Internetüberwachung

Abgehört

US-Geheimdienste können weltweit Kommunikation in Telefon- und Datenleitungen abfangen und auswerten. Das ist auch eine besondere Herausforderung für Kanzleien, deren Geschäftsgrundlage absolute Vertraulichkeit im Umgang mit Mandantendaten ist.

Cryptopartys sind derzeit hoch im Kurs. Die Besucher erfahren auf diesen Treffen, wie sie ihre Kommunikation via Internet sicherer machen. „Genauso, wie ich mein Auto abschließe, müssen auch Daten vor dem Zugriff von Unbefugten grundsätzlich geschützt werden, unabhängig davon, ob es Geheimdienste oder Kriminelle sind“, sagt Jimmy Schulz. Der Politiker saß in der vergangenen Legislaturperiode für die FDP im Bundestag und ist Gründer des Unternehmens „Cyber Solutions – Kommunikative Datentechnik“. Anfang September zeigte er auf einer Cryptoparty im Berliner Reichstag interessierten Abgeordneten verfügbare Sicherheitswerkzeuge für deren Laptops.

Bundesregierung hält sich mit Informationen zurück

Mitglieder der Regierung informieren die Öffentlichkeit bislang nur spärlich über den Umfang der US-Geheimdienstaktivitäten auf deutschem Boden beziehungsweise über die, die sich gegen deutsche Staatsbürger richten. Somit können Whistleblower Edward Snowden und Guardian-Journalist Glenn Greenwald die Weltöffentlichkeit immer wieder mit neuen Enthüllungen überraschen. Die Reaktionen in der Öffentlichkeit auf die Abhöraktionen reichen von „Habe ich schon immer geahnt“ bis zu „unglaubliche Verletzung demokratischer Grundrechte“.

Auch Kanzleiinhaber beschäftigt das Thema, sind sie doch qua Standesrecht zur Vertraulichkeit bezüglich der Mandantendaten verpflichtet. Im Lichte von „Prism“ und „X Key Score“ ist das keine leichte Aufgabe. Die Datev hat nach Bekanntwerden der Affäre einen sechsfach höheren Informationsbedarf auf ihren Internetseiten mit Datev-Sicherheitslösungen registriert und auch erste Neukunden in diesem Segment verzeichnet. „Beispielsweise stellen wir einen deutlich steigenden Absatz der Datev-E-Mail-Verschlüsselung fest“, sagt Uwe Reipa, bei der Datev verantwortlich für die Vermarktung der Sicherheitslösungen.

Auch bei der HMD Software AG gibt es Informationsbedarf. Vorstand Martin Moser leitet diese Anfragen an das Partnerunternehmen Munker Unternehmensberatung weiter. „Der Zulauf zu Informationsveranstaltungen ist deutlich angestiegen und damit sind wir schon einen entscheidenden Schritt weiter: Nur wenn es ein flächendeckendes Bewusstsein für Datenschutz und Datensicherheit gibt, können wir auch davon ausgehen, dass unsere Daten nicht nur bei einigen wenigen, sondern bei den meisten unserer Geschäftspartner sicher sind und rechtskonform behandelt werden. Dieses Bewusstsein und das notwendige Verständnis für die Thematik können wir jetzt schaffen. Insofern haben die Veröffentlichungen rund um Edward Snowden sicher einen positiven Effekt“, erläutert Geschäftsführerin Christine Munker.

Softwareanbieter wie Addison, Datev oder HMD-Software betonen in diesem Zusammenhang die Sicherheit ihrer ASP-, SAAS- und Online-Lösungen. Alle Modelle eint, dass sensible Daten in einem gesicherten Rechenzentrum liegen, das den deutschen Datenschutzgesetzen unterworfen ist. Die Übertragung der Daten zwischen Kanzlei und Rechenzentrum erfolgt dabei gesichert per VPN und verschlüsselt. „Auf Steuerberater zugeschnittene ASP-Lösungen sind eine sehr gute Alternative zur eigenen IT-Landschaft und lösen einige Sicherheitsprobleme im Handumdrehen. Solche Rechenzentren erfüllen höchste Ansprüchen in puncto Datensicherheit und werden von Experten überwacht. Rechenzentren können Sicherheitsvorkehrungen umsetzen, die eine Einzelkanzlei sich niemals leisten kann und will. Hackerangriffe sind dort beispielsweise an der Tagesordnung und die Systeme sind bestens darauf ausgerichtet, diese Angriffe abzuwehren“, sagt Beraterin Munker.

Wer Bauchweh bei der Übertragung und Speicherung von Mandantendaten in einem Rechenzentrum hat, dem bleibt nur ein lokaler Kanzleiserver, der keine Verbindung zur Außenwelt hat. „Der Gedanke ist richtig, aber in der Praxis schwer umsetzbar. Wir sprechen von einem System, in dem kein Server oder Arbeitsplatz, auf dem personenbezogene oder sensible Daten abgelegt werden, einen Internetzugang erhält. Das erzeugt einen nicht zu vernachlässigenden internen Aufwand, allein schon um den Empfang und Versand von E-Mails zu organisieren“, sagt Munker.

Firewalls und Virenscanner als Basisausstattung

Für Uwe Reipa von der Datev gehören Firewalls und Virenscanner zur Grundausstattung beim Schutz vor externen Angriffen, mit denen sich das Kanzleinetzwerk absichern lässt. „Schwieriger ist der Schutz von Daten auf dem Transportweg. Hier ist die konse-

quente Nutzung von Verschlüsselungslösungen geboten“, so Reipa. Schließlich haben die Geheimdienste Zugriff auf Datenströme an etlichen Knotenpunkten der internationalen Daten- und Telefonleitungen. „Bei einer vernünftigen Verschlüsselung ist auch für Nachrichtendienste der Aufwand so hoch, dass die Entschlüsselung mehrere Wochen oder gar Monate dauern würde, um den Schlüssel für eine E-Mail zu knacken“, sagt IT-Sicherheitsexperte Christian Schaaf (siehe Interview S. 43).

Endscheidend ist die Schlüssellänge, entsprechende Verschlüsselungsverfahren sind lange bekannt und im Markt etabliert, doch bei Nutzern noch unbeliebt. Bei einem asymmetrischen Verschlüsselungsverfahren muss der Absender erst den öffentlichen Schlüssel des Empfängers kennen, um ihm oder ihr eine verschlüsselte E-Mail schicken zu können. Nur der Empfänger kann mit seinem privaten Schlüssel die Nachricht dechiffrieren. Einen herben Vertrauensverlust erlitt die Technik, als die Öffentlichkeit erfuhr, dass Microsoft den US-Spionen Einsicht in verschlüsselte Mails auf seiner Online-Plattform „Outlook.com“ gewährte. Aber auch auf die Microsoft-Cloud-Speicher Skydrive sowie das Telefonprogramm Skype hat der NSA Zugriff. Aber auch Apple, AOL, Facebook, Google, Yahoo und You Tube waren durch Gesetze wie den „Foreign Intelligence Surveillance Act“ (FISA) und den „Patriot Act“ gezwungen, der NSA Zugang zu den Servern zu verschaffen. Die meisten amerikanischen Online-Dienste kann eine Kanzlei umgehen, aber bei den Betriebssystemen und Office-Programmen auf PC und Laptop dominieren Produkte von Microsoft. Niemand mag heute mit absoluter Sicherheit ausschließen, dass die US-Entwickler Hintertüren für die NSA integrieren mussten. Somit kommt Alexander Koschier, Bereichsleiter Marketing & Sales, bei Agenda zu dem Schluss: „Es gibt keine absolute Datensicherheit. Als IT-Anwender kann ich nur – unter Beachtung des Aufwand-Nutzen-Verhältnisses – das Niveau so weit erhöhen, dass es mit normalen Mitteln unwahrscheinlich ist, dass ein anderer Zugriff auf meine Daten erlangt. Dieser Status gilt allerdings nur zu einem Zeitpunkt. Innerhalb kurzer Zeit können neue Technologien meine Sicherheitsbemühungen aushebeln und ich muss nachziehen. Datensicherheit ist also ein Thema, dass man als Steuerberater ausgewiesenen Spezialisten überlassen muss.“

„Vollkommener Schutz vor Lauschangriffen unmöglich“

Nüchtern sieht es auch Ralf Kurka, Geschäftsführer und Leiter Entwicklung der Produktlinie Addison bei der Wolters Kluwer Software und Service GmbH im baden-württembergischen Ludwigsburg: „Einen vollkommenen Schutz vor Lauschangriffen wie Prism oder Tempora gibt es letztendlich nicht, da die Einflussmöglichkeiten eher gering sind. Auch die Verschlüsselung von E-Mails bietet nur einen teilweisen Schutz, da die Metadaten nicht verschlüsselt sind.“ Unter Metadaten versteht man die Angaben, wann wer mit wem und wo kommuniziert hat. Damit können die Überwacher detaillierte Bewegungs- und Kommunikationsprofile erstellen.

Wie teuer umfassender Datenschutz und Datensicherheit in einer Kanzlei werden, ist schwer zu beziffern. „Eine Rolle spielen dabei sowohl die jeweiligen Anforderungen als auch die Größe und Komplexität des zu schützenden Netzwerks und der Grad des eigenen Aufwands zur Pflege der Sicherheitsinfrastruktur. Der Einstiegspreis in unsere Sicherheitslösung Datev-Net pro liegt zum Beispiel bei monatlich rund 40 Euro netto. Dafür braucht sich der Anwender um nichts selbst zu kümmern. Er stellt in seiner Kanzlei den von uns gelieferten Router auf – den Rest übernimmt die Datev“, erklärt Uwe Reipa.

Technischer Schutz ist die eine Seite, die Umstellung menschlicher Gewohnheiten die andere. So meint Ralf Kurka von Wolters Kluwer Software: „Man sollte die Diskussion nicht auf die Technologie einengen; der wichtigste Faktor ist immer der Mensch, der sich Passwort, Zugangskontrollen usw. merken oder mitführen muss – hier sind Grenzen gesetzt, da die Anwendungen auch handhabbar bleiben müssen. Es kommt darauf an, hier das richtige Maß zu finden. Was hilft die tollste Sicherheitstechnik, wenn sie unpraktisch ist und im Alltag immer wieder umgangen wird.“

» Auf Nummer sicher

Mit folgenden Maßnahmen lässt sich der Datenschutz in der Kanzlei verbessern.

1 **Rechenzentrum:** ASP- und SAAS-Angebote bieten ein hohes Maß an Sicherheit. Die Datenübertragung ist in der Regel verschlüsselt, die Rechenzentren sind gegen externe Hacker-Angriffe als auch Feuer, Überschwemmung, Stromausfall, Datenverlust und Einbruch besonders geschützt. Wichtig ist, einen Anbieter auszuwählen, der diese Kriterien erfüllt und sein Rechenzentrum in Deutschland betreibt.

2 **Firewall:** Überwacht den Datenverkehr am Ein- und Ausgang des Kanzleinetzwerkes.

3 **Virenscanner:** Erkennt Trojaner und andere Malware auf lokalen Festplatten.

4 **Verschlüsselung:** E-Mails und sämtliche sensiblen Daten sollten auf dem Weg zu Mandanten, Behörden wie auch in Rechenzentren verschlüsselt und im besten Fall gesichert (Virtual Private Network, VPN) übertragen werden.

5 **Cloud-Speicher:** Kommerzielle Anbieter wie Dropbox, Sky Drive, Box, Google Drive und Apples I-Cloud sollten nicht für Mandantendaten genutzt werden. Daten sollten mithilfe von Anbietern wie Boxcryptor.com oder Cloudfogger.com/de vor der Übertragung verschlüsselt werden. Die Telekom betreibt mit dem Mediencenter einen Cloud-Speicher mit Rechenzentren in Deutschland.

Quelle: Autor

Dirk Kunde

ist Diplom-Volkswirt und betreibt das Journalistenbüro Textkunde in Hamburg. Seine Schwerpunkte bilden die digitale Wirtschaft sowie nutzwertorientierte Geldthemen.

E-Mail: kunde@textkunde.de