

Anonymität, Sicherheit oder Überwachung?

Identitäts-Management in E-Mail-Verkehr und Internet ist schwierig.

Wir haben Ihnen gezeigt, wie wichtig eine Vielfalt Ihrer Identitäten für Ihre Privatsphäre ist. Wir haben Ihnen erläutert, dass diese Vielfalt hier und da aus wirtschaftlichem Interesse unterminiert wird. Wir haben Ihnen aber auch Beispiele geliefert, wie staatlicherseits eine unzureichende Abwägung zwischen gesellschaftlichem Nutzen und Ihrem persönlichen Datenschutz zu Konflikten führen kann. Aber zur Kontrolle – und zum Schutz – Ihrer Identitäten-Vielfalt gerade in der modernen Welt der digitalen Kommunikation gehört noch ein weiterer Faktor von elementarer Bedeutung: Sie selbst. Sie surfen im Internet? Sie besuchen Webseiten von Freunden, Händlern, zur persönlichen Information oder zum Zeitvertreib? Viel Spaß und viel Erfolg. Ist Ihnen aber auch klar, dass Sie als Online-Nutzer mehr Spuren hinterlassen als Ihnen vielleicht lieb ist? Wer im Internet surft, tut dies in der Regel unter dem Verlust seiner Anonymität. Das beginnt schon bei der Einwahl ins “Netz der Netze”: Als privater Nutzer bekommen Sie – genauer: Ihr Computer – von Ihrem Internet-Provider eine so genannte IP-Adresse zugewiesen. Diese Nummer ist nun (zeitlich befristet) die weltweit eindeutige Identität Ihres Computers – welches Internet-Angebot Sie auch während der Dauer dieser Verbindung aufrufen, immer wird diese IP-Adresse in der Statistik des angewählten Web-Servers gespeichert.

Die Provider haben nur eine begrenzte Anzahl von IP-Adressen zur Verfügung: Wenn Sie Ihre Verbindung unterbrechen, bekommt Ihre eben genutzte IP-Adresse ein anderer Nutzer; und wenn Sie sich erneut einwählen, wird Ihnen in der Regel eine andere IP-Adresse als zuvor zugewiesen. Das hat zunächst zur Folge, dass ein von Ihnen besuchter Web-Server Sie nicht als Person, sondern lediglich als Kunden des Providers XY identifizieren kann. Nur durch wiederholte Besuche, vielleicht in Verbindung mit Cookies oder mit persönlichen Daten, die Sie dort eingeben, ließe sich errechnen, dass Sie der Besucher gewesen sind. Aber das bedeutet nicht, dass Sie anonym bleiben können beziehungsweise geblieben sind. Denn die von Ihnen genutzte IP-Adresse ist mit der exakten Zeit der Nutzung durch Sie und Ihren persönlichen Daten beim Provider gespeichert, zumindest für die Abrechnungsdauer. Hat also etwa der Betreiber der von Ihnen besuchten Webseite einen triftigen Grund, Sie zu identifizieren, kann er juristisch von Ihrem Provider die entsprechenden Daten erlangen.

Wohlgemerkt: Das ist der legale Weg – illegal lassen sich Ihre Web-Spuren noch ganz anders verfolgen. Das gilt insbesondere, falls Sie sich und Ihren Computer nicht ausreichend geschützt haben sollten. Für Leute, die sich auskennen und keine Skrupel haben, lässt sich Ihr PC relativ problemlos sowohl nach Ihren Passwörtern als auch nach ganzen Dateien oder Dateistrukturen durchsuchen, und zwar ohne, dass Sie etwas davon bemerken. Die Quittung für Ihren Leichtsinns erhalten Sie aber

spätestens, wenn Sie entweder direkt attackiert werden – ob durch Werbebombardements oder durch gefährliche Software – oder wenn unter Ihrer Identität woanders Schaden angerichtet wird. Noch wichtiger als Ihr Surf-Verhalten ist aber Ihr Umgang mit der persönlichen Kommunikation. Hier ist nicht nur Ihre Privatsphäre in Gefahr – sondern auch die Ihrer Freunde und Kollegen: Jede von Ihnen verschickte E-Mail wandert unverschlüsselt im Klartext über eine Vielzahl von Internet-Servern, bis der Empfänger sie liest. Umgekehrt gilt dasselbe für jede E-Mail, die Sie empfangen. Das ist ein nicht zu unterschätzendes Risiko für die Vertraulichkeit Ihrer Mitteilungen. Zwar ist angesichts der Menge von E-Mails, die durchs Internet gepustet werden, die Wahrscheinlichkeit gering, dass ausgerechnet eine Ihrer Botschaften von unliebsamen Zeitgenossen abgegriffen wird, um ihren Inhalt zu missbrauchen – aber auszuschließen ist es keinesfalls.

Daneben sollten Sie auch die Gefahr nicht unterschätzen, dass Ihre E-Mail mit vielleicht vertraulichen Mitteilungen beim falschen Adressaten landet: Jede Mail wird auf ihrem Wege von Ihnen zum Empfänger zunächst in Pakete zerlegt. Die werden über oft unterschiedliche Zwischenstationen zum Zielservers weitergereicht, dort wieder zusammengefügt und dem Empfänger zugestellt. Dieses Verfahren führt gelegentlich dazu, dass Ihre E-Mails woanders landen als Sie es wollten – und das kann durchaus zu Problemen führen.

Schließlich bleibt noch zu erwähnen, dass es Hacker gibt, die systematisch und zum Teil hochprofessionell in Mail-Servern Nachrichten abfischen ohne jedes Interesse am Inhalt dieser E-Mails. Diese Leute sind auf der Jagd nach E-Mail-Adressen, um diese entweder selbst mit Werbung und ähnlichem Spam zuzumüllen oder um sie an einschlägige Werbefirmen zu verhökern. Sie sollten also im eigenen Interesse und aus Rücksicht auf Ihre Mail-Partner äußerst behutsam umgehen mit der Adressierung von E-Mails: Ihre Nachricht an XYZ ist für diese Leute weit weniger interessant als eine Nachricht, die Sie gleichlautend und mit offener Adressierung an viele Leute senden. Die Programme, die solchen Mail-Piraten die Adressen anderer Menschen abfischen helfen, heißen nicht ohne Grund "Harvester"; es sind Erntemaschinen, die alles abfräsen, was sie im Netz erwischen: Massen-E-Mails mit offenen Verteilern, Web-Sites und Web-Veröffentlichungen aller Art (einschließlich PDF), auf denen Mail-Adressen stehen – die "Harvester" sind eingerichtet auf die Suche nach dem für Mailadressen typischen Zeichen (@). Falls Ihre Adresse einmal in der Datenbank eines Spammers gelandet ist, bleibt sie dort für immer und ewig: Wer solche Adressen lukrativ an Spammer verkauft oder selbst zuspammt, registriert nicht, ob Sie Ihre Adresse inzwischen gesperrt oder abgemeldet haben. Auch sollten Sie keinesfalls einem Spammer mitteilen, Sie wollten aus seinem Verteiler gelöscht werden: Sie signalisieren ihm damit nur, dass Ihre Adresse noch funktioniert, das hebt für ihn deren Marktwert, vielleicht liefern Sie ihm sogar ungewollt weitere Daten über sich zur Verfeinerung Ihres Profils.

Selbstverständlich sind all diese Probleme auch der Kommunikationswirtschaft sowie den staatlichen Stellen wohlbekannt. Softwarefirmen, Provider, Internethandel oder Behörden diskutieren schon seit längerem über mögliche Systeme zum Identitäts-Management im Internet. Aber auch hier zeigen sich vielfältige Widersprüchlichkeiten, für die es bislang keine Lösungen gibt, die alle Seiten befriedigen: Einerseits fordern Politiker etwa grenzüberschreitende Standards bei der Online-Identifizierung von Nutzern; die digitale Kommunikation müsse so sicher werden wie die Papierpost. Damit könnten, heißt es, das Vertrauen in Internetgeschäfte oder Online-Verwaltungsvorgänge ("E-Government") gestärkt und Identitätsmissbrauch bekämpft werden. Andererseits befürchten Datenschützer und kritische Wissenschaftler, aber auch Teile der Internetwirtschaft, dass durch ein staatlich getragenes Identitäts-Management nur Möglichkeiten zur großflächigen Überwachung geschaffen würden.