

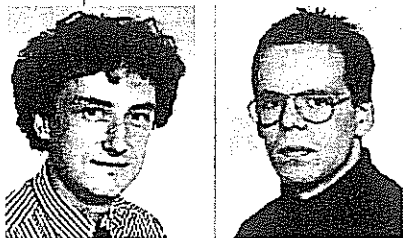
Intranet: Gefahr für Know-how-Schutz

Die Steigerung der Effizienz durch Zeitersparnis bei kommunikativen Arbeitsabläufen und die damit verbundene Kostenreduzierung sind entscheidende Gründe für die Unternehmen, Intranets als lokale Netz einzuführen. Bei einer aktuellen, europaweiten Umfrage verfügten bereits 31% der Großunternehmen über ein Intranet, weitere 47% planen den Einsatz in den nächsten zwei Jahren. Doch diese Art der Vernetzung birgt Sicherheitsrisiken.

von Lutz Gaeth und Michael Haack, Berlin

Ziel einer Intranet-Realisierung ist die wirkungsvolle Unterstützung von Geschäftsprozessen über die physischen Grenzen des Unternehmens hinaus. Verbindungen zu Kunden, Außendienstanschlüssen, Heimarbeitsplätze, unternehmensweite Netze über mehrere Standorte und die Tendenz zu virtuellen Unternehmen fördern die Vernetzung. Unter Intranet ist dabei die Nutzung von Internet-Technologie für unternehmensinterne Netze zu verstehen. Dazu gehören beispielsweise die für WWW-Seiten verwendete Beschreibungssprache HTML und das Protokoll HTTP, Programmier- bzw. Scriptsprachen wie JAVA, Javascript,

Über unsere Autoren:



Lutz Gaeth (l.) arbeitet seit Jahren als Dipl. Wirtschaftsingenieur (FH) und Dipl.-Informatiker in der Hard- und Softwareentwicklung. Seit 1992 ist er bei der UBIS GmbH als Berater im Bereich Unternehmenssicherheit tätig.
Michael Haack (r.) ist Dipl.-Informatiker und seit 1995 ebenfalls als Berater im Bereich Unternehmenssicherheit bei der UBIS GmbH tätig.

CGI und Active-X, die E-Mail-Protokolle SMTP, POP3 sowie als Basisprotokoll TCP/IP.

Die Verwendung dieser erprobten und herstellerunabhängigen Technik ist kostengünstig und bringt Vorteile bei der externen Verbindung, denn die offenen Standards erleichtern die Kommunikation mit unterschiedlichen Partnern. Damit wird auch die Basis zum Electronic Commerce mit anonymen Kunden geschaffen.

Bedrohungen und Risiken

Mit der Übernahme der Technologie werden allerdings auch die meisten sicherheitskritischen Aspekte vom Internet auf das firmeneigene Intranet vererbt. Zentrales Problem ist, daß die Sicherheitsanforderungen an ein geschlossenes Informationsnetz (Intranet) denen eines offenen Netzes (Internet) in starkem Maße widersprechen.

Das Kapital eines Unternehmens liegt heute in den Informationen, und genau in diesem Schlüsselsegment werden die Unternehmen mit einer völlig neuen Anforderungen an die Sicherheit konfrontiert. Ein Beispiel: Anfänglich waren E-Mails als Ergänzung zur hausinternen Nachrichtenübermittlung gedacht. Mit wachsender Akzeptanz wurden auch wichtige, vertrauliche Inhalte per E-Mail versandt. Heute ist es ein zentrales Medium zur Kommunikation mit externen Unternehmensstandorten und den Kunden. Zu beobachten ist, daß je „normaler“ und alltäglicher die Nutzung wird, desto sorgloser gehen die Mitarbeiter offensichtlich da-

mit um. Daß die versandten Informationen nun nicht mehr „im Firmengebäude“ bleiben, sondern über eine unbekannte Anzahl von Zwischenstationen (hops) übermittelt werden und dort in der Regel unverschlüsselt vorliegen, ist den meisten Nutzern nicht bewußt. Doch auch Manipulationen im Netz innerhalb des eigenen Unternehmens sind konkrete Bedrohungen.

Die entstehende Bedrohung ist nicht neu: Es geht, wie schon bei den traditionellen IT-Netzwerken der Unternehmen, um Vertraulichkeit, Verfügbarkeit und Integrität der Daten, um die Möglichkeit, daß vertrauliche Informationen abgehört werden und um das Risiko, daß für die Geschäftsprozesse essentielle Informationen verfälscht oder vernichtet werden. Doch mit dem Intranet werden neue Angriffsflächen geschaffen. Die wichtigsten Bedrohungen im Intranet-Umfeld sind:

- Angreifer, die trojanische Pferde einbringen oder mit Schnüffel-Programmen (Sniffer) Paßworte und sensible Daten abhören könnten.
- die Risiken für Vertraulichkeit und Integrität der Information. Entscheidungen, die aufgrund falscher Daten gefällt werden, setzen die Existenz des Unternehmens aufs Spiel. Interne (eigene Mitarbeiter) und externe Angreifer (Hacker, Wettbewerber) könnten versuchen, über die häufig gut dokumentierten Lücken in der Internet-Technologie vorsätzlich Daten zu verändern oder Programme einzuschleusen, die dieses für sie tun (Viren, Würmer). Die Sicherheitsrisiken von Java und Active-X, Programmiersprachen, mit denen Programme entwickelt werden, die auf dem Rechner während der Netzverbindung allerlei nützliche, aber auch gefährliche Abläufe regeln. Im direkten Vergleich ist Java aufgrund einer „Java Virtual Machine“, die direkte Zugriffe auf das Filesystem des ausführenden Computers nicht zuläßt, weniger unsicher, als Active-X.

Besonders gefährdet ist der elektronische Zahlungsverkehr (electronic commerce) – wobei neben den vorsätzlichen Angriffsversuchen die fahrlässigen Falscheingaben und Bedienungsfehler der berechtigten Anwender als Schadenquelle nicht zu unterschätzen sind.

- Werden die wesentlichen betrieblichen Prozesse durch IT-Systeme auf Ba-

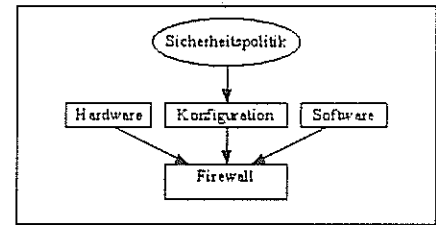
Intranet: Gefahr für Know-how-Schutz

sis des Intranets unterstützt, ist das Unternehmen von der Verfügbarkeit der Systeme und der Daten abhängig. Ein technisch bedingter oder vorsätzlich herbeigeführter Ausfall von entscheidenden Komponenten kann - bei fehlenden Notfallmaßnahmen - Folgen bis hin zum Konkurs haben. Angriffe, die auf das Lahmlegen der Zielsysteme durch Erzeugen einer Überlastung zielen („denial of service-attack“, „flooding“, „bombing“), sind bereits mehrfach vorgekommen.

Schutzmaßnahme Firewall

Wer heute seine unternehmensrelevanten Daten gegenüber den angesprochenen Bedrohungen schützen will, muß diesen Maßnahmen entgegensetzen, zum Beispiel Firewalls, kombinierte Hard- und Software-Lösungen, die den Kommunikationsablauf zwischen internem und externem Netz prüfen und unzulässige Zugriffe abwehren sollen. Doch noch immer werden Firewall-Systeme nur als Sicherheits-Alibi eingekauft. Nicht selten tun sich danach durch eine mangelhafte Administration - nicht durch undurchdachte Lösungen - gravierende Sicherheitslücken auf. Meist wird mit Firewall eine „einfache“ Software assoziiert, die nach der Inbetriebnahme sofort für die nötige Sicherheit sorgt. Doch der Firewall-Ansatz geht über einfache, technische Mechanismen hinaus. Vielmehr handelt es sich dabei um ein Konzept, das zu seiner effektiven Realisierung mehrere Komponenten umfaßt.

Neben der Hardware ist die Software das Kernstück eines Firewall-Konzeptes. Die Konfiguration dieser Software erfordert genaue Kenntnisse über die im Unter-

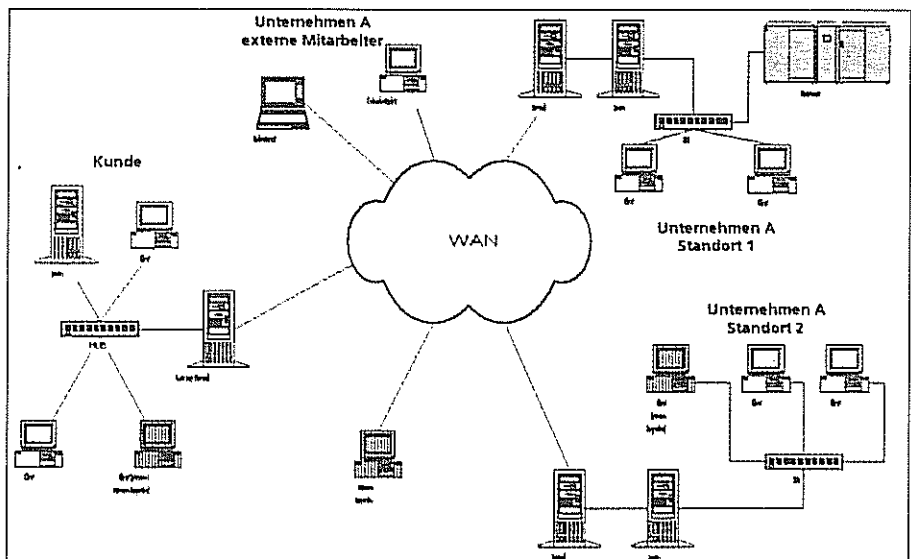


Komponenten eines Firewall-Konzeptes

nehmen verwendeten Dienste und Protokolle. Darüber hinaus sind Kenntnisse über benötigte Virenschutz-Mechanismen, verwendete Applikationen, erforderliche Zugriffsrechte sowie angewandte Verschlüsselungen notwendig. Ein konkretes Beispiel einer möglichen Firewall-Konfiguration zeigt die untenstehende Abbildung.

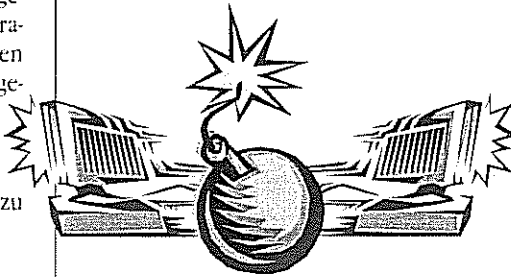
Anhand der Konfigurationsoberfläche sind alle relevanten Informationen auf einen Blick abzulesen. In den fünf Reihen sind für verschiedene Quellen (source) und Ziele (Destination) die erlaubten Dienste (Service) aufgeführt sowie die auszulösenden Aktionen (Action) und die Art der Protokollierung (Track). Die letzte Zeile verdeutlicht die realisierte Sicherheitspolitik: Alles, was nicht explizit erlaubt ist, löst einen Alarm (Alert) aus.

Wie diese Konfiguration im Einzelfall aussieht, muß jedes Unternehmen für sich entscheiden. Dazu bedarf es einer gemeinsamen Plattform, einer unternehmensweiten Sicherheitspolitik, die den Schutzbedarf der einzelnen Informationen definiert und damit die Vorgaben für die Sicherheitseinstellungen liefert. Erst dann lassen sich die Sicherheitsfragen beantworten, die beim Einsatz eines Intranets in Verbindung mit externen Zugriffen entstehen:



Konfigurationsoberfläche am Beispiel des FireWall-1 von Checkpoint.

- Welche Zugriffsrechte sollen die eigenen Mitarbeiter innerhalb des Intranets haben, zum Beispiel auf die Daten anderer Niederlassungen? Die eingerichteten Rechte sollten nicht aus Unkenntnis oder aus diffuser Angst vor einer zu restriktiven, produktivitätsbeschränkenden Einstellung zu großzügig vergeben werden.
- Auf welche Informationen sollen Zugriffe von außen (Außendienst, freie Mitarbeiter) möglich sein? Achtung: Aufgrund der bei Telearbeitsplätzen nicht mehr möglichen Zutrittskontrolle könnten unerwünschte Zugriffe auf externe Arbeitsplatzrechner (Heimarbeitsplätze) oder Notebooks möglich werden.
- Sollen Zugriffe zu allen Tages- und Nachtzeiten erfolgen können? Aber: Was für Zugriffe aus dem Inland eine sinnvolle Einschränkung seien kann, würde bei international arbeitenden Unternehmen Produktivitätseinschränkungen bedeuten.
- Welche Daten müssen verschlüsselt werden, und welche Qualität (Algorithmus, Schlüssellänge) muß verwendet werden? Auch hier kann nur der festgestellte Schutzbedarf Entscheidungskriterium sein. Bei internationalen Verbindungen kommen die landesspezifischen Einschränkungen für Verschlüsselungen hinzu (Beispiel Frankreich, USA), die ggf. durch andere Maßnahmen ergänzt werden müssen.
- Sollen auch die nur intern übertragenen Daten verschlüsselt werden? Bei besonders schützenswerten Informationen (Personaldaten, Geschäftsgeheimnisse, Planungsdaten) muß auch intern über den Schutz der Netzdaten entschieden werden.
- Welche sicherheitsrelevanten Tätigkeiten (Wartung, Administration) können nach außen vergeben werden? Falls externe Dienstleister, beispielsweise ein Internet-Provider, in Anspruch genommen werden, müssen auch hier Vorgaben gemacht werden.



das mangelnde Sicherheitsbewußtsein fehlende Akzeptanz unter den Anwendern trägt dann ihren Teil dazu bei, daß die Sicherheitsmaßnahmen ignoriert oder außer Kraft gesetzt werden. Da sicherheitsrelevante Vorkommnisse wegen des befürchteten Ansehenverlusts in den Unternehmen zumeist verschwiegen werden, kommt es auch nur schwer zu einer Bewußtseinsänderung.

Für alle, die sich mit Know-how-Schutz befassen, stellen diese Probleme eine Herausforderung dar: Durch Kenntnis des Schutzbedarfs der verarbeiteten Informationen und der Umsetzung einer umfassenden, aktuellen Sicherheitspolitik kann aber ein angemessenes Sicherheitsniveau erreicht werden. Auch hier gilt, daß nur ein integriertes und umfassendes, auf die konkrete Unternehmenssituation zugeschnittenes Schutzkonzept funktionieren kann, denn die Gesamtsicherheit ist nur so gut, wie das schwächste Glied in der Kette der Einzelmaßnahmen. In den meisten Fällen muß zur Erarbeitung eines auch die Informationstechnologie einbindenden Sicherheitskonzeptes ein externer Partner hinzugezogen werden, der über das notwendige Know-how verfügt, besonders dann, wenn keine eigene Abteilung für IT-Sicherheit vorhanden ist. ✓

Fazit

Das Intranet wirft eine Reihe zusätzlicher Sicherheitsprobleme gegenüber LANs auf. Ein Hauptproblem von Sicherheitsmaßnahmen ist, daß diese oftmals störend wirken und der gerade gewonnenen Bequemlichkeit entgegenstehen. Die durch