KANZLEIMANAGEMENT

„BEACHTUNG ERFÄHRT DER DATENSCHUTZ OFT ERST DANN, WENN EIN SCHADEN EINGETRETEN IST"

DARUM GEHT ES

Das Thema Umgang mit dem Internet, Verschlüsselung und Schutz der Mandantendaten ist ein so umfassendes Thema, dass man ohne weiteres sehr viel Zeit mit reichlich Literatur oder Internetquellen zu diesem Sujet verbringen kann. Die besonderen Sorgfaltspflichten, denen Anwaltskanzleien nachzukommen verpflichtet sind, machen es in diesem Zusammenhang zu einem unausweichlichen Muss, sich mit dieser Thematik zu beschäftigen.

Die Zeit, in der Viren und Trojaner oder sonstige Schädlinge aus den digitalen Weiten die wesentliche Bedrohung für die Bildschirmarbeiter waren, ist längst passé. Vor noch gar nicht vielen Jahren beließen es viele Anwender - wenn überhaupt - bei einer Antivirensoftware, die dann häufig auch noch in unregelmäßigen Abständen mit Updates gefüttert wurde.

Seitdem hat sich viel geändert. Es geht dabei gar nicht einmal nur um die unzähligen neuen Varianten übler Schädlinge wie Trojaner, Keylogger oder ähnliche digitale Störenfriede. Denn seit einigen Jahren haben viele neue Techniken dafür gesorgt, dass die Gefahrenquellen nicht mehr nur im Internet, sondern auch bei den Übertragungswegen selbst oder unzureichenden Verschlüsselungen liegen. Die Vernetzung von Bürocomputern, die kabellose Internetnutzung (WLAN) oder der Datenaustausch mittels mobiler Smartphones sind anschauliche Beispiele für die Entwicklung. Auch die vielen neuen Speichermedien wie USB-Sticks, Speicherkarten oder kleine MP3-Player machen im Gegensatz zu den Zeiten, in denen noch Disketten ausgetauscht oder Sicherheitskopien auf CDs oder Bändern angefertigt wurden, einen Tansfer selbst größerer Datenmengen spielend einfach.

OFFENE SCHEUNENTORE IN KANZLEIEN

Neue Techniken bedeuten jedoch häufig im Umkehrschluss auch neue offene Tore für Unbefugte und Kriminelle. Und diese sehen sich häufig in der komfortablen Situation, dass sie gar nicht mehr irgendwo eindringen müssen, sondern lediglich zu schauen haben, wo solche Tore offenstehen. Und in vielen Kanzleien kann man insoweit gar von offenen Scheunentoren sprechen, denn Sicherheit und Datenschutz beim Umgang mit der EDV in der Kanzlei spielen oft nur eine Nebenrolle, der kaum Beachtung geschenkt wird.

Was mag da passender sein, als zu dem Thema einen fachkundigen Spezialisten zu Wort kommen zu lassen, der dieses Thema sowohl mit dem nötigen Know-how als auch aus der Sicht eines Juristen erläutern kann? Stefan Bühner ist Rechtsanwalt und seit zwei Jahren als Kanzleiberater tätig. Er betreibt auf seiner Internetseite **www.anwalten.de** ein Projekt mit aktuellen Neuigkeiten der Jurasoft Unternehmensgruppe (RA-Micro, RA-RC, DictaNet) und Wissenswertem aus dem juristischen IT-Umfeld. Auf seinen Internetseiten finden sich fortlaufend Informationen zu den Themen Datensicherheit, Diktiersoftware, Signaturkarten und vielem mehr. Im nachstehenden Interview gibt Bühner einige wichtige Tipps und Hinweise für Rechtsanwaltsfachangestellte bei ihrem täglichen Umgang mit den „Kollegen" Tastatur und Maus.

? *Als Kanzleiberater in IT-Fragen setzen Sie sich intensiv mit spezifischer Anwaltssoftware wie RA-MICRO oder Dictanet und den neuen Entwicklungen in diesem Segment auseinander. Wie reagieren die Entwickler dieser Software auf die steigenden Anforderungen an die Sicherheit ihrer Programme?*

Die Reaktion der Anbieter ist durchaus verschieden. RA-MICRO beispielsweise entwickelt seine Anwaltssoftware konsequent auf neuesten Microsoftstandards der .net-Technologie. In großen Umgebungen setzt RA-MICRO verstärkt auf SQL-Datenhaltung. Die Anwendung neuester Programmiertechniken ermöglicht eine schnelle Reaktion auf neue Erkenntnisse im Bereich der IT-Sicherheit und die Umsetzung bzw. Einbindung aktueller kryptographischer Verfahren, also Verschlüsselungstechniken. So wird derzeit beispielsweise mit „ra e-post" ein neues E-Dokumentenaustauschsystem entwickelt, um als Gegenstück zum elektronischen Rechtsverkehr mit den Gerichten (ERV) den sicheren, verschlüsselten elektronischen Schriftverkehr der Anwälte untereinander zu gestalten. Der Zugang zu „ra e-post" ist exklusiv deutschen Anwälten, Notaren und Steuerberatern vorbehalten.

? *Mittels Ihrer Tätigkeit haben Sie sicherlich auch viele Eindrücke von Kolleginnen und Kollegen gesammelt bzw. bekommen mit, wie das Thema „Datensicherheit" in den Büros gehandhabt wird. Setzen sich Ihrer Ansicht nach Anwaltskanzleien und Notariate mit diesem Punkt angemessen auseinander? Oder erfährt diese Thematik eher eine zu geringe Beachtung?*

Nach meiner Erfahrung erfährt dieser Punkt zwar Beachtung. Allerdings sind vielen Kollegen die technischen Hintergründe zu komplex und zu umfangreich. Schließlich sollen Anwälte ihrem Beruf nachgehen und nicht zu IT-Sicherheitsexperten werden. Daher hilft hier nur der Einsatz von kompetenten und vertrauten Spezialisten, die sich täglich mit dieser Materie auseinandersetzen, wozu dem „gewöhnlichen" Anwender einfach die Zeit fehlt. Darüber hinaus stehen Anwälte genau wie jeder Nutzer in dem Spannungsfeld zwischen „es muss funktionieren" und „ich kümmere mich jetzt erst mal um die Hintergründe, bevor ich das Programm installiere". So kann es schon mal vorkommen, dass auch Anwälte ungesicherte WLAN-Netze betreiben. Beachtung erfährt das Thema oft erst dann, wenn bereits ein Schaden eingetreten ist oder in den Medien über spektakuläre Datendiebstähle und Sicherheitsrisiken berichtet wird.

? *Welche konkreten Empfehlungen würden Sie Kolleginnen und Kollegen und den Rechtsanwaltsfachangestellten in den Kanzleien geben, die sich für eine Schulung zum Thema „Datensicherheit oder Umgang mit elektronischer Korrespondenz" interessieren? Welche Informationsquellen würden Sie Interessierten nahelegen?*

Hier ist die Empfehlung abhängig vom technischen Verständnis und Kenntnisstand des Anwalts bzw. der Angestellten. Zur Schaffung eines grundlegenden Verständnisses sind Schulungen von regionalen IT-Systemhäusern oder Internetseiten wie z.B. die Seite **www.bsi-fuer-buerger.de** gut geeignet. Zur Vertiefung und um sich dauerhaft auf einem aktuellem Wissensstand zu halten, kann man Internetseiten wie **www.heise.de** oder die spezielle Seite **www.heise.de/security** sowie entsprechende Newsletter empfehlen. Dies ist jedoch extrem zeitaufwändig. Die für den Anwalt einfachste Möglichkeit ist die Einbindung von externen IT-Spezialisten als Dienstleister.

? *In einigen Büros mangelt es schon an grundsätzlichen Schutzvorkehrungen. Wie sollte der ideale „Standardschutz" aussehen, für den jede Kanzlei Sorge tragen sollte?*

Der ideale Standardschutz wäre ein in der Kanzlei tätiger Administrator oder zumindest eine Person, die technisch geschult ist und das System regelmäßig wartet und überwacht. Die Internetanbindung sollte grundsätzlich durch eine Hardware-Firewall nach außen erfolgen. Diese Firewall sichert das Kanzleinetzwerk gegen Angriffe von außen und kann je nach Ausführung zum Virenscan und als Spamfilter eingesetzt werden. Weiterhin ist der Einsatz von Antivirensoftware auf Servern und Arbeitsplatzrechnern für den internen Schutz unbedingt notwendig. Die aktuellen Bedrohungen in Form von Schadsoftware und Trojanern gelangen über verschiedene Wege wie z.B. Datenträger oder durch den Besuch einer Internetseite auf

die PCs. So gibt es Berichte über USB-Speicher, MP3-Player oder digitale Bilderrahmen, die bereits beim Verkauf mit Schadsoftware infiziert waren.

? *Während noch vor zehn Jahren eine vernetzte EDV nicht die Regel und auch die Internetnutzung in den Kanzleien noch nicht derart routiniert wie heute Bestandteil des Büroalltags war, werden heute immer mehr Arbeiten online erledigt. Welche besonderen Gefahren bringt dies mit sich und welche Schutzmechanismen bietet eine Anwaltssoftware insoweit?*

Eine Anwaltssoftware als solche kann grundsätzlich keinen Schutz gegen Angriffe aus dem Internet bieten. Dies ist primär Aufgabe der bereits oben erwähnten Hard- und Software, also Firewalls und Antivirenprogramme. Der Zugang zur Anwaltssoftware als solcher und zu speziellen Bereichen der Anwaltssoftware kann durch Vergabe von Benutzerrechten und Chiffren gesteuert werden. In einigen Bereichen wie z.B. bei den Adressdaten erfolgt durch die Anwaltssoftware eine verschlüsselte Speicherung. Hierdurch sind die gestohlenen Daten für den Dieb wertlos. Die Diktiersoftware DictaNet bietet beispielsweise die Möglichkeit, digitale Diktate verschlüsselt per E-Mail zu versenden.

? *Sind Ihnen Fälle bekannt, in denen mangelnde Sicherheitsvorkehrungen in den Kanzleien zu erfolgreichen Hackerangriffen oder Datenabfluss geführt haben?*
Welche Probleme können solche unangenehmen Vorkommnisse nach sich ziehen?

Aus meiner eigenen Erfahrung kann ich von solchen Fällen zum Glück nicht berichten. In den Fachmedien sind derartige Fälle jedoch schon veröffentlicht worden. Die Anwälte sind gem. § 43a BRAO und § 2 der Berufsordnung zur Verschwiegenheit verpflichtet. Diese Verpflichtung schließt auch eine entsprechende Absicherung der Kanzlei und der IT-Ausstattung ein.

? *Viele Anwender betonen, wie sinnvoll die Nutzung alternativer Internetbrowser wie Firefox oder Opera bzw. E-Mail-Programme wie Mozilla Thunderbird ist, um sicherer im Internet zu surfen bzw. sich viele Viren oder andere Schädlinge von den eigenen PCs fernzuhalten, die für das gängige Programm Outlook geschrieben sind. Ist das zutreffend oder werden auch alternative Browser und E-Mail-Programme zunehmend stärker von Virenprogrammierern berücksichtigt?*

Die hohe Anzahl der im letzten Jahr für die von Ihnen angesprochenen Alternativprogramme – insbesondere Firefox und Thunderbird – erschienenen Sicherheitsupdates zeigt, dass auch diese Programme vermehrt Ziel von Angriffen sind. Unabhängig von den eingesetzten Programmen zum Internetsurfen und E-Mail-Empfang ist daher zu empfehlen, stets die aktuellsten Versionen zu verwenden und alle Sicherheitsupdates unverzüglich nach Veröffentlichung zu installieren. Eine unter Sicherheitsaspekten vorgenommene Konfiguration der Programme kann viele „Sicherheitslücken" schließen. Die derzeit im Umlauf befindlichen Viren und Schädlinge nutzen jedoch nicht nur die Internetbrowser und E-Mail-Programme, sondern auch viele weitere Programme, die oft auf den Rechnern der Anwälte installiert sind. Beispielsweise sei hier der Acrobat Reader genannt. Auch viele Programme zum Abspielen multimedialer Inhalte sind beliebte Einfallstore. Programme wie der Windows Media Player, Quicktime, VLC oder Winamp sind sehr populär. Aber auch Zusatzprogramme (AddIns) und Erweiterungen der Browser wie z.B. Flash und ActiveX machen einen PC anfällig für Schädlinge. Hier hilft oft nur das Abschalten dieser Funktionen, wobei jedoch viele Internetseiten dann nicht mehr korrekt dargestellt werden können.

? *Viele Juristen kommunizieren via Blackberry oder arbeiten in ihren Kanzleien mit WLAN-Verbindungen, die ungeschützt ein großes Risiko darstellen. Welche besonderen Sicherheitsvorkehrungen empfehlen Sie Kollegen und Fachangestellten, die mittels Smartphones Daten zwischen Büro und Heimarbeitsplatz austauschen und in den Büros mobile Datenträger oder drahtlose Kommunikation nutzen?*

Allgemein kann bei der Nutzung mobiler Geräte, egal ob Smartphones oder Notebooks, eine Verschlüsselung der Daten auf diesen Geräten empfohlen werden. Für Notebooks gibt es beispielsweise Möglichkeiten, das komplette System zu verschlüsseln. So sind bei einem Diebstahl zumindest die Daten des Rechtsanwalts vor fremden Zugriffen geschützt. Datenzugriffe mit den Geräten sollten über eine gesicherte Verbindung wie z.B. VPN (Virtual Private Network) erfolgen.

Notebooks für Business-Anwender bieten heute bereits Zugangsschutz über Fingerprintsensor. Das ermöglicht dem Anwalt, das Notebook durch Auflegen eines Fingers auf einen Sensor zu aktivieren oder zu entsperren. Auch das Bios der Notebooks bietet verschiedene Möglichkeiten zum Schutz der Computer. So kann sowohl der Zugang zum Computer selbst als auch zum Bios, in dem die Grundeinstellungen des Computers hinterlegt sind, geschützt werden. Einige Modelle bieten per Bios auch einen Zugriffsschutz auf die Festplatte des Computers.

? *Ein häufiges Problem stellt auch das Kapern der eigenen E-Mail-Adresse dar, mit der dann tausendfach Spamsendungen versendet werden. Wie sollte sich eine Kanzlei verhalten, wenn sie feststellt, dass die eigene E-Mail-Adresse missbräuchlich verwendet wird?*

Hier muss man unterscheiden. Das „Kapern" der Mailadresse kann in der Form geschehen, dass solche Massenwerbung von einem fremden Server z.B. auf Togo versendet wird und die Mailadresse der Kanzlei lediglich als Absender erscheint. Hiergegen kann sich die Kanzlei faktisch kaum wehren, da die tatsächlichen Mailabsender zwar zu ermitteln, aber schwer zu verfolgen sind. Die zweite Möglichkeit ist, dass der Mailserver bzw. das E-Mail-Postfach der Kanzlei „gehackt" und für einen Spamversand missbraucht wird. Hier muss die Kanzlei unverzüglich tätig werden, da diese Mails, die ja nun von dem tatsächlichen Mailaccount der Kanzlei ausgehen, der Kanzlei möglicherweise zuzurechnen sind. Ein weiteres Problem ist, dass die Kanzlei über ihre Mailadresse massenhaft Spam bekommt und hierdurch der Aufwand zur Nutzung der Mailadresse erschwert wird. Hier kann den Kanzleien nur ein sorgsamer Umgang mit der eigenen E-Mail-Adresse geraten werden. Auch die Nutzung verschiedener Adressen für allgemeine Kanzleipost, Newsletter und elektronischen Rechtsverkehr kann hier Abhilfe schaffen.

Weiterhin sollten Rechtsanwälte und Kanzleien darauf achten, dass die Mailadressen nicht auf den Internetseiten der Kanzlei veröffentlicht werden – viel sinnvoller für eine Kontaktaufnahme ist der Einsatz von serverseitigen Formularen, in denen der Interessierte dann Text und Absenderangaben eingibt. Diese Formulare sollten durch Captchas (Sicherheitsabfragen in Form von kleinen Rechenaufgaben oder Zahlenkombinationen) gegen Missbrauch gesichert werden. Weiterhin ist eine „verschlüsselte" Darstellung zu empfehlen. Dies kann z.B. dadurch erreicht werden, dass die Mailadresse auf der Internetseite als Grafik dargestellt wird.

Herzlichen Dank für Ihre Antworten!