Es kann von IT- Sicherheitsmanagern herangezogen werden, um eine individuelle Schutzbedarfsanalyse vorzunehmen und ein maßgeschneidertes Sicherheitskonzept zu entwickeln.

Bei dem IT- Grundschutz Handbuch handelt es sich um eine umfangreiche Sammlung von Standard-Sicherheitsmaßnahmen, die in ausgedruckter Form 3 Ordner füllen i.d.R. jedoch auch auf dem Medium CD erscheinen. Das „Handbuch“ ist beim BSI kostenlos verfügbar (<http://www.bsi.bund.de/>). Neben dem Handbuch bietet das BSI zweitägige Seminare als Grundlage zum Verständnis des Grundschutzhandbuches an.

⁴ Penetration Tests mit juristischer Absicherung, auch „ethical Hacking“ genannt

6. Teilbereiche IT Security



Die Grundlage für eine kompetente Beratung ist ein umfassendes Wissen über verfügbare e-Security Technologien, Produkte und Trends. Eine kompetente Beratung konzentriert sich nicht allein auf einzelne Technologie- oder Produktbereiche. Die diversen Security Technologien wurden i.d.R. nicht für Interoperabilität entworfen. Das Ziel des Kunden (z.B. „Virenbwehr“) kann auf verschiedenen Wegen mit jeweils verschiedenen Implikationen auf andere IT- Bereiche (z.B. Management und Verhaltensmaßnahmen für die Mitarbeiter) erreicht werden. IT- Security ist daher eine ganzheitliche Angelegenheit, die Menschen, Prozesse und Technologie gleichermaßen betrifft.

Der IT- Security Markt befindet sich noch in den Anfängen. Einer Vielzahl von Funktionen steht eine noch größere Anzahl von Produkten gegenüber. Heutigen Netzwerken wird mit steigender Tendenz ein hohes Maß an Funktionalität abverlangt. Der Grad der Funktionalität verhält sich dabei oft umgekehrt proportional zur Sicherheit des Systems. Mehr Funktionalität sollte daher stets die zusätzlich erforderlichen Sicherheitsmaßnahmen berücksichtigen.

Generell gilt, dass zusätzliche Maßnahmen die Sicherheit erhöhen. Wenig Sinn macht es jedoch wenn die Kosten aller gewählten Maßnahmen den Wert des zu schützenden Wirtschaftsguts übersteigen. Die Entscheidung welche Sicherheitsmaßnahme in welcher Ausprägung implementiert werden soll muss daher genauso wirtschaftliche als auch technische Aspekte berücksichtigen und ist individuell unterschiedlich zu betrachten.

Die im Folgenden aufgeführten Security Themen sollen die einzelnen Aspekte des Arbeitsbereichs E-Security darstellen. Dabei ist grundsätzlich immer zu berücksichtigen, dass IT-Security Produkte nicht isoliert betrachtet werden dürfen sondern immer in größerem Zusammenhang gesehen werden müssen.

6.1 Schwachstellenanalyse / Security Audit

Eine Schwachstellenanalyse setzt sehr viel Know-How voraus, da sie sämtliche Teilbereiche der IT-Infrastruktur ganzheitlich erfassen muss. Die ständig erforderliche Aus- und Weiterbildung der Auditoren ist für viele Unternehmen wirtschaftlich kaum vertretbar. Für externe Dienstleister spricht auch der höhere Grad an Neutralität. Security Audits bilden daher das Geschäftspotential von Dienstleistern,

die ihr Know-How kontinuierlich in verschiedenen Projekten anwenden können und deren Wertschöpfung in der Mehrfachnutzung ihrer Know-How Investitionen liegt. Security Audits werden daher als „Initial- Packet“ als auch als regelmäßiger Service (Soll / Ist Vergleich mit abgeleitetem Maßnahmenkatalog) angeboten.

6.2 Security Policies

Neben den wirtschaftlichen und technischen Aspekten sind für eine ausreichend sichere Umgebung stets Verfahrensweisen (Policies) zu definieren und eine Infrastruktur zu deren Umsetzung zu schaffen. Selbst abgeschottete Netzwerke sind einem Virus ausgeliefert, der physisch mittels Laptop eingeschleppt bzw. in einem Dokumentenmakro vom Geschäftspartner unwissentlich versandt wurde. Wie sehen die Eskalationsprozeduren im „K-Fall“ aus? Was geschieht mit den umfangreichen Protokollen der Firewalls? Wer wertet diese wie aus? Was geschieht bei Diebstahl eines Laptops? Nach welchen Regeln werden Updates und Patches installiert? Wer regelt die Art & Laufzeit von Passwörtern? Dieses sehr umfangreiche Thema „Security Policies“ (= Vorgabe zum Erkennen von und verantwortungsvollen Umgang mit Sicherheitsrisiken) ist ein wesentliches Element von Security Workshops und sollte integraler Bestandteil jedes Security- oder e-Business Projekts sein. Die Definition der Security Policy steht am Anfang jedes Security Projektes und geht direkt aus dem Audit hervor. Eine Security Policy definiert den Sollzustand in abstrakter Form und ist vorzugsweise modular aufzubauen. Eine wirkungsvolle Security Policy muss von der Unternehmensleitung als strategisches Ziel erkannt und entsprechend unterstützt werden. Die Ausarbeitung der Security Policy ist eine Dienstleistung, die in enger Zusammenarbeit mit dem Kunden erbracht wird.

6.3 Public Key Infrastruktur (PKI)

PKI wird oft als der „große Ansatz“ bezeichnet, da PKI den Anspruch erhebt einen überall und für jedermann verfügbaren universellen Mechanismus zur Sicherung von Authentifizierung und Vertraulichkeit zu bieten.

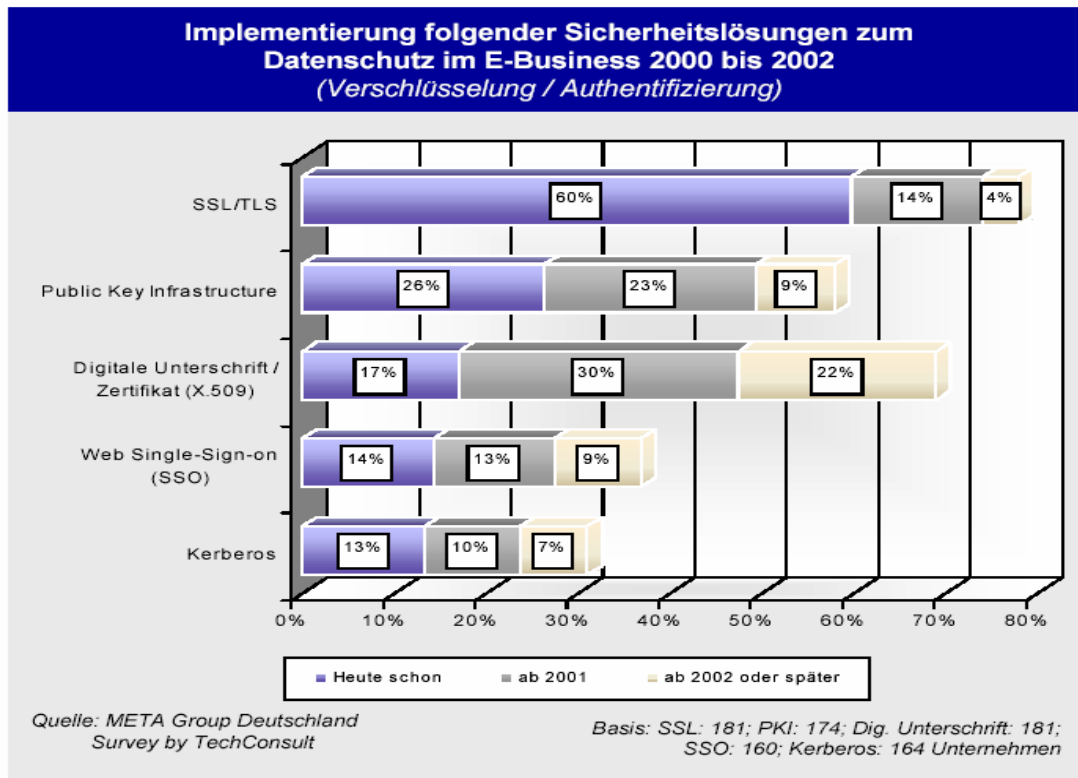
Große PKI Implementierungen gibt es in Deutschland z.B. bei Bayer, Bertelsmann, BMW, Commerzbank, DaimlerChrysler, Deutsche Bahn, Deutsche Bank, Dresdner Bank, HypoVereinsbank, Mannesmann, Siemens, Thyssen, VW etc...

Die Kosten für Anschaffung und Betrieb des „großen Ansatzes“ sind jedoch erheblich und nicht immer wirtschaftlich zu rechtfertigen. Die „großen PKI Lösungen“ werden – wie bei jeder Infrastruktur - umso effizienter, je mehr Benutzer, Systeme und Anwendungen partizipieren. Oft werden daher voneinander unabhängige, in sich geschlossene Teillösungen implementiert um die Anforderungen an Authentifizierung und Verschlüsselung zumindest punktuell zu ermöglichen. Mit Zunahme der Benutzer und Anwendungen verringert sich jedoch die Akzeptanz der Nutzer (aufgrund mehrfacher Anmeldeprozeduren) und es steigt der Administrationsaufwand (durch die Verwaltung unterschiedlichster Systeme) als auch das Sicherheitsrisiko (je mehr Passwörter erforderlich sind, um so schwächer werden diese). Ideal ist eine offene Architektur von PKI- Punktlösungen, die bei Bedarf eine Skalierung zur umfassenden PKI erlaubt.

Zum Aufbau einer PKI innerhalb von Unternehmensgrenzen gibt es eine Vielzahl möglicher Designs, die sich neben der teilweise sehr unterschiedlichen Lizenzstruktur besonders in ihrer Kompatibilität untereinander unterscheiden. Die Integration zweier geschlossener PKIs (z.B.: Extranet zweier Unternehmen) kann schon gravierende Probleme bereiten. Zur Authentifizierung über Unternehmensgrenzen hinweg wird eine relativ aufwändige Infrastruktur benötigt um Schlüssel und Zertifikate der Anwender zu verwalten. Eine „offene“ PKI erfordert die Integration einer - aus Sicht der Kommunikationspartner - vertrauenswürdigen dritten Partei (Trust Center). In Deutschland gibt es nur eine kleine Anzahl wichtiger Trust Center⁵. Die wesentlichen Elemente einer PKI sind neben dem Trust Center und verwandter Themen wie z.B. der Digitalen Signatur⁶ die Funktionen zur Authentifizierung der Kommunikationspartner, Sicherung der Vertraulichkeit von Informationen und Wahrung der Integrität von Dokumenten.

⁵ TeleSec (Deutsche Telekom AG), SignTrust (Deutsche Post AG), TC Trustcenter (Hamburg), TeleCash (Stuttgart), CCI (Meppen), Datev, D-Trust (Berlin), Identrus (Globales Bankenkonsortium)

⁶ zur Sicherstellung der Verbindlichkeit von Dokumenten



6.3.1 Authentifizierung und Autorisierung

Die Authentifizierung des Benutzers ist integraler Bestandteil jedes e-Business Prozesses. Nur wenn die Teilnehmer (Personen oder IT-Systeme) eindeutig identifizierbar sind ist ein Geschäftsprozess überhaupt durchführbar.

Unter *Authentifizierung* versteht man die Feststellung der Identität und unter *Autorisierung* die Zuteilung von *Rechten*. Es gibt Produkte für jede der Funktionen als auch Kombinationen.

Allgemein wird von „starker“ und „schwacher“ Authentifizierung gesprochen. Die Ausprägung ergibt sich aus Art, Implementierung und Anzahl der verwendeten Technologien. Zur Authentifizierung von Personen gibt es im Wesentlichen 3 Möglichkeiten: Identifikation über das, was man hat (z.B. SecureID- oder Chipkarte, USB-Token, BIOS Authentifizierung), weiß (z.B. UserID und Password) und/oder ist (Biometrische Merkmale, z.B. Fingerabdruck, Gesicht- oder Iriserkennung).

Mechanismen zur Authentifizierung müssen besonders in Zusammenhang mit Unternehmensportalen, Verzeichnisdiensten, Single-Sign-On und PKI gesehen werden. Die Produktauswahl hängt von einer Vielzahl kundenspezifischer Faktoren ab. (siehe 6.3).

Beratungsleistungen im Umfeld von größeren Projekten zu Authentifizierung und Autorisierung setzen u.a. umfangreiches Know-How und Erfahrung bei der Planung von Verzeichnisdiensten voraus. Entsprechende Projekte können sich von der Planungs- bis zur Implementierungsphase über viele Monate hinziehen. Kleinere, abgegrenzte Projekte können der Ausgangspunkt für die Konsolidierung von Verzeichnisdiensten oder einer PKI sein. In jedem Falle sollte angestrebt werden Beratungsleistungen auch bei kleineren Projekten einzubringen um das Potential längerfristig qualifizieren und ggf. beeinflussen zu können.

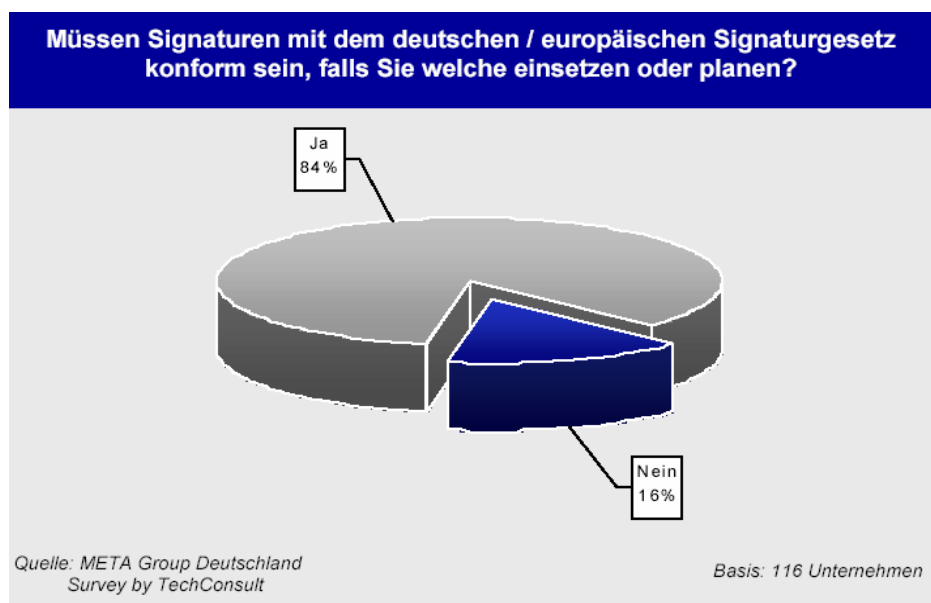
Am Markt findet man diverse Technologien, Architekturen und Designs zur **Authentifizierung** von Personen und Systemen (i.d.R. basierend auf dem X.509 Standard für **digitale Zertifikate**, die von einem Trust Center – oft die eigene IT-Abteilung – erstellt werden; z.B.: *Microsoft's Active Directory zur Authentifizierung mit Kerberos zur Autorisierung oder Novell's eDirectory sowie spezialisierte PKI-Lösungen von Verisign, EnTrust, Valicert, SecureID etc...*). Im wesentlichen ist zwischen „LAN-“ und „Internetfähigen“ PKI-Implementierungen zu unterscheiden. LAN Implementierungen basieren teilweise auf hauseigenen Standards oder sind aufgrund ihres Designs für Internetumgebungen weniger geeignet. Internetfähige PKI-Designs weisen internetkonforme flache Verzeichnishierarchien auf (z.B.: Anton.Mueller@Firma.de), verwenden Standard Internetprotokolle (z.B. LDAP), unterstützen offene Standards zur Funktionserweiterung und sind hochgradig verfügbar (z.B durch Cluster).

6.3.2 Verbindlichkeit

Nach einer Umfrage der Meta Group hatten bis 2001 bereits 17% der Unternehmen X.509 basierende Zertifikate implementiert (technologische Grundlage der rechtsverbindlichen digitalen Signatur). In 2001 beabsichtigen weitere 30% und ab 2002 weitere 22% den Einsatz.

Nach der Ratifizierung des Gesetzes zur digitalen Signatur hat die elektronische Unterschrift mittlerweile Rechtsgültigkeit. Das Signaturgesetz regelt die Produktion, die Verwaltung, den Einsatz und die rechtliche Verwendung von Signaturen. Gerade im Umfeld des E-Government kommt der digitalen Signatur auf Grundlage von PKI eine zentrale Rolle zu.

Aus juristischer Sicht sind trotz der mittlerweile erzielten Rechtssicherheit noch ein paar offene Punkte zu klären. Der Nachweis für Missbrauch und damit die Haftungsfrage ist aus technischen Gründen nicht ganz so klar geregelt wie bei den traditionellen Methoden. Trotzdem ist das Thema „Digitale Signatur“ eminent wichtig, da es für die Verbindlichkeit von unternehmens- übergreifenden e-Business Prozessen steht. Das aktuelle Technologie-, Produkt- und Rechtsumfeld sollte jedem kompetenten e-Business Berater zumindest in seinen Grundzügen bekannt sein.



6.3.3 Vertraulichkeit

Vertraulichkeit von geschäftlichen Dokumenten ist eine weitere wichtige Voraussetzung von e-Business Prozessen. Die Wahrung der Vertraulichkeit wird entweder durch de-facto Standards wie SSL/TSL⁷ für Webseiten oder S/MIME für e-Mail Dienste gewährleistet. Im mehr privaten Umfeld ist das Open Source Produkt PGP⁸ weit verbreitet, von dem es auch kommerzielle Versionen gibt. Für die Schlüsselverwaltung gibt es unterschiedliche Möglichkeiten: Von manuell über Punktlösungen bis zu mit Verzeichnisdiensten integrierten umfassenden Single-Sign-On und VPN Verfahren.

6.3.4 Integrität

Auch die Unverfälschtheit von Dokumenten ist eine Voraussetzung von e-Business Prozessen. Unverfälschtheit wird technisch durch Implementierung bestimmter mathematischer Algorithmen gewährleistet. Dabei handelt es sich i.d.R. um Softwarelösungen. Zusätzlich Services wie z.B. Zeitstempeldienste können die Einbeziehung von Trust Center erforderlich machen. Zeitstempel dienen dem Nachweis wann Dokumente erstellt bzw. versandt wurden und sind im Geschäftsverkehr für Prozesse wie z.B. Preisstellung, Auftragserteilung, -stornierung, Lieferzeiten etc. praktisch unverzichtbar.

⁷ SSL: Secure Sockets Layer, TSL: Transport Security Layer (Verschlüsseltes Internetprotokoll auf http- Basis)

⁸ PGP: Pretty Goog Privacy

6.4 Netzwerk

Ein wesentlicher Stützpfeiler der Netzwerksicherheit ist die Zuverlässigkeit der eingesetzten Netzwerkprotokolle hinsichtlich Authentifizierung, Vertraulichkeit und Integrität. Die in jüngster Zeit wieder häufig in der Öffentlichkeit diskutierten DOS (Denial Of Service⁹) Attacken, Identitätsübernahmen (Phishing), Datendiebstähle etc. sind ein deutliches Zeichen für die Angreifbarkeit der derzeitigen Internetprotokollsuite (IPv4).

6.4.1 Firewalls

Prominentestes Produkt aus dem Bereich Netzwerksicherheit ist die *Firewall*. Eine Firewall regelt, kontrolliert und protokolliert den Verkehr zwischen unterschiedlichen Schutz- bzw Sicherheitszonen. Marktführer sind Checkpoint (Software) und Nokia (Appliances¹⁰). Auch CISCO beansprucht eine Führungsposition, fokussiert jedoch mehr den VPN Markt (s.u.). Die Bandbreite der Modelle ist sehr facettenreich und reicht von der kostenlosen Freeware für den Privatanwender bis zum hochverfügbaren Unternehmensgateway mit integriertem Proxy, Virenschanner, Mail und andere Applikationen. Gerade im Bereich verteilter Enterprise Firewalls und VPNs (s.u.) spielt das Thema „Administration“ eine zunehmend wichtigere Rolle.

Aufgrund der relativ hohen Anschaffungskosten und des kontinuierlich hohen Administrationsaufwands sowie der notwendigen Personalvorhaltung für den Notfall stehen mittelständische Betriebe oft vor der Frage des Outsourcings und suchen dediziert Beratung hierzu bzw. Managed Services Partner.

6.4.2 Virtuelle Private Netze

VPNs (Virtuelle Private Netze) nutzen das öffentliche Internet für Standort- übergreifende private Kommunikations-Verbindungen. Damit Unbefugte geschäftskritische Informationen und Anwendungen nicht einsehen können, schaffen VPNs getrennte logische Einheiten, die nur einem geschlossenen Benutzerkreis zugänglich sind. 21 Prozent der deutschen Unternehmen mit mehr als 50 Mitarbeitern setzen diese Technik bereits erfolgreich ein - Tendenz steigend.

Markttreiber Virtueller Privater Netzwerke sind die hohen Sicherheitsanforderungen an Remote- Verbindungen von SOHO¹¹ ins Unternehmensnetz als auch die durch die Internetanbindung erzielbaren Kosteneinsparungen für die Verbindungskosten (im Vergleich zu Wähl- und Mietleitungen). Weiterhin erlauben VPNs große Flexibilität aufgrund der homogenen Internetstruktur.

VPNs werden anwenderseitig (z.B. Home Office und Filialen) oft mit Softwarekomponenten oder Appliances realisiert. Die Appliances vereinigen dabei heutzutage praktisch sämtliche, auf Anwenderseite benötigten Netzwerkfunktionen¹² in einem Gerät). Appliances sollten mittels eines zentralen Regelwerkes administrierbar sein, so dass sie praktisch „Plug & Play“ Charakter haben. Die Preise für die SOHO Geräte sind oft geringer als die eines PCs. In größeren Unternehmen werden VPN Services i.d.R. zentral durch Firewall- Funktionen realisiert. Die zentrale IT benötigt für VPNs leistungsfähige und hochverfügbare Unternehmens- Gateways (Firewalls).

6.4.3 Netzwerksicherheit

Die hauptsächliche Funktionsweise handelsüblicher Firewalls ist heute noch meist die eines Paketfilters. Ein Paketfilter kann Protokollkonforme Datenströme nicht am Eindringen ins Unternehmen hindern. Die passierten Daten können trotz „Unbedenklichkeitserklärung“ der Firewall im Unternehmensnetz jedoch noch immer beträchtlichen Schaden verursachen bzw. die Sicherheit des Netzes kompromittieren.

Es werden ständig neue Möglichkeiten entdeckt, Firewalls zu überlisten.

Verschiedene Konzepte werden derzeit diskutiert um die Sicherheitslücken der heutigen Internetprotokollsuite zu schließen. Sie reichen von zügiger Einführung sicherer Protokolle (IPv6: Protokollsuite u.a. zur Verbesserung von Authentifizierung und Vertraulichkeit) bis zur Gegenschlags Philosophie der Internet Sheriffs. Gerade im Bereich „Cyber Warfare“ versuchten sich sogar bereits Spin-Offs von Unternehmen wie *Price Waterhouse Coopers* zu profilieren. Dabei überwiegen noch

⁹ DOS,DDOS: Überlastung von Servern bis zur Blockierung der Funktionalität

¹⁰ Appliance: „Black Box“ aus Hard- und Software; Nur durch Funktionalität definiert

¹¹ SOHO: Small Office / Home Office

¹² Router (ggf. mit Alternativverbindung), Firewall, Verschlüsselung und Switch

ungeklärte juristische Aspekte insbesondere bei der „aktiven“ Abwehr von Hacker Attacken. Gegen wen darf sich ein Gegenschlag richten und wie ist die Haftungsfrage bei den kaum vermeidbaren „Kollateralschäden“ geregelt ?

Netzwerksicherheit ist ein umfangreicher, schnell wachsender Arbeitsbereich.

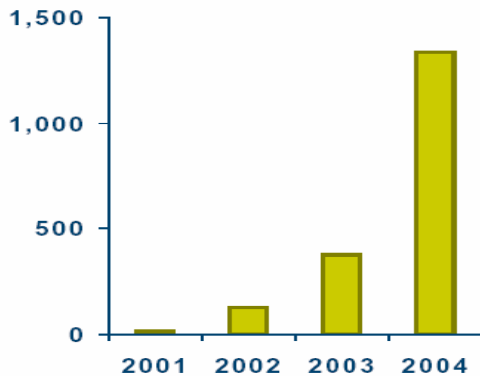
6.5 Mobile Business

Die meisten großen und mittelständischen Unternehmen haben bereits eine „Wireless“ Strategie definiert. Davon betroffen sind insbesondere die Bereiche Fernzugriff für mobile Mitarbeiter, Funk- LANs oder ganz allgemein: drahtloser Zugriff auf e- Services des Unternehmens.

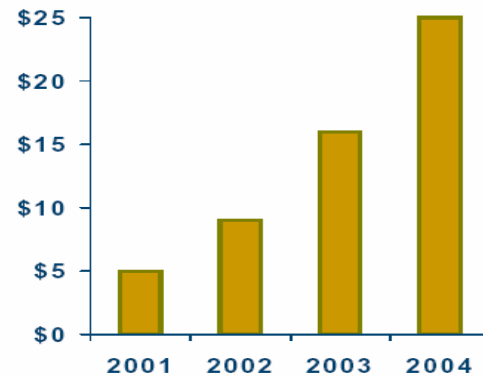
E.g., US Mobile eBanking

E.g., Mobile eBusiness Services

Customers (000)



Billions WW



Source: IDC 2002

6.5.1 WLAN¹³

Wireless LANs gelten als eine der Schlüsseltechnologien der nächsten Jahre. Da auf WLANs prinzipiell jedermann in Reichweite eines Hot-Spots (bis über 100m) zugreifen kann, sind diese unter besonderer Berücksichtigung von Sicherheitsaspekten zu planen. Wichtige Themen im Bereich WLAN sind Authentifizierung und Vertraulichkeit der gespeicherten Daten und des Datentransfers als auch der Virusschutz für mobile Geräte. Mobile Geräte sind im wesentlichen Laptops und PDAs.

6.5.2 UMTS

UMTS fällt mittelfristig aufgrund der hohen Flächendurchdringung eine langfristig größere Bedeutung als der WLAN Technologie zu. UMTS soll u.a. den Durchbruch für (insbesondere B-2-C) M-Commerce bringen. Im Gegensatz zur WLAN Technologie ist die sichere Authentifizierung bei UMTS bereits Teil der Netzwerk Infrastruktur.

6.6 Software

6.6.1 Betriebssystem

Es vergeht keine Woche, in der nicht neue Sicherheitslücken in Betriebssystemen erkannt werden. Entgegen der weit verbreiteten Annahme betrifft dieses Problem nicht nur die Betriebssysteme aus dem Hause Gates. Betriebssysteme sind die Plattform für Anwendungen und müssen daher eine Vielzahl von Funktionen zur Verfügung stellen. Sicherheitsgefahren gehen dabei von mangelhafter Implementierung, von schlechter Produktpflege (Patches) und Programmierfehlern (z.B. Buffer Overflow) aus.

¹³ Wireless Local Area Network

6.6.2 Middleware

Unter dem Begriff „Middleware“ versteht man die Software Infrastruktur eines Netzwerkes, die auf Plattform- und Netzwerkinfrastruktur aufsetzt. Dazu zählen z.B. Verzeichnisdienste, Application Server und Management Software. Besonders gefährdet sind all jene Komponenten oder Services, die aufgrund ihrer Aufgabendefinition aus der Internetzone erreichbar sein müssen. Durch die direkte Erreichbarkeit tragen sie i.d.R. zu größerem Funktionsumfang oder zur Effizienz der Infrastruktur bei, erhöhen jedoch gleichzeitig das Gefährdungspotential.

Auch Datenbanken stellen aufgrund ihrer Struktur eine Gefährdung der Vertraulichkeit dar. Die Gefahr mit konstruierten Abfragen und/oder Eingaben auch ohne Berechtigung vertrauliche Informationen (z.B. personenbezogene Daten) durch Korrelation der Ergebnisse in Erfahrung zu bringen kann zwar reduziert, doch kaum vermieden werden. Hier sind Sicherheitsmaßnahmen auf organisatorischer Ebene ausschlaggebend.

6.6.3 Anwendungen

Sicherheitslücken in Anwendungen beruhen i.d.R. auf schlechter Softwarequalität. Die Verfügbarkeit neuer Produkte entscheidet oft über deren Erfolg oder Misserfolg. Der Markt toleriert eher Fehler in Produkten als ein spätes Erscheinungsdatum. Es ist daher leider üblich, dass gerade Produkte mit hoher Marktdurchdringung oft eher schlampig programmiert wurden. Qualitätssicherungsmaßnahmen wie in der herstellenden Industrie weit verbreitet, haben sich bei den Anwendungsentwicklern aufgrund des Käuferverhaltens noch nicht durchsetzen können. Abhilfe schafft in solchen Fällen nur das regelmäßige Einspielen neuer Patches und Updates sowie die Beobachtung entsprechender Newsgroups.

6.7 Content Security

Unter Content Security versteht man die Gewährleistung der Sicherheit auf der Ebene von Informationsinhalten.

6.7.1 Malicious Code (Viren, Würmer, Trojaner, Malware u.a.)

Infiziert ein Virus erst einmal ein System (Arbeitsplatzrechner oder Unternehmensserver), hat es Zugriff auf alle Systemressourcen, die es zu seiner Verbreitung im Netzwerk nutzen kann.

Es gibt viele Arten von Viren. Man klassifiziert zum einen nach der Art und Weise der Verbreitung und zum anderen nach dem angerichteten Schaden. Die meisten Viren sind relativ harmlos und richten kaum offensichtlichen Schaden an. Bösartige Viren verändern Daten in mehr oder minder großem Umfang, veranlassen Arbeitsplatzrechner heimlich an automatisierten Hackerattacken teilzunehmen oder spionieren Passwörter und Kartennummern aus. Jeder dieser Viren – auch die vorgeblich harmlosen - kompromittiert die Systemsicherheit und verletzt die Systemintegrität. Tickende Zeitbomben sind das Ergebnis.

Es gibt viele Wege, wie ein Virus in Clientrechner oder Server eingeschleust werden kann. Ausführbare Dateien in eMail Anhängen, Makros von Textverarbeitungssystemen, „mobiler Code“ wie ActiveX, JavaScript, ActionScript (Flash), Java Applets u.v.a.m.

Viren sind schwer in den Griff zu bekommen, da sie erst bekämpft werden können nachdem sie entdeckt und analysiert wurden. Bis zu diesem Zeitpunkt sind oft bereits erhebliche Schäden entstanden. Man schätzt, dass der Industrie allein durch die Beseitigung der Schäden des *I Love You* Virus im Mai 2000 weltweit ein Schaden von mehreren Milliarden US\$ entstanden ist.

Die meisten derzeit verbreiteten Scanner basieren auf dem Vergleich von Dateien auf bekannte Virenmuster („Signaturen“). Diese Virenmuster werden vom Softwarehersteller regelmäßig (meist täglich, bei manchen sogar stündlich) im Internet aktualisiert. Virenscanner erkennen und beseitigen je nach Design die Viren bereits auf den Proxy- und Mailservern des Unternehmens bevor sie das Zielgerät erreichen und sie verrichten ihre Arbeit direkt auf den mobilen Endgeräten, da diese auch direkt mit dem Internet in Verbindung kommen und unter Umgehung des Unternehmensschutzes infizieren können.

Das Problem o.a. Virenscanner ist, dass nur Viren erkannt werden, die bereits vom Scannerhersteller gefunden und vom Administrator aktualisiert wurden. Da es zu diesem Zeitpunkt bereits ein großflächiger Befall eingetreten sein kann, werden neue technologische Ansätze vorangetrieben (z.B. Heuristic Analyzer, Redundant Scanner, Behavior Blocker, Integrity Checker), die es der Software

ermöglichen sollen auch völlig unbekannte Viren z.B. aufgrund ihres „verdächtigen“ Verhaltens erkennen zu können.

6.7.2 URL Filter und Content Scanner

URL Filter blockieren den Zugriff auf Webseiten, die in für Mitarbeiter „unproduktive“ Kategorien fallen. Die Filter arbeiten auf Basis elektronischer Kategorielisten (ähnlich wie Virens Scanner mit Listen von Signaturen arbeiten), die vom Hersteller regelmäßig aktualisiert werden. URL Filter sind einfache Tools, die auf Internet Gateways im Rahmen größerer Security Projekte implementiert werden können.

Unter *Content Scannern* versteht man Tools, die „den Mitarbeiter vor sich selbst schützen“. Dies ist natürlich ein Marketingstatement um Berührungspunkte abzubauen. Tatsächlich beabsichtigen Unternehmen mit dem Einsatz sog. „Content Scanner“ Mitarbeiter von unproduktiver Arbeitszeit und erhöhten Kommunikationskosten durch privates Internetsurfen und durch Kommunikation mittels privater eMails abzuhalten. Dabei wird der Inhalt sämtlicher Information bei manchen Tools bereits vor dem Zustandekommen der Kommunikation am Unternehmens Gateway analysiert und ggf. isoliert. Das Konzept ist durchaus nicht unumstritten. Gegner dieser Technologie führen u.a. an, dass Content Scanning nur die Symptome verfehlter Mitarbeiterführung bekämpfen statt die Ursachen zu beseitigen.

Trotz aller Gegenargumente ist der Markt für *Content Scanner* im Wachstum begriffen. Fast wichtiger als die Technologie selbst ist die Beachtung juristischer Feinheiten bei der Implementierung der Policies (Betriebsrat einschalten, Verhaltensmaßregeln für Mitarbeiter und Administratoren kommunizieren, Einverständniserklärungen einholen etc...).

6.8 Systemintegrität

6.8.1 Host basierendes Intrusion Detection

Nach Entfernung von Viren oder erfolgreich bekämpften Hackerangriffen stellt sich stets die Frage nach der verbliebenen Integrität des Systems. Was haben Viren im System verändert? Welche Kuckuckseier hat der Hacker hinterlassen? Um unliebsame Überraschungen auszuschließen kann es erforderlich sein, eine Vielzahl von Systemen mit großem Aufwand neu aufzusetzen.

Wie der Begriff „Intrusion Detection“ bereits impliziert ist es Ziel dieser Technologie ein unrechtmäßiges Eindringen in die Sicherheitszone eines Unternehmensnetzes möglichst schnell zu erkennen. Dies kann durch regelmäßiges Scannen von Systemdateien, der Registry, Userlisten, Verzeichnissen oder durch die Beobachtung des Netzwerkverhaltens geschehen.

Anbieter, wie z.B. *Tripwire*, bieten Softwarelösungen, die mit Hilfe von Hashwerten¹⁴ Systemdateien automatisiert auf deren Integrität prüfen und der Administration erheblichen Aufwand sparen können, indem veränderte Dateien schnell identifiziert werden.

Bei der Verhinderung von Manipulation an Systemdateien spricht man auch von „Server-Protection“. *Nimble* und *Code Red* hätten bei Einsatz dieser Techniken kaum eine Chance gehabt.

6.8.2 Netzwerk basierendes Intrusion Detection

Wird „live“ nach Abweichungen von üblichen Netzwerkverkehrsmustern gesucht spricht man von *Netzwerk basierendem Intrusion Detection*. Diese Intrusion Detection Technologie erfordert großes Know-How von Seiten des Anwenders bzw. Administrators. Trotz – oder gerade wegen – der eingebauten Intelligenz der Tools. Bereits bei der Erstellung von Policies und der Platzierung der Netzwerksensoren werden tiefgehende Kenntnisse und Erfahrung benötigt. Die Interpretation der Alarme und die entsprechende Justage der Policies im Betrieb sind Sache des Fachmanns.

6.9 Sonstige Aspekte

6.9.1 Juristische Grundlagen

Insbesondere bei den Themen „Strike Back“ zur aktiven Hackerabwehr, Content Scanning und Rechtsverbindlichkeit digitaler Signaturen und Zertifikaten im PKI- Umfeld sind die juristischen Gegebenheiten zu beachten. In manchen Randbereichen (z.B. Haftung bei Missbrauch digitaler Signaturen) fehlt derzeit noch die Erfahrung über praktizierte Rechtsprechung.

¹⁴ eine Art Prüfsumme

6.9.2 Schulung

Der Erfolg eines Security Projektes hängt wesentlich von der aktiven Beteiligung der Mitarbeiter ab. I.d.R. ist das der Großteil der Belegschaft. Projektteams müssen daher mit besonderer Sorgfalt zusammengestellt werden und großen Wert auf Schulung der Mitarbeiter legen.

6.9.3 Managed Services

Outsourcing von Security Funktionalität kann in bestimmten Situationen günstiger sein als der Betrieb einer eigenen Security Infrastruktur.

Gerade im Bereich IT- Security sind die Kosten für die „Einmalnutzung“ von Know-How Trägern vielen Unternehmen zu hoch. Hierzu sollten die Angebote von Managed Service Providern analysiert werden.

6.9.4 Verfügbarkeit

Verfügbarkeit wird neben Authentifizierung, Vertraulichkeit und Integrität häufig als vierte Hauptsäule der IT- Security erwähnt. Ziel aller Security Arbeitsbereiche muss es daher sein, Produkte und Technologien u.a. nach Verfügbarkeitskriterien zu kategorisieren (Dies trifft prinzipiell auch für die Skalierbarkeit von Lösungen zu). Besondere Priorität genießen Verfügbarkeitsmerkmale auf Netzwerk- und Anwendungsebene.

6.9.5 Management

Heute verfügbare Security- Produkte wurden i.d.R. nicht auf Kompatibilität und Integration untereinander entwickelt. Die Managementintegration ist jedoch ein entscheidender Aspekt des für die Kunden wichtigen Total Cost of Ownership. Bei der Produktauswahl sollte auf ein möglichst hohes Integrationsniveau und weniger auf die neuesten Features Wert gelegt werden.

6.9.6 Physische Sicherheit

Neben den IT spezifischen Maßnahmen führt das IT- Grundschriftbuch u.a. Maßnahmenkataloge zur Gebäude Infrastruktur auf. Hierzu gehört z.B. der Brandschutz, Pförtnerdienst, die Anordnung schützenswerter Gebäudeteile, Blitzschutzanlagen etc. Insgesamt sind Stand 2001 58 Maßnahmen allein für die Gebäude Infrastruktur definiert.

7. Produktauswahl

Die Produktauswahl erfolgt nach folgenden Kriterien:

- Offenheit (Standards, Interoperabilität, Integrationsfähigkeit)
- Skalierbarkeit
- Verfügbarkeit
- Managementintegration
- Marktposition

Hersteller (Marktführer und Innovatoren), die den Anspruch erheben o.a. Kriterien zu entsprechen:

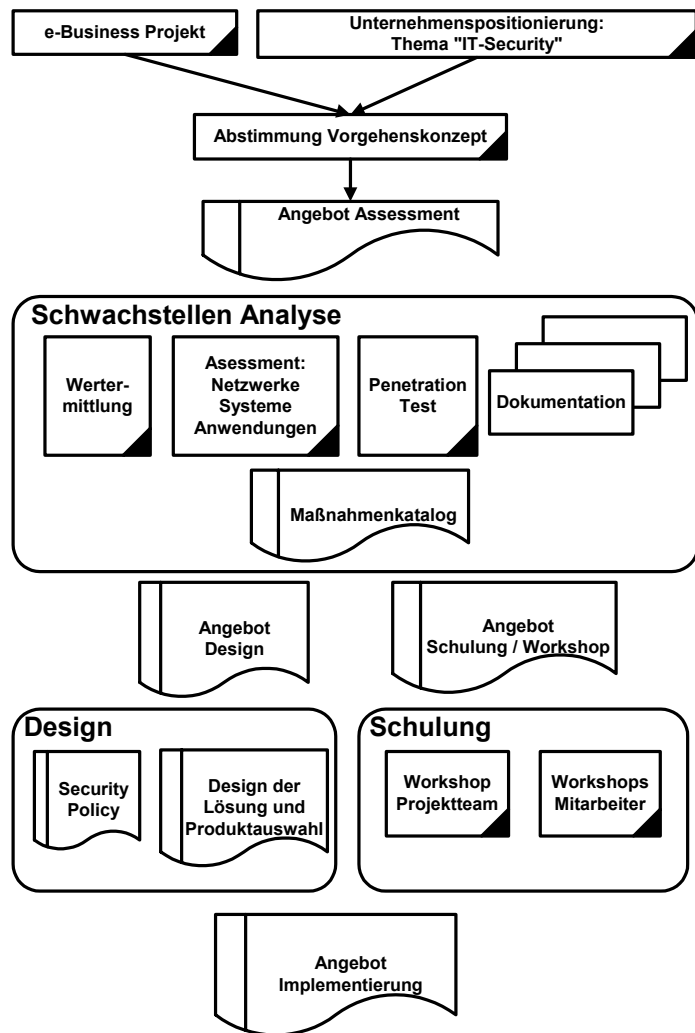
- Trend Micro (alle Arten der Virenbekämpfung)
- Verisign (Zertifikate, Authentifizierung)
- SUN (Authentifizierung, Single-Sign-On, PKI)
- Checkpoint, Cisco (Firewalls und VPN)
- Nokia (Appliances auf Basis von Checkpoint Software)
- Webtrends (Firewall Log Analyzer)
- Rainfinity, Stonebeat (Firewall Clustering)
- Sonicwall (preisgünstige Alternative zu kleinen Nokia Appliances)
- RSA (starke Authentifizierung mit SecureID)
- ISS, Tripwire, Intrusion.com (Intrusion Detection)
- Icnogito, Webwasher, Websense, Surfcontrol (Content Scanner / Filter)

Aufgrund des Widerspruchs zwischen der Forderung nach reduzierter Komplexität zur Verbesserung der Sicherheit und den heute noch vorwiegend verwendeten „Multi Purpose“ Plattformen geht die Tendenz immer mehr in Richtung dedizierter Appliances oder auch „Blades“. Dabei handelt es sich um „Black Boxes“, die sich einzig durch ihre Funktionalität und Schnittstellen definieren.

8. Projektphasen und Services

8.1 Schwachstellenanalyse (Assessment)

Die Schwachstellenanalyse beinhaltet einen betriebswirtschaftlichen und einen technisch orientierten Teil. Im betriebswirtschaftlichen Teil wird der Wert der zu schützenden Informationen und Betriebsmittel erfasst. Für die Ermittlung des Wertes abstrakter Informationen und Ressourcen eines Unternehmens gibt es im Gegensatz zu den mittlerweile weit verbreiteten ROI Tools für die unterschiedlichsten Zwecke (z.B. *Migration* oder *Konsolidierung*) derzeit noch keine allgemein anerkannten Vorgehensweisen. Im technischen Teil erfolgt die Bestandsaufnahme der Ist-Situation, die Analyse der Infrastruktur und der verwendeten Technologien als auch der Penetration Test. Aus dieser Analyse wird ein abstrakter Maßnahmenkatalog erstellt.



8.2 Design

In der Designphase wird der abstrakter gehaltene Maßnahmenkatalog auf die konkreten Anforderungen der vorhandenen Infrastruktur und der im Markt verfügbaren Produkte heruntergebrochen. Je nach Umfang des Projektes kann es erforderlich sein, mehr oder minder aufwändige Security Policies aufzustellen. Als Ergebnis der Designphase folgt das Angebot für die Implementierung. Bei den Workshops oder zur Vorbereitung können bereits Produktspezialisten von Herstellern und/oder Distributoren hinzugezogen werden. Die Beratungsleistungen sollten nach Möglichkeit Organisations- und Prozessberatung beinhalten.

Design Services umfassen u.a.:

- Aufnahme und Dokumentation der betrieblichen und technischen Anforderungen
- Entwicklung der Netzwerkarchitektur und Definition der „Quality of Service“
- Erstellung einer Security Policy
- Erstellung des technischen Designs auf Basis der zuvor fixierten Anforderungen
- Planung und Berücksichtigung strategischer Erweiterungen der Netzwerkumgebung
- Bewertung und Auswahl der bevorzugten Technologien, Hersteller und Produkte

8.3 Implementierung

Implementierungsservices enthalten häufig die Leistungen:

- Projektmanagement und Projektcontrolling
- Prototyping und Pilotierung
- Systemkonfiguration und –integration
- Systemtest

- Dokumentationsdienste
- Roll-Out Management
- Inbetriebnahme der Lösung
- Training und Systemschulungen

8.4 Betrieb

Für die Softwarepflege bieten praktisch alle Hersteller bezahlbare und kostenfreie Internet Update Verfahren an.