Sichere Nutzung des Internet

Empfehlungen der Notarnet GmbH

Notarnet GmbH

Burgmauer 53

50667 Köln

Tel.: 0221-257 52 01

Fax: 0221-25 68 08

E-Mail: info@notarnet.de

Stand: 11. März 2004

Inhaltsverzeichnis

1. Einleitung

Das Internet gehört im Notariat – wie in vielen anderen Berufen – mittlerweile zu den standardmäßig eingesetzten Arbeitsmitteln. Der Versand von E-Mails als Kommunikationsmittel mit den Beteiligten hat dabei sicherlich die größte Bedeutung, zunehmend rückt jedoch auch die Informationsrecherche in den Vordergrund. Hier sind sowohl das fachliche als auch das allgemeine Angebot in den letzten Jahren so gewachsen, dass der Webbrowser zu einer echten Arbeitshilfe geworden ist.

Hacker-Angriffe bedrohen EDV-Anlagen

Jeder, der sich mit dem Thema „Computer und Internet“ auch nur oberflächlich beschäftigt hat, ist mit Fragen und Problemen zur Sicherheit des Mediums konfrontiert worden. Nachrichten über Viren und Hacker-Angriffe, katastrophale Geschichten vom Versagen wichtiger EDV-Einrichtungen und von unwiederbringlichen Datenverluste haben allseits für Sensibilität gesorgt. Der eine oder andere wird die Folgen dieser Probleme bereits am eigenen Leib erfahren haben.

Gerade in mittelständischen Organisationsstrukturen, wie sie auch in den meisten Notariaten vorzufinden sind, können diese Risiken beherrscht werden. Dabei ist zunächst bei der Sicherheitsplanung das notwendige Augenmaß zu wahren, d.h. die Wahrscheinlichkeit eines Angriffes und der potentielle Schaden zu bewerten. Sowenig wie der Notar seine Büroräume in einen Hochsicherheitstrakt verwandelt, sowenig sind Schutzeinrichtungen in Industriestärke für seine Datenverarbeitung vonnöten – auch wenn diese ihm gerne verkauft werden.

Notaramt erfordert verantwortungsvollen Umgang mit EDV-Anlage

Auf der anderen Seite sind aber auch die erhöhten Anforderungen zu beachten, die aus der mit dem öffentlichen Amt verbundenen besonderen Vertrauensstellung und der gesetzlichen Verschwiegenheitspflicht resultieren. So ist

das Ausspähen und Bekanntwerden großer Mengen von Urkunds- und Personendaten eine gravierende Belastung nicht nur für den betroffenen Notar, sondern für die Wahrnehmung des gesamten Berufsstandes.

Orientiert an diesen Punkten muss der Notar einen vernünftigen Weg finden, seine Daten adäquat vor Gefahren zu schützen, die aus der Nutzung des Internet resultieren.

Dieses Dokument soll dem Notar eine Hilfestellung an die Hand geben, damit er die Gefährdungen, die aus seiner konkreten Internet-Nutzung entstehen, einschätzen und geeignete Maßnahmen ergreifen kann, die unter Berücksichtigung eines angemessenen Kosten-Nutzen-Verhältnisses einen zweckmäßigen Schutz ermöglichen.

2. EDV-Sicherheit als andauernder Prozess

Wettlauf zwischen Angreifern und Produktherstellern/Nutzern

Entscheidend für das Verständnis „guter“ Datensicherheit ist die Einsicht, dass es niemals damit getan ist, einmalig ein Produkt anzuschaffen oder eine Software zu installieren und sich dann auf der sicheren Seite zu fühlen. Computersicherheit ist ein andauernder Prozess, der sich am ehesten mit einem Wettlauf zwischen Angreifern auf der einen und den Herstellern von Anwendungssoftware und Sicherheitseinrichtungen (und damit natürlich deren Nutzern) auf der anderen Seite vergleichen lässt. Die über die ganze Welt verteilten Angreifer suchen unentwegt nach neuen Schlupflöchern oder Systemschwächen, die sich ausnutzen lassen, um Unheil zu stiften. Die Angreifertypen variieren dabei vom meist jugendlichen Hacker, dem es ohne erkennbaren Eigennutzen – ähnlich einem virtuellen Hooligan – vorrangig um die Erzeugung von Datenchaos in verschiedensten Formen geht, bis hin zum professionellen Industriespion, der unter erheblichem Ressourceneinsatz gezielt Daten ausspäht oder unbrauchbar macht.

EDV-Sicherheit muss fortwährend überprüft und aktualisiert werden

Darum ist es notwendig, die getroffenen Maßnahmen turnusmäßig darauf zu überprüfen, ob sie gegenüber den Risiken, auf deren Beherrschung sie abzielen, noch aus-

reichend wirksam sind. Gleichfalls sollte man einen Weg finden, neue Entwicklungen im Auge zu behalten, deren Risiken nicht mehr von den bestehenden Schutzmaßnahmen umfasst werden (dazu im Einzelnen unten).

3. Der „menschliche Faktor“ – ausschlaggebend für verlässliche Sicherheit

Eine weitere zentrale Weisheit der EDV-Sicherheit ist, dass die besten technischen Schutzmaßnahmen nichts helfen, wenn die Anwender fahrlässig oder mutwillig durch ihr Verhalten Sicherheitslücken schaffen. Dies ist ein ernsthaftes Problem, da Sicherheitsmaßnahmen oftmals konträr zur Bequemlichkeit der Anwender und der Benutzerfreundlichkeit der Programme wirken. Das beste Beispiel ist der Umgang mit Passwörtern: Aus Sicherheitsperspektive ist es empfehlenswert, bei jedem Zugriff auf geschützte Funktionen das Passwort erneut abzufragen, sichere (und damit in der Regel kompliziertere und längere) Passwörter zu benutzen und diese regelmäßig zu wechseln. In der Praxis neigt der Anwender dazu, ein einfaches Passwort (z.B. Nachname, Geburtsdatum, Name des Haustieres) zu wählen, es nicht zu wechseln und es zur besseren Erinnerung aufzuschreiben oder von der Anwendung speichern zu lassen – sämtlich Verhaltensweisen, die im täglichen Arbeitsumfeld verständlich erscheinen mögen. Sie erlauben es jedoch einem einigermaßen kompetenten Angreifer, ein solches Passwort in kurzer Zeit zu „knacken“. Ein anderes bekanntes Beispiel ist die von einem Mitarbeiter von zuhause mitgebrachte virenverseuchte Diskette.

Mitarbeiter müssen für EDV-Sicherheit sensibilisiert werden

Darum ist es von großer Bedeutung, neben den nachfolgend detaillierten technischen Sicherheitsmaßnahmen auch die Mitarbeiter, die EDV und Internet nutzen, für die Sicherheitsrisiken zu sensibilisieren und entsprechend zu schulen. Empfehlenswert ist darüber hinaus, Regeln für den Umgang mit EDV und Internet schriftlich niederzule-

gen, diese den Mitarbeitern nahezubringen und deren Einhaltung konsequent durchzusetzen.[1]

4. Szenarien für den Internetanschluss im Notarbüro

Ausgangspunkt für die Darstellung sollen die klassischen derzeit in Notarbüros anzutreffenden Zugangsszenarien sein.

a. Der Einzelplatz-PC

Vom Büronetz getrennter Einzelplatzrechner bietet brauchbares Schutzniveau, wenn weitere Regeln beachtet werden

Die Installation des Internet-Zugangs (oft über einen „Volks-Provider“ wie T-Online oder AOL) auf einem einzelnen Rechner, der im übrigen nicht physisch mit dem Büronetzwerk verbunden ist, ist typischerweise in kleineren Büros anzutreffen und auch bei sicherheitsbewussteren Kollegen verbreitet. Hier kann „gesurft“ werden, ohne die Kanzleidaten im Netzwerk unmittelbar zu gefährden. Der Empfang und Versand von E-Mails an einem derartigen Rechner (oft unter Nutzung der vom Internet-Provider angebotenen Schnittstelle) ist weitgehend unkritisch.[2]

---

[1] Eine wertvolle Informationsquelle zum Thema „Sicherheit von IT-Anlagen“ ist das „IT-Grundschutzhandbuch“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Es ist als elektronische Fassung kostenlos unter http://www.bsi.bund.de/gshb/ erhältlich, kann aber auch als Loseblattausgabe bezogen werden. Vgl. zu diesem Problemkreis Kap. 3.2 (Personal). Auf der BSI-CD (Bezugsquelle: http://www.bsi.bund.de/gshb/deutsch/aktuell/bezug.htm) finden sich in der Rubrik „Hilfsmittel“ auch Beispiele für Dienstanweisungen und Merkblätter.

[2] Es ist absehbar, dass diese schlichte Anbindung den modernen elektronischen Kommunikationsformen schon bald nicht mehr gerecht wird. Mit der zunehmenden Zahl der Anwendungen wächst die Attraktivität eines Internet-Zugangs am Arbeitsplatzrechner. Die Möglichkeit, mit einzelnen Sachbearbeitern über gesonderte E-Mail Adressen zu kommunizieren, kann für die Aus-

Diese Lösung bietet jedoch keine abschließende Sicherheit und passt aufgrund der beschränkten Einsetzbarkeit zunehmend nicht mehr in den modernen Bürobetrieb. Der Austausch von Vertragsentwürfen ist vielfach eine der Primäranwendungen für E-Mail im Notariat. Zur Speicherung und Weiterverarbeitung müssen die Daten jedoch zunächst ins Netzwerk überspielt werden. Das geschieht in der Regel auf dem unhandlichen Umweg über eine Diskette (oder moderner: einen USB-Speicherstick). Auf diesem Übertragungsweg lassen sich jedoch auch Viren übertragen, insbesondere sog. „Bootsektorviren“[3] oder „Makroviren“[4]. Darum ist es notwendig, zumindest auf dem Internet-PC einen aktuellen Virenscanner (Überwachungsprogramm, dass den Rechnerbetrieb auf das Auftreten bekannter Schadprogramme überwacht und vor diesen schützt) zu unterhalten. Besser ist es, wenn das Netzwerk selbst auch entweder zentral oder an der betreffenden Arbeitsstation vor Virenbefall geschützt ist. Es darf keine Datei in das Netzwerk übertragen werden,

---

sendarstellung positiv wirken und die gezielte Bearbeitung der Vorgänge beschleunigen. Entscheidend ist aber wohl das absehbare Zusammenwachsen der Bürosoftware mit dem Internet-Datenaustausch. So könnten die Grundbuchdaten in für die Urkunde verwertbarer Form unmittelbar vom Grundbuch-Server abgefragt und in die interne Datenbank eingepflegt werden. Umgekehrt kann die Bürosoftware Meldungen wie z.B. die Veräußerungsanzeige oder (schon jetzt) die elektronische Meldung an das Vorsorgeregister generieren und verschicken, ohne dass zusätzlicher Aufwand entsteht. Übertragungsfehler werden so gleichfalls minimiert.

[3] Computerviren, die sich auf Wechselmedien (z.B. Disketten, CD-ROMs, etc.) verbergen und aktiv werden, sobald das Medium eingelegt wird.

[4] Schadprogramme, die in Dokumentdateien (z.B. MS-Word- oder MS-Excel-Dokumenten) enthalten sind und je nach Programmeinstellung beim Öffnen des Dokuments ausgeführt werden.

die nicht von einem aktuellen Virenscanner untersucht worden ist.

Keine Anbindung des Internet-Rechners an das Büronetz ohne geeignete Sicherheitsmaßnahmen

Leider die gefährlichste Lösung ist die bequeme „kleine“ Anbindung des Internet-Zugangsrechners an das Notariatsnetz, bei der Dateien ohne den Umweg über Disketten etc. im Netzwerk verfügbar gemacht werden können – ohne dass andere Arbeitsstationen unmittelbaren Zugriff auf das Internet hätten. Der normalerweise mit der Einzelplatzlösung verbundene Sicherheitsgewinn ist hier lediglich Illusion. Auch der Umstand, dass keine dauerhafte Verbindung mit dem Internet besteht, sondern nur bei Bedarf aufgebaut wird (Modem- oder ISDN-Lösung) hilft nicht weiter, da es genug Methoden gibt, auch solche Verbindungen für Angriffe zu Nutzen, z.B. indem der Zugang ohne Wissen des Anwenders automatisch wieder hergestellt wird.

b. Der Netzwerk-Anschluss

Anschluss des Kanzleinetzwerkes als zukunftssichere Alternative

Die Option, das Kanzleinetzwerk über einen Router[5] oder ein ähnliches geeignetes Gerät an das Internet anzuschließen, lässt grundsätzlich den Rundum-Einsatz aller Aspekte der Internet-Kommunikation zu, öffnet auf der anderen Seite aber potentiell das gesamte interne Netz und alle dort aktuell verfügbaren Daten für Angreifer aus dem Internet. Dieser Anschlusstyp kann vor dem Hintergrund der Verschwiegenheitspflicht des Notars und den mit dem Betrieb der EDV verbundenen Sorgfaltspflichten nur empfohlen werden, wenn gleichzeitig ein wirksames Sicherheitskonzept umgesetzt wird. Hierzu gehö-

[5] Gerät, das den Internetzugang für verschiedene Rechner innerhalb eines geschlossenen Netzwerks vermittelt.

ren die später noch näher beschriebenen Sicherheitsmaßnahmen auf Netz- und Serverebene sowie an den einzelnen Arbeitsplatzrechnern. So genannte „Router“ oder „Proxies“, die den technischen Anschluss einer Mehrzahl von Rechnern an einen Internetzugang erlaubt, sind hier keinesfalls ausreichend. Notwendig ist als weitere Schutzmaßnahme ein als „Firewall“ bekanntes Gerät, das jedoch auch seinen Zweck nur erfüllen kann, wenn die Sicherheitseinstellungen fachmännisch und sorgfältig konfiguriert sind.

WLAN (Funknetzwerk) für Notarbüros derzeit zu unsicher

Nach derzeitigem Stand der Technik ist zumindest für den Notariatsbereich dringend von der Verwendung drahtloser Netzwerktechnik[6] abzuraten. Selbst bei Nutzung der in die Technik integrierten Sicherheitsmechanismen kann der Datenverkehr relativ leicht abgehört werden. Ein Angreifer kann sich unter Umgehung der mit dem Internet-Angriff verbundenen Schwierigkeiten sofort als „Insider“ in das Netz hängen. Er kann Datenverkehr abhören und Netzwerkdaten aktiv ausspähen und hat dafür einen erheblich höheren Datendurchsatz zur Verfügung.

Während dem Netzwerkzugang aufgrund seiner vielfältigen Einsatzmöglichkeiten sicherlich die Zukunft gehört, bringt er für den Notar die volle Breite der Sicherheitsprobleme der Internetnutzung, die er in adäquater Weise angehen muss.

c. Heimarbeitsplätze

Nicht notwendig Internet-Nutzung im engeren Sinne, gehört die Nutzung von Datenfernübertragungstechniken zur Anbindung von Heimar-

---

[6] WLAN=“Wireless Local Area Network“, übliche Standards: IEEE 802.11b,11a oder 11g

beitsplätzen an das Kanzleinetz auch zu den Gesichtspunkten, die bei der Sicherheitsbetrachtung einzubeziehen sind.

Die technische Anbindung über eine unmittelbare Einwahlmöglichkeit (ISDN oder Modem im Notarbüro) bringt dabei grundsätzlich das Risiko mit sich, dass ein Unbefugter versucht, sich über diesen Weg privilegierten Zugang zu den Kanzleidaten zu verschaffen. Hier sind in Abstimmung mit dem technischen Dienstleister wirksame Schutzmaßnahmen zu ergreifen, die dies verhindern - zumindest ein effizienter Passwortschutz. Die unmittelbare Einwahl ist jedoch nicht anfällig für systematische Angriffe aus dem Internet.

In moderneren Systemen wird auch aus Kostengründen mitunter eine sogenannte „VPN“[7]-Verbindung für die externe Anbindung gewählt. Diese nutzt grundsätzlich eine zum Kanzleinetzwerk bestehende Internet-Verbindung, ist aber durch die verwendete Verschlüsselungstechnik bei richtigem Einsatz grundsätzlich sicher.

Feste Anbindung von Heimarbeitsplätzen erfordert zusätzliche Absicherung

Ein erhöhtes Risiko besteht allerdings, weil bei dieser Variante eine dauerhafte Verbindung zwischen Internet und Kanzleinetzwerk notwendig ist, die im Verhältnis mehr Angriffsfläche bietet als die Verbindung, die nur bei Bedarf aufgebaut wird und darum z.B. nachts abgeschaltet ist. Diesem Risiko kann nur durch eine besonders sorgfältige Sicherungsstruktur, insbesondere auf Firewall-Ebene, begegnet werden.[8]

---

[7] Virtual Private Network = Virtuelles Privatnetzwerk.

[8] Vgl. hierzu Kapitel 9.3 (Telearbeit) des BSI-Grundschutzhandbuches.

5. Gefahrenpotentiale

Unterschiedliche Nutzungsformen der Internet-Dienste bergen unterschiedliche Gefahren, die im Folgenden in groben Zügen dargestellt werden sollen.

a. Bei der Nutzung von E-Mail

E-Mail ist nach wie vor eine der beliebtesten Anwendungen im Internet und ist einer der primären Gründe für viele Notarkanzleien, sich mit diesem Thema auseinanderzusetzen. Der einfache und schnelle Nachrichtenaustausch auf diesem Weg gehört für viele schon zum guten Ton und bringt auch Arbeitserleichterungen im Alltag mit sich. Insbesondere das zusammenwirkende Arbeiten an Dokumenten wie Vertragsentwürfen gehört vielfach schon zur täglichen Praxis.

Text-Dateien können versteckte Informationen enthalten

Versendet der Notar Textdokumente – unabhängig davon, ob sie zur bloßen Kenntnisnahme oder zur Weiterverarbeitung bestimmt sind – sollte er sich im klaren darüber sein, dass Textverarbeitungsprogramme (insbesondere die verschiedenen Versionen von Microsoft Word) oftmals eine Vielzahl von verdeckten Informationen (zum Beispiel zurückliegende Änderungen am Text) speichern, die ein Kundiger mit wenigen Handgriffen sichtbar machen kann. Darum ist es empfehlenswert, bei zur Kenntnisnahme bestimmten Inhalten auf geeignetere Alternativformate wie PDF[9] umzustellen und beim Austausch zur Weiterverarbeitung versteckte Infor-

[9] Portable Document Format, wird zumeist erzeugt mit dem Programm „Adobe Acrobat“, es gibt jedoch auch kostenfreie Alternativen wie „FreePDF“.

mationen abzuschneiden, z.B. durch Speicherung im rtf-Format[10].

i. Viren, Würmer und Trojaner

Diese drei Phänomene sind eng verwandt, unterscheiden sich aber in Ziel und Funktionsweisen. Gemeinsam ist ihnen, dass sie sich vorzugsweise per E-Mail verbreiten.

Viren sind unselbstständige Programmroutinen, die sich – meist nach unabsichtlichem Aufruf – selbst reproduzieren und vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen. Die Infektion eines Systems mit einem Virus kann verschiedenste Wirkung haben, je nachdem, wie der Programmierer sie konstruiert hat. Wirkungen reichen von schlichten Belästigungen bis hin zur weitmöglichsten Zerstörung aller zugänglichen Daten. Innerhalb eines Netzwerkes verbreiten sich Viren oftmals blitzschnell, wenn keine Schutzmaßnahmen getroffen wurden.

Würmer haben die zusätzliche Fähigkeit, sich aggressiv über die Kommunikationsschnittstellen des befallenen Rechners zu verbreiten. Klassische Würmer versenden Kopien ihres Programmcodes an alle im E-Mail-Adressbuch eingetragenen Kontakte des befallenen Rechners, so dass die Adressaten „befallene“ Mails von ihrem Notar bekommen. Daneben richten Würmer oft noch weiteren Unsinn an, versenden z.B.

---

[10] Rich Text Format, regelmäßig in alle Textverarbeitungen integriert und unter „Speichern unter…“ verfügbar.

zufällig ausgewählte Dateien des infizierten Rechners an die Opfer.

Trojaner sind Programme, die – wie ihr historisches Vorbild – eine „virtuelle“ Hintertür im befallenen Rechner öffnen, um Angreifern Zugang zu den Daten und oft die vollständige Kontrolle über den Rechner zu ermöglichen.
Primärer Schutz gegen derartige Risiken ist die Verwendung eines geeigneten Virenscanners (dazu unten Ziff. 6.a, S. 21), der aber niemals vollständige Sicherheit bieten kann, da es oftmals eine gewisse Zeit dauert, bis neue Schadprogramme von den Scannern erkannt werden.

Vielfältige Bedrohungen durch E-Mail-Inhalte

Die genannten Schadprogramme werden oft als E-Mail-Anhang, sog. „Attachment“, versendet und sind regelmäßig so gestaltet, dass sie bei oberflächlicher Betrachtung völlig harmlos wirken. Aus diesem Grund ist jeder E-Mail-Anhang als potentiell gefährlich zu bewerten, bis er einer genaueren Untersuchung unterzogen worden ist.

Die in der E-Mail enthaltene Absenderangabe eines womöglich bekannten Kommunikationspartners ist alleine nicht ausreichend, um eine übersendete Datei als vertrauenswürdig einzustufen, da moderne Schadprogramme derartige Adressen regelmäßig verfälschen können. Auch die in der Betreffzeile enthaltenen Bezugsinformationen sind oftmals so formuliert, dass sie auf wichtige geschäftliche oder private Informationen hindeuten.

Entsprechend sollten Mitarbeiter verpflichtet werden, weder an einem Einzelplatzzugang noch im Kontext einer Netzwerkverbindung E-Mail-Anhänge ohne vorherige Prüfung zu

öffnen, da bereits ein falscher Klick zur Ausführung von schädlichem Programmcode führen kann. Bestimmte besonders gefährliche Dateitypen (z.B. .exe, .com, .bat, .scr) sollten regelmäßig sofort gelöscht werden, wenn die Vertrauenswürdigkeit nicht zweifelsfrei feststeht.

ii. Ungesicherte und nicht authentifizierte Kommunikation

E-Mail ist ein grundsätzlich unsicherer Kommunikationsweg, wenn nicht zusätzliche Maßnahmen ergriffen werden.

Die herkömmlicherweise für die Übermittlung von E-Mails benutzte Technik hat einige gravierende Schwächen, durch die sie sich von herkömmlichen Postdiensten unterscheidet. Zum einen sind die Absenderinformationen (in der Regel die E-Mail-Adresse des Absenders) so leicht zu manipulieren, dass man der Herkunft einer E-Mail nicht ohne weiteres vertrauen kann. Zum anderen geschieht die Übertragung der E-Mail über das Netz weitgehend ungeschützt, so dass sie zum einen von einem hinreichend geschickten Angreifer mitgelesen, aber auch verändert oder unterdrückt werden kann.

Wenn diese Technik im Notarbüro in Kenntnis dieser Risiken im Beteiligtenverkehr eingesetzt wird, ist es aus Gründen der Verschwiegenheitspflicht unerlässlich, vom Kommunikationspartner die Einwilligung in die Nutzung einzuholen und möglichst zu dokumentieren. Die ausdrückliche Anforderung eines Beteiligten, Daten auf dem E-Mail-Weg zuzuleiten, dürfte dem genügen.

Elektronische Signatur und Verschlüsselung dienen Identifikation und Vertraulichkeit

Es gibt technische Wege, den genannten Schwächen abzuhelfen. Die qualifizierte elektronische Signatur erlaubt einen sicheren Rückschluss auf die Person des Absenders. Die Verschlüsselung der Mail-Inhalte schützt vor Kenntnisnahme und Manipulation.[11] Beide Verfahren verlangen jedoch einigen technischen Aufwand von beiden Kommunikationspartnern, der meist nur bei regelmäßiger Kommunikation zweckmäßig erscheint[12]. Die technische Entwicklung verspricht hier mittelfristig Vereinfachungen.

iii. Spam – E-Mail-Müll

„Spam“ beeinträchtigt die Effizienz der E-Mail-Kommunikation

Unter „Spam“ versteht man unverlangt zugestellte E-Mails, die zumeist Werbebotschaften unterschiedlichster Couleur zum Inhalt haben. Der Kostenvorteil des E-Mail-Versands gegenüber herkömmlicher Post hat in diesem Bereich zu einem explosiven Missbrauch des Mediums geführt, der oftmals dazu führt, dass „gespammte“ E-Mail-Konten aufgrund des Missverhältnisses zwischen relevanten Nachrichten und unbrauchbarem Datenmüll nicht mehr zu gebrauchen sind.

Die Abwehr von Spam ist trotz neuer gesetzlicher Sanktionen und allgemeiner Anstrengung seitens der großen Mail-Dienstanbieter nicht leicht. Sog. „Spamfilter“-Programme sollen die Mehrzahl der

E-Mail-Adresse möglichst wenig verbreiten

[11] Ein Beispiel für derartige Techniken sind die im Notarnetz integrierten Funktionen auf der Basis der Programme Microsoft Outlook und Signtrust Mail.

[12] Für die zukünftige Kommunikation im Rahmen des elektronischen Rechtsverkehrs mit Justiz und Behörden wird die qualifizierte elektronische Signatur absehbar zur vorgeschriebenen Standardtechnik werden.

unerwünschten Botschaften ausfiltern, schwanken aber in ihrer Wirksamkeit. Der beste Tip für die Vermeidung von Spam ist, die E-Mail-Adresse so wenig wie möglich bekanntzugeben, am Besten nur den unmittelbaren Kommunikationspartnern. Die Verwendung der Mailadresse beim Internet-Surfen oder die Bekanntgabe auf der eigenen Webseite führt erfahrungsgemäß mittelfristig zu einer unaufhaltsamen Spamflut.

b. Bei der Nutzung des World Wide Web

Risiken lauern nicht nur bei der Nutzung von E-Mail, sondern auch beim bloßen „Surfen“ im World Wide Web. Lücken und Fehler in den eingesetzten Programmen erlauben es dem böswilligen Gestalter, in schädlicher Weise das Verhalten des abfragenden Rechners zu beeinflussen, bis hin zur Ausführung von beliebigem Programmcode.

Auch beim Internet-Surfen drohen Risiken

i. Schädliche Inhalte auf Webseiten

Die Gestaltungsmöglichkeiten, die die aktuelle Internettechnik dem Seitenprogrammierer zur Verfügung stellt, erlauben diesem insbesondere die Nutzung von Programmschnittstellen. Programmiersprachen wie „Java“, „Javascript“ und „ActiveX“ sind in modernen Zugangsprogrammen[13] eingebaut und gestatten das einfache Herunterladen von Programmen und deren Ausführung. Die Sicherheitsfunktionen dieser Programmiersprachen sind mitunter eher schwach ausgeprägt.

[13] z.B. Microsoft Internet Explorer ab Version 5

Typisch ist z.B. die Anfrage einer Webseite, zusätzliche Software auf dem Rechner installieren zu dürfen, um Seiteninhalte besser anzeigen zu können. Derartigen Ansinnen ist stets mit äußerster Skepsis zu begegnen, da der Anwender nicht wirklich einschätzen kann, was sich hinter dem ihm unbekannten Programmcode verbirgt.

Viele solcher Probleme lassen sich durch die kontinuierliche Aktualisierung der eingesetzten Programme (Internetbrowser, Betriebssystem, Office-Programm) und die bewusste Nutzung der von den Programmen angebotenen Sicherheitsoptionen (zu beiden s.u. Ziff. 6.d. und e., S. 24 ff.) wirksam bekämpfen. Allerdings führt eine Sperrung von problematischen Komponenten wie ActiveX oftmals dazu, dass Webseiten nicht richtig angezeigt werden oder Funktionen nicht nutzbar sind.

ii. Dialer

„Dialer“ bauen ohne Rückfrage teure Internetverbindungen auf

Sog. „Dialer“ sind kleine Schadensprogramme, die (meist unbemerkt vom Benutzer) teure Internetverbindungen über 0190-Nummern aufbauen. Wird der Dialer nicht bemerkt, wartet mit der nächsten Telefonrechnung oft eine unangenehme Überraschung. Gefährdet durch Dialer sind ausschließlich Internet-Nutzer, die ein Modem oder eine ISDN-Karte an den Rechner angeschlossen haben.

Der Gesetzgeber ist in diesem Bereich zwischenzeitig tätig geworden und bemüht sich, das Unwesen einzudämmen.

Vorbeugung ist jedoch in jedem Fall empfehlenswert, da auf diesem Weg bereits im Vorfeld Aufwand und Ärger vermieden werden kann.

Neben dem vorsichtigen Umgang mit den oben genannten Installationsanfragen helfen gegen Dialer auch spezielle Verteidigungsprogramme, die kostenlos im Internet erhältlich sind.[14]

iii. Ungesicherter Informationsaustausch mit Webseiten

Ähnlich wie bei der Übertragung von E-Mail werden auch die Daten, die mit dem World Wide Web ausgetauscht werden, grundsätzlich ungeschützt übertragen. Dieser Umstand ist bei der bloßen Abfrage von Standardinformationen wie z.B. Nachrichten-Webseiten grundsätzlich unproblematisch. Sensibler ist jedoch offensichtlich das Versenden eigener Informationen über das Netz, beginnend mit Passwörtern und persönlichen Daten bis hin zu wirtschaftlich bedeutsamen Daten wie Kontoverbindungen oder gar Kreditkartennummern.

SSL-Protokoll dient der vertraulichen Datenübermittlung an Internetseiten

Für den vertraulichen Informationsaustausch stellt die Internet-Technik standardmäßig das sog. SSL-Protokoll[15] zur Verfügung, das dafür sorgt, dass die Daten verschlüsselt übertragen werden und damit vor unbefugter Kenntnisnahme ge-

[14] Z.B. www.yaw.at.

[15] Abk. für „Secure Socket Layer“ (“Sichere Verbindungsebene”).

schützt sind.[16] Initiieren kann eine derartige SSL-Verbindung nicht der Anwender, sondern lediglich die abgefragte Internetseite, deren Betreiber allerdings nicht gezwungen ist, diese Option anzubieten. Das Kürzel „https://...“ vor der Seitenadresse und ein Schloss-Symbol in der unteren Zeile des Zugangsprogrammes weisen auf die Verwendung eine verschlüsselten Verbindung hin. Von einer Übermittlung sensibler Informationen über eine nicht derart geschützte Verbindung muss eindeutig abgeraten werden.

Online-Banking-Schnittstellen sind regelmäßig mit entsprechender Sicherheitstechnik ausgerüstet. Die DONot untersagt in § 27 II S.2 die Verwendung von Online-Banking für Anderkonten.[17]

iv. Webmail

Ein populäres Angebot sind aktuell Internet-Dienste, die es erlauben, per Browser-Schnittstelle von jedem beliebigen Rechner auf ein Internet-Mail-Konto zuzugreifen.[18] Da diese Dienste den E-Mail-Empfang unter Umgehung des eigentli-

---

[16] So bedient sich das Zentrale Vorsorgeregister der Bundesnotarkammer für die Dateneingabe sowie die Beauskunftung über Internet dieser Sicherheitstechnik.

[17] In diesem Zusammenhang wird in Zukunft die weitere Entwicklung der Sicherheitstechniken bei der Kontoführung abzuwarten sein. Eine Neubewertung bei der Überarbeitung der Dienstordnung scheint zumindest nicht ausgeschlossen.

[18] Aktuelle Beispiele sind die Dienste von Yahoo Mail, gmx, Hotmail und Web.de

chen E-Mail-Programmes und dessen Schutzvorrichtungen ermöglichen, eröffnen sie eine Schutzlücke, die nur schwer zu überwachen ist. Soweit die Nutzung von Webmail am Arbeitsplatz überhaupt zugelassen wird, sollten für Zugriffe erhöhte Sicherheitsanforderungen gelten.[19]

c. Angriffe auf aktive Verbindungen

Jede Internet-Verbindung ist ein Angriffsziel

Unabhängig davon, ob das Büro nur zeitweise per Wählanschluss (Modem, ISDN oder DSL) oder dauerhaft über Standleitung mit dem Internet verbunden ist, wird jede aktive Netzverbindung regelmäßiges Ziel von Hacker-Angriffen. Diese versuchen, durch Ausnutzung bekannter Sicherheitslücken Zugriff auf die angeschlossenen Rechner und deren Ressourcen zu erlangen. Diese Angriffe sind regelmäßig ungezielt, spielen sich aber außerhalb des Blickfeldes des Anwenders ab.

Firewalls bieten bei fachmännischem Einsatz und geeigneter Technik weitgehenden Schutz gegen derartige Angriffe bieten (s.u. Ziff. 6.b., S. 22).

6. Schutzmaßnahmen

Zur Abwehr der aufgeführten und weiterer Gefahren der Internet-Nutzung bedarf es eines geeigneten Schutzkonzepts, das die bereits angesprochenen Elemente von Personalführung und –schulung sowie nachhaltiger Pflege mit der notwendigen technischen

---

[19] Zu Problembeschreibung und Sicherungsmaßnahmen vgl. IT-Grundschutzhandbuch des BSI (Siehe Fn. 1), Kapitel G 5.103 (Missbrauch von Webmail) und M 5.96 (Sichere Nutzung von Webmail).

Infrastruktur koppelt. Im folgenden werden einzelne Elemente einer solchen Struktur vorgestellt.

a. Virenschutz

Virenscanner in verschiedensten Variationen gehören seit längerer Zeit bereits zur Standardausstattung der meisten Rechner. Derartige Programme können entweder anhand von Listen oder verdächtigen Strukturen Schadprogramme auffinden und unschädlich machen. Dieser Schutz erfolgte früher oftmals per Aufruf des Nutzers, heute in der Regel automatisch im Hintergrund. Überwacht werden zumeist sämtliche Dateien, auf die zugegriffen wird; viele Virenscanner bieten darüber hinaus auch eine Funktion an, mit der (im Zusammenspiel mit gängigen E-Mail-Programmen) eingehende E-Mails überprüft werden können.

Die bekannten Virenschutzprogramme aus dem Konsumenten-Bereich schützen lediglich den Arbeitsplatzcomputer, auf dem sie installiert wurden. Ein Büronetzwerk bedarf darüber hinaus auch eines Schutzes der zentralen Netzwerkkomponenten, insbesondere des Servers. Hierfür sind spezielle Produkte verfügbar, die oftmals auch mit Zusatztechniken den Schutz der angeschlossenen Arbeitsplätze ermöglichen.

Beim Anschluss eines Netzwerkes an das Internet sind grundsätzlich alle Arbeitsstationen sowie der Server mit einem Virenschutzprogramm auszustatten, da jeder Rechner als „Infektionsquelle“ in Betracht kommt. Bei Verwendung eines Einzelplatz-Zugangs muss dieser PC über hinreichenden Virenschutz verfügen. Zudem empfiehlt es sich, diejenigen Rechner, auf denen Daten (z.B. per Diskette) vom Einzelplatz-

PC in das Netzwerk überspielt werden, separat zu schützen.

„Virenwächter“ schützen nur bei regelmäßiger Aktualisierung

Von besonderer Bedeutung ist die Aktualität des Virenschutzes, insbesondere der sog. „Virus-Definitions-Datei“, anhand derer das Programm Viren erkennt. Angesichts der Dynamik der Entwicklung in diesem Bereich und der Risiken, die ein Datenverlust mit sich bringen würde, scheint eine zweiwöchige Frequenz angemessen. Viele moderne Programme erlauben eine Automation dieser Wartungsaufgabe. Das setzt jedoch regelmäßig eine Internetverbindung voraus, so dass für den Schutz nicht angebundener Netzwerke andere Wege für die Aktualisierung vorzusehen sind.[20]

b. Firewalls

Firewalls schützen das Netzwerk vor unbefugten Eindringlingen

Firewalls (dt. „Brandschutzmauern“) sind Soft- oder Hardwareeinrichtungen, die dazu dienen sollen, unerwünschten Netzwerkverkehr zu unterbinden. Das betrifft beide Datenrichtungen: Ins Netzwerk hinein und aus dem Netzwerk hinaus. Firewalls gehorchen bestimmten Regeln, die festlegen, welcher Datenverkehr unerwünscht ist. Von der Qualität dieser Regeln ist abhängig, wie groß der Schutz ist, den die Firewall dem Netzwerk bietet. Die Formulierung und Anpassung derartiger Regeln ist eine Aufgabe für den EDV-Fachmann.

Mit einer Firewall alleine ist noch keine umfassende Sicherheit erreicht

Es ist wichtig, die Grenzen des Firewall-Schutzes zu kennen. Eine Firewall ist kein Allheilmittel gegenüber den Gefahren aus dem Internet. Wenn die Firewall bestimmte Typen von Daten nach ihren Vorgaben durchlässt (z.B. In-

[20] Vertiefte Hinweise zum Virenschutz finden sind im Grundschutzhandbuch des BSI (Fn.1) in Kapitel 3.6 (Computer-Virenschutzkonzept).

ternetseiten aus dem World Wide Web oder E-Mails), besteht in diesem Bereich oftmals kein weiterer Schutz. Eine Fehlbedienung des Anwenders kann dann ohne weiteres zu Schadensvorfällen führen. Der Einsatz einer Firewall macht damit einen besonnenen und informierten Umgang mit dem Medium keineswegs entbehrlich.

Firewalls gibt es in Software- und Hardware-Varianten. Sog. „personal Firewalls“ schützen ähnlich wie lokale Virenscanner die Arbeitsstationen, auf denen sie installiert sind. Dabei ist die Identität von schützendem und zu schützendem System ein struktureller Sicherheitsnachteil. Auch ist es ungünstig, wenn der Anwender die Einstellungen der Firewall beeinflussen kann. Aus diesem Gründen spricht vieles dafür, einen separaten, zentralen Netzwerkschutz über eine Büro-Firewall zu verwirklichen. Dazu kann man entweder einen speziellen PC mit entsprechender Software ausstatten oder ein nur für diesen Zweck vorgesehenes Spezialgerät einsetzen. Die Preisunterschiede der angebotenen Lösungen sind groß. Es sollte ein angemessenes Verhältnis zwischen Schutzbedarf, Sicherheitsniveau und damit verbundenem Aufwand angestrebt werden.

Ebenso wie beim Virenschutz muss auch die Firewallkomponente kontinuierlich überprüft und notwendigenfalls aktualisiert werden. Die Wartungsfrequenzen dürfen hier etwas länger sein, z.B. quartalsweise oder halbjährlich. Darüber hinaus empfiehlt es sich, etwa vorhandene Protokolldateien regelmäßig zu untersuchen, um

Unregelmäßigkeiten oder gezielte Angriffe aufzuspüren.[21]

c. Intrusion Detection-Systeme

Das „Aufspüren von Eindringlingen“ (Intrusion Detection) ist ein verhältnismäßig junger Trend bei der IT-Sicherheit. Man kann es sich als ein Programm vorstellen, das selbstlernend den Datenverkehr im Netz beobachtet und auf Anomalitäten überwacht. Es würde z.B. Alarm schlagen, wenn ein Nutzer plötzlich versucht, den gesamten Inhalt des Servers herunterzuladen und auf einem Datenträger zu speichern oder mit hoher Frequenz Anmeldeversuche bei einer für ihn nicht freigegebenen Ressource vornimmt.

Derartige Systeme sind derzeit in ihrer Effizienz umstritten und aufgrund der hohen Kosten und des erheblichen Wartungs- und Mitwirkungsaufwandes für ein typisches Notarbüro überdimensioniert.

d. Aktualisierung sicherheitsrelevanter Software

Veraltete Software kann besonders sicherheitsanfällig sein

Einer Aktualisierung bedürfen nicht nur Virenschutz und Firewall, sondern sämtliche sicherheitsrelevanten Softwarekomponenten auf allen einsetzten Rechnern. Dazu gehören insbesondere: Betriebssysteme, Internet-Zugangsprogramme, E-Mail-Programme, Büroanwendungen wie Textverarbeitung und Kalkulationsprogramme sowie Datenbanken. Natürlich muss auch die auf dem Server laufende

---

[21] Vertiefte Hinweise zu den Anforderungen an eine Firewall sowie zu Umgang und Wartung damit finden sich im IT-Grundschutzhandbuch des BSI (Fn. 1) in Kapitel 7.3 (Firewall).

Programme zur Fehlerbehebung sind beim Hersteller kostenlos verfügbar

Software auf dem neuesten Stand sein. Der Hintergrund dieser Maßnahme ist die Vielzahl von sicherheitsrelevanten Fehlern, die in diesen Programmen ununterbrochen gefunden und behoben werden. Die Mehrzahl aller erfolgreichen Angriffe auf Computersysteme nutzen bekannte Schwächen aus, für die der Hersteller schon Lösungen zur Verfügung gestellt hat.

Auch diese Software-Updates lassen sich beim Einsatz moderner Software (z.B. MS Windows XP) automatisieren, soweit der Rechner über einen Internetanschluss verfügt.

e. Nutzung vorhandener Konfigurationsmöglichkeiten

Fast alle Programme, insbesondere aber diejenigen, die als Kernfunktion den Internet-Zugang herstellen, erlauben es, über umfangreiche Einstellmöglichkeiten eine Vielzahl von risikobehafteten Funktionen abzuschalten oder einzuschränken. Die Vornahme dieser Einstellungen setzt Kenntnisse der zugrunde liegenden Technik voraus. Es ist aber möglich, effektive Einstellungen durch einen Fachmann entwickeln zu lassen und diese dann als Teil der Vorschriften über die Internetnutzung am Arbeitsplatz überall anzuwenden.[22]

f. Kontrolle des Datenflusses

„Datensammler“ melden Informationen über Rechner und Benutzer ohne Rückfrage weiter

Bei moderner Software, angefangen vom Windows-Betriebssystem bis hin zum neuen Druckertreiber, ist eine zunehmende Tendenz erkennbar, während des Betriebes des Rechners verdeckt Informationen zu sammeln und diese

[22] Vgl. hierzu BSI-Grundschutzhandbuch (Fn. 1), Kapitel M 4.151 (Sichere Installation von Internet-PCs).

unaufgefordert und ohne Mitwirken des Anwenders an den Hersteller oder Dritte weiterzugeben. Während die meisten Verwendungszwecke für diese Art der Datensammlung harmlos sein mögen, ist die gesamte Praxis im Lichte der Verschwiegenheitspflicht des Notars bedenklich. Es gibt Maßnahmen, die dem Nutzer in diesem Bereich eine stärkere Kontrolle über den Datenfluss ermöglichen. Dazu gehören insbesondere gut konfigurierte Firewalls, die derartige Meldungen unterbinden wie auch (meist kostenfreie) Spezialsoftware, die die „Datensammler“ findet und abschaltet.

g. Einsatz von Backup-Systemen

Ohne regelmäßige Datensicherung keine Datensicherheit

Nur der Vollständigkeit halber sei erwähnt, dass eine funktionstüchtige Datensicherung für den Fall eines Datenverlustes unerlässliche Voraussetzung für ein funktionierendes Sicherheitskonzept ist. Die Details sind auch hier durchaus anspruchsvoll und bedürfen regelmäßiger Aufmerksamkeit.[23]

7. Notarnetz-Anschluss als Rundumsicherung

Das Notarnetz bietet wirksamen Schutz mit geringem Wartungsaufwand

Eine Lösung, mit der die Sicherheitsrisiken aus der Nutzung von Internet-Anschlüssen beherrscht werden können, ist der Internet-Anschluss über das von der Notarnet GmbH angebotene Notarnetz-VPN. Die Technik des VPN erlaubt es, den gesamten Internet-Verkehr des Notariats über einen zentralen Server zu leiten, der mit den notwendigen Sicherheitsvorkehrungen (Firewall) ausgestattet ist. Zum Sicherheitskonzept gehört weiterhin ein E-Mail-Postfach für jeden Teil-

[23] Vgl. hierzu Kapitel 3.4 (Datensicherungskonzept) im BSI-Grundschutzhandbuch.

nehmer, das durch einen leistungsfähigen Virenscanner geschützt ist. Die Wartung und Überprüfung der Sicherheitskomponenten geschieht zentral durch Fachpersonal im Rechenzentrum. Insbesondere die gleichfalls von diesem geleistete kontinuierliche Überwachung des Notarnet-Netzwerkes und die kurzfristige Reaktion auf Zwischenfälle und Bedrohungen bieten ein Sicherheitsniveau, das ansonsten mit den Mitteln eines mittelständischen Büros nicht zu erreichen ist. Die Sicherheitsarchitektur des Notarnetzes ist vergleichbar mit der eines größeren Unternehmens mit eigener IT-Sicherheitsabteilung.

Die Signaturkarte ist der Schlüssel zum elektronischen Rechtsverkehr

Der Zugang zum Notarnetz-VPN wird gesichert durch die Signaturkarte der Zertifizierungsstelle der Bundesnotarkammer und ist darum auch vor Missbrauch innerhalb des Büros geschützt. Die Signaturkarte bietet darüber hinaus weitere Anwendungsmöglichkeiten bei der bereits oben angesprochenen Signatur und Verschlüsselung von E-Mails.

Zusatznutzen durch Informationsangebote

Zum Notarnetz gehört außerdem als exklusiver Inhalt der Zugriff auf die Gutachtendatenbank des DNotI. Eine Recherche in den ca. 10.000 ausgewählten Gutachten zu speziellen, notarrelevanten Fragen erlaubt die schnelle Lösung von Rechtsproblemen auch nicht alltäglicher Natur – rund um die Uhr und ohne Wartezeiten.

Das Sicherheitspaket des Notarnetzes hat für den Notar den Vorteil, dass er ohne Zusatzinvestitionen in die eigene Infrastruktur und ohne Wartungsaufwand eine hochwertige Komplettlösung für die technische Seite der Internetsicherung erhält. Auch bei Anschluss an das Notarnetz-VPN bleibt ein verantwortungsvoller und Sicherheitsbewusster Umgang mit dem Online-Medium unerlässlich.

Informationen über den Anschluss, die Teilnahmevoraussetzung und den Preis können im Internet unter www.notarnetz.de abgerufen oder bei der NotarNet

GmbH (Burgmauer 53, 50667 Köln, Tel.: 0221-2575201, Fax: 0221-236808) angefragt werden.

8. Weiterführende Informationen

Da es sich bei der EDV-Sicherheit um ein höchst dynamisches und komplexes Feld handelt, können viele Probleme an dieser Stelle nur angerissen werden und allgemein nicht soweit vertieft werden, wie sie es womöglich verdient hätten. Es gibt jedoch sowohl im herkömmlichen Papiermedium als auch im Internet eine grosse Zahl von Angeboten, die eine weitere Recherche ermöglichen. Insbesondere sei dabei auf zwei Quellen hingewiesen:

Das bereits mehrfach genannte IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik ist eine umfassende Fundgrube, die sämtliche Aspekte der EDV-Sicherheit behandelt. Aufgrund seines Umfangs und seines gesamtheitlichen Ansatzes ist es für das typische Notarbüro eher als Nachschlagewerk denn als Leitfaden geeignet.

Das Grundschutzhandbuch ist (kostenpflichtig) in Papierform oder (gratis) als CD-ROM oder Internet-Download erhältlich. Informationen. Bezugsmöglichkeiten und weitere Informationen sind unter http://www.bsi.bund.de/gshb/ abrufbar.

Ausführlichere Informationen über das Thema Internetsicherheit im Notariat enthält ein Fortbildungsskriptum, das auf Anfrage in elektronischer Form über die NotarNet GmbH zu beziehen ist.