

Die moderne Rechtsanwaltskanzlei

Sicherheit und Datenkommunikation

von Siegfried Streitz

Der neue Mandant möchte den Entwurf über die Auflistung der Zusatzleistungen als Datei schicken, in die unmittelbar die Änderungen aufgenommen werden sollen... Was ist hier für den Anwalt zu beachten? Welche Hard- und Softwareeinrichtungen sind notwendig, um im Internet Informationen zu suchen und zu surfen? Was ist zu tun, um einen Befall des Systems mit Viren zu vermeiden? Wie kann ich einen Schriftsatz in elektronischer Form meinem Kollegen an einem anderen Standort senden? Was ist ein VPN (Virtual Private Network)?

Diese und ähnliche Fragestellungen werden in zunehmendem Maße an die Anwälte herangetragen; in vielen Kanzleien ist es schon selbstverständlich geworden, die Unterlagen in (Beratungs-) Mandaten nur noch in elektronischer Form auszutauschen.

Hierfür ist der Einsatz einer angepassten Infrastruktur erforderlich, die gerade im Hinblick auf die auftretenden Folgekosten sorgfältig geplant werden muss. Der Autor hat im Beitrag Was die EDV wirklich kostet (NJW-CoR 4/99, 231ff.) schon dargelegt, dass der Erstinvestitionsaufwand weniger als 20% der Gesamtkosten beträgt. Entscheidend für die Rentabilität sind somit die Betriebskosten.

Im folgenden wird zunächst dargelegt, welcher Nutzen mit dem Einsatz elektronischer Kommunikationsmedien verbunden ist. Anschließend werden unterschiedliche Lösungskonzepte gegeneinander abgewogen, um die Vor- und Nachteile deutlich zu machen. Die mit den einzelnen Lösungen verbundenen Aufwendungen werden nach einmaligen und laufenden Kosten untergliedert, um eine fundierte Investitionsentscheidung zu ermöglichen.

1. Verbesserungspotential

In elektronischer Form können nicht nur Texte, sondern auch Fotos, Aufstellungen, Skizzen, Kalkulationen usw. über-

mittelt werden. Die gängigen Standard-Anwendungsprogramme können mit vielen dieser Dateiformate umgehen und besitzen eine Reihe von Filtern, damit z. B. auch in einer Textverarbeitung Fotos oder Kalkulationen bearbeitet werden können.

Grundgedanke ist die Arbeitsaufteilung; ein Dokument soll nur einmal elektronisch erstellt und anschließend von mehreren Personen genutzt werden können. Dies erstreckt sich nicht nur auf Korrekturen und Nachbearbeitungen, sondern auch auf die Suche nach Begriffen oder die Wiederverwendung in anderen Unterlagen.

So kann beispielsweise ein Mandant eine Mehraufwands-Aufstellung in elektronischer Form übermitteln, die anschließend vom Anwalt in einen Schriftsatz eingefügt und so nachbearbeitet werden kann, dass nur die für den Rechtsstreit relevanten Spalten im Schriftsatz ausgedruckt werden. Diese Version wird dem Mandanten wieder zurück übermittelt, damit er für die Folgeperioden direkt die gewünschte Darstellungsweise verwendet. Das gleiche Verfahren kommt auch bei der Bearbeitung von Vertragsentwürfen zum Einsatz, bei denen neben den juristischen auch tatsächliche, kaufmännische und technische Gegebenheiten berücksichtigt werden müssen, die in aller Regel dem Anwalt nur teilweise bekannt sind.

Exkurs: Die Vorteile werden deutlich, wenn die elektronische Form mit einer reinen Fax-Vorlage verglichen wird: Hierbei liegen die Dateien nur als Bild vor, das entweder neu erfasst werden muss oder nur mit Hilfe von Montagearbeiten (Ausschneiden, Zusammenetzen/Einfügen) weiter verwendet werden kann. Eine Änderung einzelner Teile ist somit sehr aufwendig; auch bleibt immer deutlich, dass es sich um ein eingescanntes Dokument mit abweichendem Layout und schlechterer Qualität handelt. Diese Nachteile können nur vermieden werden, wenn eine Klarschrifterkennung (OCR - Optical Character Recognition) durchgeführt und das Abbild des Textes wieder in eine Buchstaben-Darstellung überführt wird. Diese Vorgehensweise ist jedoch auf-

wendig, da bei der Klarschrifterkennung Fehler auftreten und eine manuelle Nachbearbeitung der Regelfall ist.

Ein weiterer wesentlicher Aspekt ist der Kostenfaktor: Die Übermittlung einer Information als elektronische Post (E-Mail) kostet nahezu nichts, während bei der Faxübertragung erhebliche, zeitabhängige Telekommunikationskosten anfallen. Auch der Schnelligkeitsfaktor kann bedeutsam sein: Bei der Wahl eines leistungsfähigen Partners für die E-Mail-Kommunikation (ein sog. ISP - Internet Service Provider) ist in den meisten Fällen gewährleistet, dass eine E-Mail nach wenigen Minuten ihren Empfänger erreicht, während eine Faxübertragung von zwei freien Faxgeräten (beim Sender und Empfänger) abhängig ist und für die Übermittlung größerer Dokumente mehr Zeit benötigt. Anschließend ist das Faxdokument wie ein Papierdokument weiter zu behandeln und muss vom Faxgerät weiter verteilt werden.

Demgegenüber kann eine E-Mail-Kommunikation wesentlich direkter sein, da sie bei einer entsprechenden Organisationsstruktur unmittelbar dem Anwalt zugestellt wird. Hier müssen jedoch geeignete Konzepte gewährleisten, dass der Anwalt nicht mit unerwünschter Kommunikation konfrontiert wird.

Nicht zuletzt ist die Erstellung einer E-Mail wesentlich rationeller und effizienter durchzuführen als der Versand eines Telefax, bei dem neben der Anfertigung eines Deckblattes weitere Sekretariatsabläufe wie Ausdruck, Unterschriften, Papiermanagement etc. notwendig sind.

Der Einsatz von elektronischer Kommunikation besitzt somit folgende Vorteile:

- Arbeitsaufteilung
- Bearbeitbarkeit von zugeliferten Informationen
- Wiederverwendbarkeit
- Schnelligkeit
- Erhöhung der Unmittelbarkeit der Kommunikation
- Kostenersparnis

Ein von der E-Mail-Kommunikation

getrennt zu betrachtendes Thema ist das Surfen im Internet, das technisch abweichend realisiert ist und grundsätzlich unabhängig von der E-Mail-Kommunikation ist. Im Abschnitt 3.4 Weitergehende Internetnutzung wird auf die Abgrenzung näher eingegangen.

2. Risiken

Nun gibt es auch Kehrseiten: Der Versand einer E-Mail über das Internet kann am ehesten mit der Übermittlung einer Postkarte verglichen werden. Dabei ist diese Postkarte von nahezu jedermann einsehbar, während bei der Beförderung von Postkarten nur ein besonders verpflichteter Personenkreis die Möglichkeit besitzt, vom Inhalt Kenntnis zu nehmen, bis sie in einen Briefkasten eingeworfen wird. Bei einer E-Mail ist dieser Personenkreis faktisch nicht eingrenzbar, in der Regel ist er nicht besonders verpflichtet und die Einsichtnahme ist mit technischen und maschinellen Maßnahmen vergleichsweise leicht möglich.

Von hier ist der Weg nicht weit zur Erfüllung der subjektiven und objektiven Tatbestandsmerkmale des § 203 StGB (Verletzung von Privatgeheimnissen). Der Anwalt ist gut beraten, entweder eine Einwilligung des Mandanten zu besitzen oder die Informationen besser zu schützen.

Daneben können auch Informationen verändert werden; ein elektronisches Radieren hinterlässt im Gegensatz zu Modifikationen in gebundenen Handelsbüchern keine Spuren.

Ein weiteres Problem besteht darin, dass Dokumente in elektronischer Form

leicht manipuliert werden können, was insbesondere auch die Absenderangabe betrifft. So ist es mit vergleichsweise geringem Aufwand möglich, über die wahre Person des Absenders zu täuschen.

Aus technischer Sicht bedeutet dies, dass folgende Ziele anzustreben sind:

- Vertraulichkeit
- Datenintegrität
- Authentizität

3. Lösungskonzepte

Grundsätzlich bieten sich zwei verschiedene Lösungswege an: Als weniger aufwendige, aber auch nicht so weitreichende Lösung die Verschlüsselung von elektronischen Informationen und als aufwendigere, aber auch wesentlich belastbarere Lösung die Einrichtung sicherer Verbindungen.

3.1 E-Mail-Funktionsweise

Zum besseren Verständnis wird zunächst erläutert, welche Einrichtungen vorliegen müssen und welcher Ablauf bei der Erstellung von E-Mails angewendet wird (s. Abb. 1).

Grundsätzlich wird für den Versand von E-Mails ein Dienstleister benötigt, der als Internet-Service-Provider (ISP) bezeichnet wird. Dieser bietet meist eine ganze Palette von Dienstleistungen an, von denen hier jedoch nur der E-Mail-Versand und -Empfang von Interesse sind. Der Anwalt besitzt mindestens einen PC, der mit einem Modem oder einer ISDN-Karte ausgestattet ist.

Damit wird über das öffentliche Telekommunikationsnetz eine Verbindung mit dem ISP hergestellt. Der ISP selbst ist mit besonders leistungsfähigen Verbindungen an das Internet angeschlossen und empfängt die für den Anwalt bestimmten E-Mails aus dem Internet. Er speichert sie in einem Postfach zwischen, das regelmäßig vom Anwalt geleert wird.

Auf umgekehrte Weise erfolgt der Versand der E-Mails. Der Anwender übermittelt die E-Mails an den ISP, der sie wiederum in das Internet einspeist.

Alternativ/ergänzend besteht dazu auch die Möglichkeit, die Betreffzeilen von E-Mails als sogenannte Kurznachrichten (SMS – Short Message Service) auf einem Handy anzuzeigen zu lassen.

Mittlerweile gibt es einige 100 ISPs in Deutschland, die eine erhebliche Bandbreite hinsichtlich der Qualität und der Ausgestaltung ihrer Dienste aufweisen.

Der wesentliche Kostenfaktor ist der Aufbau der Verbindung vom Anwalt zum ISP, der von einigen ISPs zum Pauschaltarif (ca. 30,00 DM pro Monat) angeboten wird oder alternativ zum (Orts-)Gesprächstarif im Bereich einiger Pfennige pro Minute oder einem anderen zeitabhängigen Tarif erfolgt. Daneben ist auch ein Call-by-Call-Zugriff möglich, der verbindungsweise abrechnet wird.

Bei dem in einer durchschnittlichen Anwaltskanzlei anfallenden E-Mail-Volumen sind die Kosten für den E-Mail-Versand über das Internet meist im pauschalen Endpreis enthalten; falls sie getrennt berechnet werden, dürften hier weniger als 10,00 DM pro Monat anfallen, auch wenn von rund fünf Arbeits-

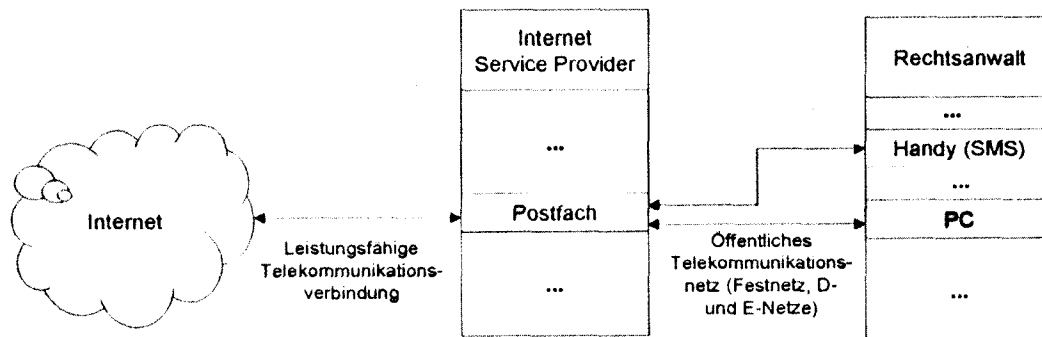


Abbildung 1: EMail-Funktionsprinzip

plätzen aus intensive E-Mail-Kommunikation erfolgt.

Exkurs Technik: Das Standardprotokoll zum Versand ist SMTP, für den Empfang wird häufig POP verwendet. Alternativ ist es auch möglich, die Verbindung zum ISP über einen Router aufzubauen, der für weniger als 1000,00 DM erhältlich ist und eine transparente TCP/IP-Verbindung zum Provider schafft, die weitere Vorteile (z. B. beim Internet-Zugriff/Surfen) aufweist.

3.2 Verschlüsselung

Ein Lösungsansatz zur Verminderung der Risiken besteht nun darin, die Nachrichten zu verschlüsseln. In der Praxis durchgesetzt haben sich asymmetrische Verschlüsselungsverfahren, bei denen zwei Schlüssel, ein privater und ein öffentlicher, verwendet werden. Der öffentliche Schlüssel erlaubt es Dritten, Nachrichten zu verschlüsseln, aber nicht wieder zu entschlüsseln. Mit dem privaten Schlüssel können die verschlüsselten Nachrichten entschlüsselt und lesbar gemacht werden. Zusätzlich kann noch ein Passwort eingesetzt werden, das beim Entschlüsseln eingegeben werden muss.

Bei diesen Verfahren werden die öffentlichen Schlüssel häufig an zentralen Stellen hinterlegt, so dass sie von jedem benutzt werden können. Der private Schlüssel wird hingegen sorgfältig aufbewahrt und nur vom Empfänger der Nachricht verwendet. Ein Nachteil des Verfahrens ist, dass zunächst immer erst der öffentliche Schlüssel von demjenigen benötigt wird, an den die Daten verschlüsselt übermittelt werden sollen (weitere Hinweise finden sich unter <http://www.streitz.de/thema/pgp.htm>).

Beim Anwalt, der eine E-Mail an einen Mandanten versenden möchte, stellt sich dann der Ablauf wie folgt dar (s. Abb. 2):

Zunächst wird mit Hilfe eines E-Mail-Programms (auch E-Mail-Client) eine E-Mail erstellt bzw. eine bestehende E-Mail bearbeitet. Dies erfolgt in der Regel an einem Arbeitsplatz. Anschließend wird diese E-Mail mit dem öffentlichen Schlüssel des Mandanten verschlüsselt, wobei in einem Netzwerk diese Schlüssel zur besseren Verwaltung zentral auf einem Server abgelegt sein sollten. Anschließend wird die E-Mail unmittelbar an den Provider versendet oder – wenn ein Netzwerk vorhanden ist – an ein gesondertes Soft-

wareprogramm, den E-Mail-Server des Anwaltes, übermittelt und von dort aus dem Provider weitergegeben.

Bei dem Empfänger ist dann eine umgekehrte Reihenfolge notwendig, wobei an Stelle des öffentlichen Schlüssels der private Schlüssel, gegebenenfalls ergänzt durch ein Passwort, eingesetzt wird.

Der private Schlüssel wird mit einem besonderen Programm generiert. Der durch eine Verschlüsselung erreichbare Schutz hängt in hohem Maße von dem verwendeten Verschlüsselungsverfahren und der Schlüssellänge ab. Schlüssellängen von 40 oder 56 Bit sind für das DES-Verfahren (Data Encryption Standard) nach dem Stand der Technik

unsicher; es sollte zumindest das Triple-DES-Verfahren mit einer Schlüssellänge von 112 Bit verwendet werden. Allerdings unterliegen amerikanische Hersteller Exportrestriktionen, die bei der Auswahl eines Produktes zu beachten sind.

Beispiele für Verschlüsselungsverfahren sind PGP, SMIME und GnuPG. Die Programmversionen mit grafischer Benutzeroberfläche sind in der Regel kostenpflichtig.

Besondere Sorgfalt muss auf die Auswahl des Programms gelegt werden, mit dem die E-Mails erstellt und verschlüsselt werden sollen (E-Mail-Client). Probleme gibt es hier bei der Integration des Verschlüsselungspro-

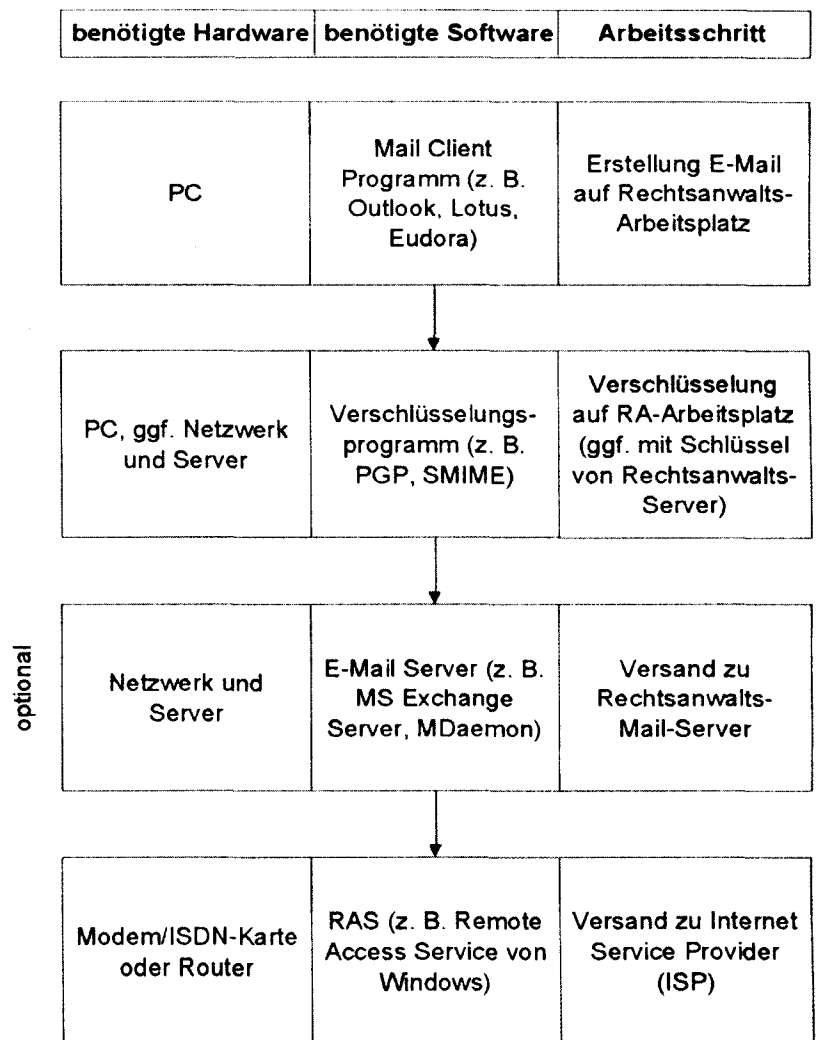


Abbildung 2: EMail-Erstellung und -Versand

gramms in den Client, was z. B. zu Problemen bei der Verschlüsselung von Anhängen oder zusammengesetzten Nachrichten führt. Praxiserfahrungen haben gezeigt, dass die Einrichtung eines derartigen Systems von Laien nicht befriedigend vorgenommen werden kann, da eine Reihe von Seiteneffekten und Randbedingungen zu beachten sind.

Nach der grundsätzlichen Klärung des Ablaufes sollen nun einige weitere wesentliche Bestandteile des Verfahrens betrachtet werden. Zunächst sind die Gestaltung einer E-Mail-Adresse und die Verteilung von E-Mails innerhalb einer Kanzlei von Interesse.

Die preiswerteste Lösung ist eine E-Mail-Adresse in der Form <Ihr Name>@<ISP>, wie sie z. B. mit RAeSchmitz@provider.de lauten könnte. In diesem Fall gibt es eine einzige E-Mail-Adresse, mit der alle E-Mails versandt und empfangen werden. Diese Adresse ist weltweit eindeutig. Zu beachten ist, dass keine Umlaute verwendet werden dürfen.

Die Nachteile werden deutlich, wenn mehrere Personen in einer Kanzlei E-Mails senden und empfangen, da dann zunächst eine manuelle Aufteilung notwendig ist. Dies macht einige Vorteile, insbesondere die Unmittelbarkeit, der E-Mail-Kommunikation zunichte, so dass in diesem Fall mehrere E-Mail-Adressen verwendet werden sollten. Preiswerte Lösungen sind <Kanzleimitarbeiter>@<Kanzleiname>.<Provider> (z. B. Müller@RAeSchmitz.provider.de).

Bei einem Providerwechsel sind jedoch hier in der Regel die E-Mail-Adressbezeichnungen zu ändern, so dass zu erwägen ist, ob nicht eine sogenannte Domäne (Internet-Adresse) der Form RAeSchmitz.de erworben werden soll. Die Kosten hierfür betragen ca. einmalig 50,00 DM für die Einrichtung und 30,00 DM pro Jahr an laufenden Kosten. In diesem Fall erhält der Anwalt alle E-Mails mit der Adressierung <beliebige Person>@RAeSchmitz.de.

Hieraus ergibt sich jedoch unmittelbar eine weitere Entscheidung: Die E-Mails sind auf die einzelnen Empfänger zu verteilen. Dies kann beim Provider geschehen, indem für jeden Benutzer ein getrenntes Postfach eingerichtet wird. Diese können von den Benutzern gesondert abgefragt werden, so dass auf der Anwaltsseite kein zusätzliches Programm (E-Mail-Server) notwendig ist; Nachteile sind jedoch erhöhte Kommu-

nikationskosten zum Provider und Probleme bei Vertretungsregelungen.

Die komfortablere Lösung ist die Einrichtung eines E-Mail-Servers beim Anwalt, so dass alle E-Mails des Postfaches beim Server abgerufen und durch den E-Mail-Server beim Anwalt automatisch verteilt werden. Dies hat den weiteren Vorteil, dass interne E-Mails innerhalb der Kanzlei nicht über den ISP laufen müssen, sondern unmittelbar vom E-Mail-Server verteilt werden können.

Die Kosten für einen E-Mail-Server betragen – abhängig von Benutzerzahl, Hersteller und Leistungsumfang – zwischen 0,00 DM und einigen 1.000,00 DM.

Zur besseren Übersicht werden in der Tabelle 1 noch einmal die Kosten für diese Lösung zusammengestellt, wobei die Existenz eines lokalen Netzwerkes (sog. LAN) beim Anwalt unterstellt wird.

Der laufende Betreuungsaufwand ist relativ gering, wenn ein geeigneter E-Mail-Server eingesetzt wird und ein oder zwei Personen mit der Benutzerverwaltung vertraut sind. Hauptprobleme sind eher die Integration der Verschlüsselungssoftware in den E-Mail-Client, die jedoch nach Überwindung von Anfangsschwierigkeiten im Regelfall stabil abläuft, so dass nur gelegentlich eine Systeminspektion vorgenommen werden muss.

3.3 Sichere Verbindung

Bei einer intensiveren Zusammenarbeit, wie sie bei verschiedenen Standorten einer Anwaltskanzlei vorliegen kann, wird eine E-Mail-Lösung häufig zu

schwach. Wenn z. B. mehrere Benutzer mit einem Anwaltsprogramm arbeiten wollen, Adressbücher standortübergreifend verfügbar sein müssen oder auch bestimmte Dokumente in anderen Standorten abrufbar sein sollen, ist eine Verbindung der Netzwerke zwischen den einzelnen Standorten notwendig (sog. LAN-zu-LAN-Kopplung). Bereits in NJW-CoR 6/98, 340ff. wurden hier verschiedene Lösungsansätze vorgestellt: Die einfachste Form sind Stand- oder Wählverbindungen über das öffentliche Telekommunikationsnetz, die z. B. mit Hilfe des Remote Access Service (RAS), der in Microsoft Windows enthalten ist, realisiert werden können. Diese Verbindungen haben relativ hohe Telekommunikationskosten und sind darüber hinaus nicht übermäßig abhörsicher.

Die Telekommunikationskosten können zwar durch die Verwendung von sog. Least Cost Routern (LCR) vermindert werden, die jeweils den günstigsten Provider auswählen. Bei einer intensiveren Zusammenarbeit fallen jedoch hier erhebliche Kosten an, die durch den Einsatz der nachfolgend vorgestellten Lösung vermindert werden können.

Die Kopplung der lokalen Netzwerke kann auch über das Internet vorgenommen werden, wie aus Abb. 3 hervorgeht. Die Kommunikationsstellen der einzelnen LANs nach außen werden hierbei mit besonderen Einrichtungen versehen, um eine sichere Verbindung über das Internet zu gewährleisten.

Derzeit sind hier zwei grundsätzlich zu unterscheidende Konzepte im Einsatz, die hier unter Verzicht auf technische Details erwähnt werden sollen: Auf einer unteren logischen Ebene der Datenkommunikation (Exkurs für Tech-

Komponente	Einmalige Kosten	Laufende Kosten pro Monat
Router	1.000,00 DM	
ISDN-Karte/Modem	300,00 DM	
Mail-Server (10 Teiln.)	500,00 DM	
Verschlüsselungssoftware	300,00 DM pro Arbeitsplatz	
Einrichtung	1 Stunde pro Rechner	
E-Mail-Client	0,00 DM	
E-Mail-Kommunikationskosten		50,00 DM
E-Mail-Adresse	50,00 DM	30,00 DM
Laufende Betreuung		150,00 DM

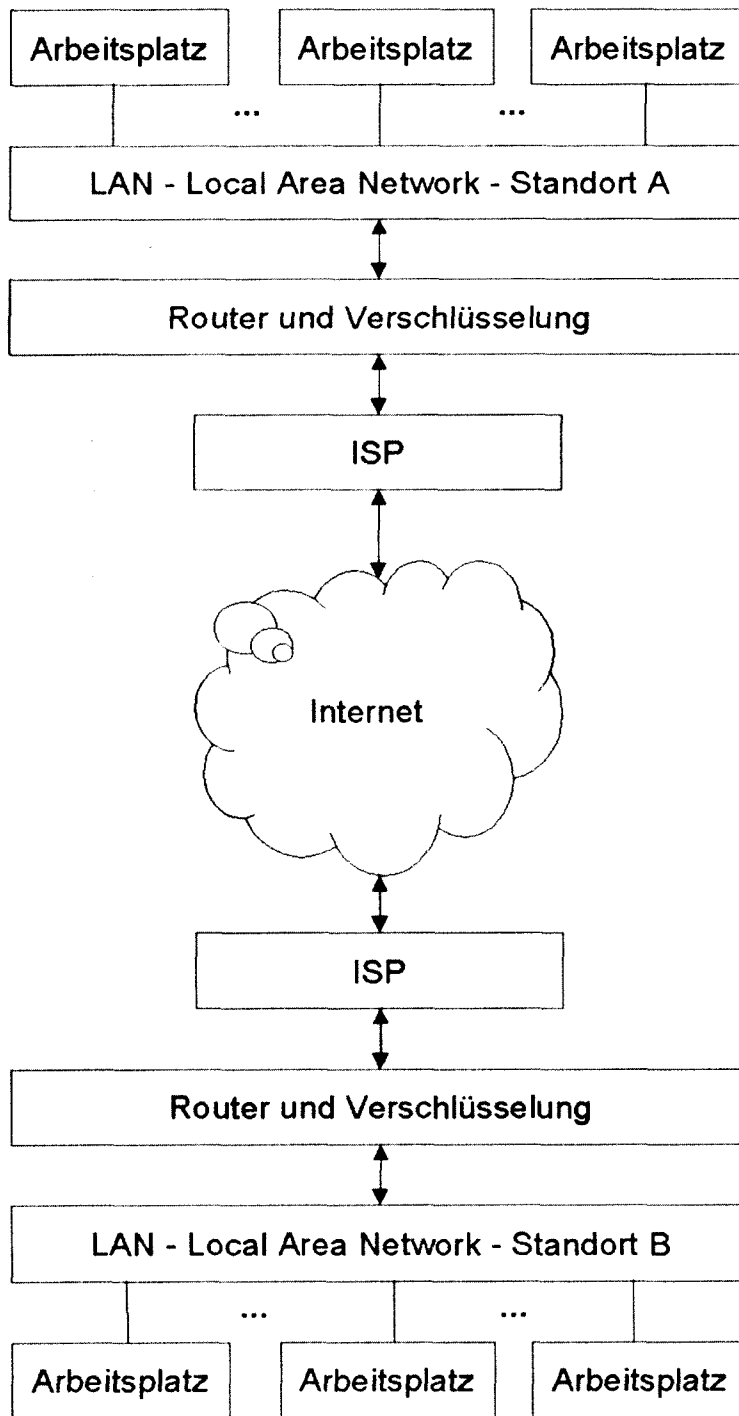


Abbildung 3: VPN (Virtual Private Network)

niker: Ebene 2 des OSI-Schichtenmodells) gibt es die Protokolle PPTP (Point to Point tunneling Protocol) des Herstellers Microsoft und das L2TP (Layer 2 Tunneling Protocol). Nachteile des ersten Verfahrens sind eine Reihe von Sicherheitslücken, die zwischenzeitlich zu Tage getreten sind; das zweite Verfahren ist nicht ausreichend standardisiert. Ferner ist der Schutz gegen Manipulationen nur relativ schwach ausgeprägt.

Alternativ gibt es auf einer höheren Ebene (Ebene 3 des OSI-Schichtenmodells) den Standardisierungsvorschlag IPSec, der sich jedoch mit sehr hoher Wahrscheinlichkeit im Rahmen der neuen Internetstandardisierung IPv6 durchsetzen wird, da der gegenwärtige Mangel an IP-Adressen eine Fortschreibung des derzeitigen Standards zwingend notwendig macht.

Es ist jedoch zu beachten, dass die Produkte, die mit IPSec arbeiten, nicht unbedingt miteinander verträglich sind, da unterschiedliche Verschlüsselungsverfahren verwendet werden. Wesentliche Voraussetzung ist die Verwendung einer festen IP-Adresse, damit die Adressierung feststeht; ein normaler Internetzugang hat in der Regel eine dynamische IP-Adresse, die für eine Sitzung zugewiesen wird und sich bei jeder Sitzung verändert. Diese sind aufgrund von Adressierungsproblemen derzeit nur mit Spezialhardware verwendbar, was für den Anwalt in der Regel nicht in Betracht kommt.

Für eine reine LAN-zu-LAN-Kopplung reicht es aus, an den Schnittstellen des LANs zum Internet jeweils einen Router vorzusehen, der eine Verschlüsselung übernimmt und die Adressierung für den anderen Partner sicher stellt (s. Abb. 3). Weitere Dienste brauchen nicht verwendet zu werden, so dass hier auch die laufende Betreuung keinen wesentlichen Aufwand verursacht.

Die Kosten können wie in Tabelle 2 auf der nächsten Seite zusammengestellt werden.

Mit dieser Einrichtung hat man ein sog. VPN (Virtual Private Network) geschaffen, das ein privates Netz im öffentlichen Internet darstellt.

3.4 Weitergehende Internetnutzung

Für die Beschaffung von Informationen im Internet („Surfen“), ist die Benutzung des HTTP-Dienstes (Hyper Text Transfer Protocol) notwendig. Eine ein-

Tabelle 2

Komponenten	Kosten einmalig	Kosten pro Monat
Feste IP	100,00 DM	100,00 DM
Internet Access (für 10 Arbeitsplätze)		100,00 DM
Router mit Verschlüsselungstechnik	Ab 2.000,00 DM	

Firewall-Lösungen sind z. B. für das Betriebssystem LINUX kostenlos erhältlich. Für andere Betriebssysteme sind Firewalls ab ca. 2.000,00 DM verfügbar; für qualitativ hochwertige Produkte sind jedoch eher 10.000,00 DM aufzuwenden. Wichtig ist eine regelmäßige (mindestens zweiwöchentliche) Analyse der Protokolle, um Unregelmäßigkeiten zu entdecken und neu gewonnene Kenntnisse umzusetzen. Die

fache Lösung ist hier die Bereitstellung eines gesonderten Internet-Rechners, der nicht mit dem LAN verbunden ist. Falls hier Probleme auftreten (z. B. Virenbefall), kann der Rechner mit Hilfe einer Sicherungskopie leicht neu installiert werden. Nachteile sind, dass die aus dem Internet gewonnenen Informationen nicht weiter bearbeitet werden können und die Integration in das LAN nicht vorhanden ist.

Dies ist insbesondere bei dienstleistungsorientierten Berufen ein schwerwiegender Nachteil, während bei einem Maschinenhersteller dieser Weg eher beschritten werden kann, da für den Kerngeschäftsbetrieb ein Internetzugang in der Regel nicht notwendig ist. Bei informationsbedürftigen Berufen ist er in vielen Fällen schon unverzichtbar bzw. wird dies in naher Zukunft werden.

In diesen Fällen ist an den Schnittstellen zum Internet eine zusätzliche Komponente, nämlich ein sog. Firewall einzurichten, die Zugriffe von Dritten verhindern soll und in vielen Fällen dabei gleichzeitig weitere Funktionen ausübt (s. Abb. 4).

Die Firewall analysiert den Datenverkehr und weist unerwünschte Daten ab. Darüber hinaus kann sie in vielen Fällen Viren erkennen und ebenfalls abweisen. Die Firewall dient somit dazu, das Internet von dem privaten Netz zu trennen.

Eine Firewall ist nur so gut, wie sie konfiguriert wurde; mit einer schlechten oder fehlerhaften Konfiguration bietet sie faktisch keinen Schutz. Daher ist unbedingt darauf zu achten, dass die Konfiguration von seriösen und erfahrenen Unternehmen vorgenommen wird.

Zu berücksichtigen ist, dass ein gesamtes VPN nur so stark ist wie das schwächste Glied im gesamten Netz. Falls z. B. neben der Firewall noch weitere Internetzugänge existieren (z. B. für die Buchhaltung oder die Personalverwaltung), die nicht über eine gleichwertige Firewall abgesichert sind, wird der Schutz des gesamten Netzes in Frage gestellt.

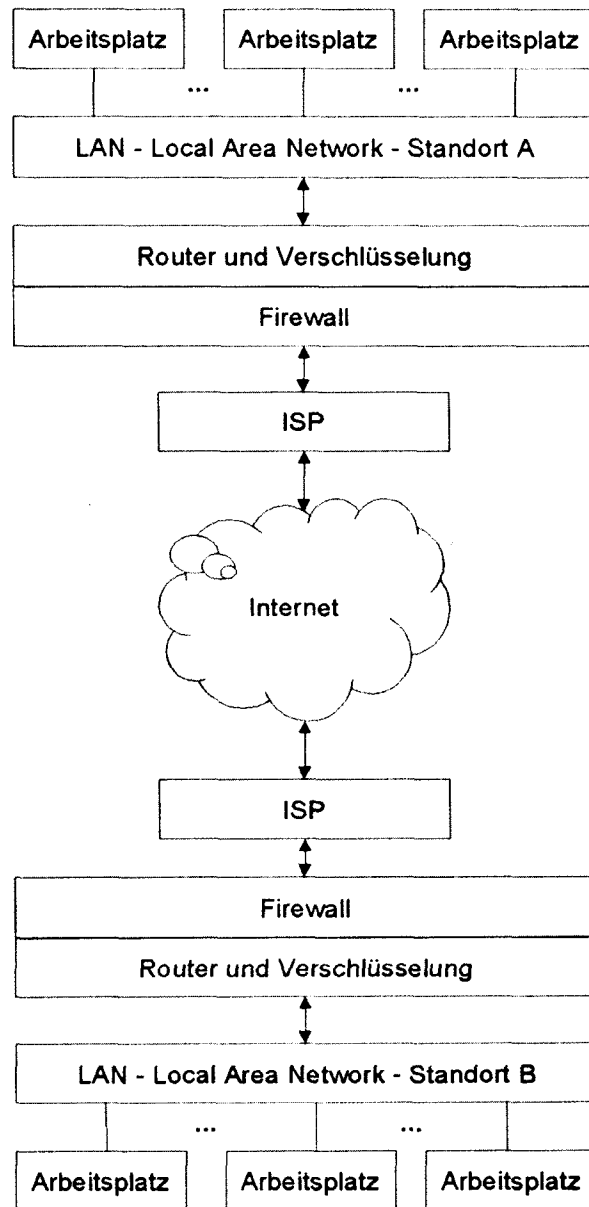


Abbildung 4: VPN (Virtual Private Network) mit durch Firewall geschütztem Internetzugang

gesamte Entwicklung ist hier sehr dynamisch; es vergeht nahezu kein Tag, ohne dass hier eine neue Sicherheitslücke oder ein Sicherheitsproblem zu Tage tritt.

Die Kosten für die Datenkommunikation über das Internet betragen für ein Zehn-Platz-System bei durchschnittlicher Nutzung grob 100,00 DM pro Monat; für den Zugang zum Internet-Service-Provider, der den Internetzugang bereit stellt, treffen die oben genannten Werte für die Verschlüsselungs-Methode zu: sie reichen von einem Pauschal tariff von 30,00 DM pro Monat bis hin zu zeitabhängigen Gebühren im Bereich einiger Pfennige pro Minute.

4. Probleme

Wie bei fast allen IT-Lösungen ist es mit der Einführung einiger Komponenten nicht getan; für einen effizienten und reibungslosen Betrieb sind eine Reihe weiterer Punkte zu berücksichtigen.

4.1 Organisatorische Regelungen

Hierzu gehören Konzepte und Verfahren, die auch beim Einsatz von PC-Systemen beachtet werden sollten. Beispielfhaft werden genannt:

- Ausreichende Dokumentation der tatsächlich installierten Lösung
- Datensicherung (insbesondere der konfigurierbaren Komponenten wie Firewall und Router)
- Regelungen von Verantwortlichkeiten
- Ergänzung der Benutzerrichtlinie um E-Mail- und Internet-Kapitel
- Umgang mit Daten (insbesondere der aus dem Internet gezogenen)
- Virenschutz
- Passwortwahl und regelmäßiger Passwortwechsel
- Fehlermeldeverfahren
- Schulung und Einführung
- Kontrollen
- Zugang zu Systemen

4.2 Gemeinsames Adressbuch

Die mangelhafte Integration der Anwaltssoftwarepakete in die E-Mail-Kommunikation führt in vielen Fällen dazu, dass getrennte Adressbestände verwaltet werden: Einmal im Anwaltsystem für die papiergebundene Kommunikation und einmal im E-Mail-Sy-

stem (vorzugsweise auf dem Server) für die E-Mail-Kommunikation. Ein Verbesserungsansatz ist hier die Verwendung eines gemeinsamen Adressbuches, die nicht notwendig im E-Mail-Server erfolgen muss. Es gibt auch getrennte Produkte wie z. B. denkom global address book.

4.3 Verfügbarkeit

Hier ist zunächst die zentrale Frage zu klären, welche maximale Ausfallzeit für den Zugang zum Internet und/oder zum VPN einzuhalten ist. Bei der Konzeption eines Systems, das diese Anforderung erfüllt, sind folgende Bereiche zu berücksichtigen:

- Hardwarekomponenten (Router, Firewall, andere aktive Netzwerkkomponenten)
- Betriebssysteme (für LAN-Server, Firewall etc.)
- Anwendungssoftware
- Organisatorische Regelungen

4.4 Datenmanagement

Zur (qualitätssichernden) Dokumentation von Abläufen ist es notwendig, dass der Versand und der Empfang von E-Mails dokumentiert bzw. protokolliert werden. Hierzu bieten die meisten E-Mail-Server und -Clients Lösungen an, die aber nicht oder nur sehr rudimentär in Anwaltssoftwarelösungen integriert sind. Hier sind organisatorische Konzepte zur Ergänzung aufzustellen, die

Testvorhaben

Derzeit ist in der Redaktion das Produkt ConNet plus Modell 2 mit Zusatzkomponenten der ConWare Netzpartner GmbH aus Karlsruhe im Test. Es realisiert die oben beschriebene Lösung einer sicheren Kommunikation über das Internet mit Hilfe des IPSec-Standards. Der erste Eindruck zeigte eine wohl-durchdachte, vorbildlich dokumentierte Lösung. Die sehr technisch orientierte Dokumentation wird durch eine komfortable Menüführung zur Konfiguration ergänzt.

Allerdings sind für die Einrichtung verteilte TCP/IP Kenntnisse notwendig, die bei einem durchschnittlichen Endanwender nicht vorhanden sind. Der Testbericht wird sich daher auf die Praxiseignung des Einsatzes in Anwaltskanzleien und die Integration mit bestehenden Systemen konzentrieren.

Von der BinTec Communications AG wurde ein vergleichbares Produkt X1000 angefordert, das bereits auf der CEBIT vorgestellt wurde. Es ist jedoch derzeit noch nicht am Markt verfügbar; NJW-CoR wird auch hier am Ball bleiben.

eine Struktur in der Verwaltung und Dokumentation der durchgeführten Kommunikationsabläufe einführen.

4.5 Systemverwaltung

Die Wirksamkeit einer Firewall hängt neben der Einrichtung entscheidend davon ab, in welchem Umfang neue Erkenntnisse umgesetzt werden. Hierzu gehören bekannt gewordene Sicherheitslücken und eine zeitnahe Analyse der Kommunikationsvorgänge. Das Eindringen in fremde Netze ist zu einem weit verbreiteten Betätigungsfeld bestimmter Personen geworden und lässt sich an Protokollen erkennen. Es ist davon auszugehen, dass auch bei kleineren Netzen mehrere Angriffe im Monat auftreten werden.

4.6 Sicherheitscheck

Daher ist eine regelmäßige Überprüfung des Systems durch fachkundige Personen ein unabdingbarer Bestandteil des Betriebes. Zur weiteren Validierung der Systembetreuung kann auch eine Sicherheitsüberprüfung durch ein darauf spezialisiertes Unternehmen durchgeführt werden, damit Pannen und Katastrophenszenarien vermieden werden.

4.7 Heimarbeitsplätze

Eine Untervariante ist die Einbindung eines Heimarbeitsplatzes über das Internet an das Kanzlei-LAN. In diesem Fall ist für den Heimarbeitsplatz nicht unbedingt eine getrennte Firewall vorzusehen; es gibt hier auch Softwareverfahren mit einer dynamischen IP-Adresse, die die Firewall des Kanzlei-LANs adressieren.

5. Ausblick

Weitergehende Informationen, die sich insbesondere mit den verschiedenen Verknüpfungsmöglichkeiten von Kanzlei-Standorten auseinandersetzen, finden sich im Internet unter www.rechtssoftware.de. Neben unterschiedlichen Konzepten wird hier auch die Auswirkungen auf die Anwendungssoftware (wie z. B. Kollisionsprüfung, Realisierung einer zentralen Datenbank) behandelt.