Inkognito im Netz unterwegs

Das Münchner Unternehmen Uniscon beschäftigt sich mit der Frage, wie Daten und Persönlichkeitsrechte auch im Internet gewahrt bleiben können. Geschäftsführer Dr. Hubert Jäger hat uns erklärt, wie das funktioniert. **Interview: Sabrina Landes**

In den 90er Jahren gruselten wir uns vor Trojanern, Viren und Würmern. Mit welchen Bedrohungen müssen wir denn heute rechnen, wenn wir das Internet nutzen?

Dr. Jäger: Die erwähnten Angriffe beruhen auf sogenannter Schadsoftware. Dagegen setzt man klugerweise Antivirus-Software ein. Schadsoftware gefährdet die Integrität des Computers. Im Internet geht es aber um ganz andere Bedrohungen. Ihre Persönlichkeit wird beobachtet und ausspioniert – jeder Klick, jede Mausbewegung kann nachvollzogen werden. Spezielle Programme zeichnen auf, welche Seiten Sie besucht haben. So wird aus vielen kleinen, scheinbar belanglosen Informationen ein ganzer Mosaikteppich geknüpft. Es entstehen persönliche Profile, aus denen Firmen mehr über einen erfahren, als man selber über sich weiß. Im Internet zahlt man mit seiner Aufmerksamkeit und den persönlichen Daten. Noch kennen wir den Wechselkurs dieser Währung nicht. Wir stehen erst am Anfang einer Entwicklung.

Das klingt sehr beunruhigend. Alles, was ich im Netz tue, kann theoretisch beobachtet werden?

Dr. Jäger: Das hängt ganz von den jeweiligen Internetseiten ab. Wenn man auf einer Webseite ist, die viele Beobachtungssoftware-Tracking-Skripte, wie man sagt, aufweist, dann kann man damit gut beobachtet werden. Nur ein kleiner Prozentsatz der besuchten Webseiten enthält keine Beobachtungssoftware. Grundsätzlich beobachten aber nicht die einzelnen Webseitenbetreiber. Zur Optimierung ihrer Webseite engagieren sie Firmen, die sich mit Tracking, mit der Beobachtung, beschäftigen. Weltweit machen das mehr als hundert Firmen. Sie sammeln auf diese Weise Informationen, wie der Betreiber seine Webseite und die Kundenansprache verbessern kann, wer seine Besucher sind. Diese Informationen eignen sich dann für Werbung und sind an sich harmlos. Aber sie summieren sich zu einer Hypothek für die Zukunft. Schon jetzt hat die Sammelei Auswirkungen auf einen persönlich, auch wenn das derzeit noch harmlos erscheint: Firmen und deren Algorithmen filtern die Informationen, die sie einem zumuten wollen, schon im Voraus. Man lebt in einem Filter Bubble wie in einer Hülle eingesperrt und erhält nur noch die Informationen, die Interessengruppen, Unternehmen etc. als nützlich für einen erachten. Letztlich bedroht das die persönliche Freiheit.

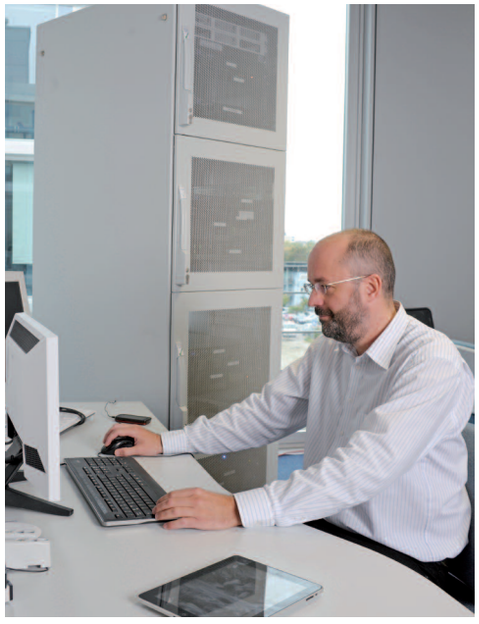
Bin ich nur beim Surfen im Internet bedroht? Was passiert beispielsweise, wenn ich mir Apps auf mein Smartphone lade?

Dr. Jäger: Ein Problem beim Herunterladen von Applikationen besteht darin, dass die heutige Hardware sehr viel Sensorik enthält. Das Gerät hat Mikrofone, es hat Orientierungssensoren, es hat noch weitere Sensoren. Applikationen können diese Informationen abgreifen und an einen zentralen Applikationsserver weitergeben. Auch solche Applikationen bedrohen die Privatsphäre und letztlich die persönliche Freiheit. Diese Möglichkeiten sind heute aber auch schon in den Browsern angelegt. Man kann bei Google beispielsweise auf ein kleines Mikrofon klicken und wenn das Mikrofon eingeschaltet ist, wird aufgenommen, was im Raum gesprochen wird.

Privat habe ich die Möglichkeit, den Rechner auszuschalten. Firmen haben diese Möglichkeit nicht. Wo sehen Sie heute die größten Sicherheitsprobleme für Firmennetzwerke?

Dr. Jäger: Die Sicherheitsverantwortlichen in Firmen sind oft verblüfft, wenn man ihnen erklärt, dass der Mitarbeiter allein durch den Internetverkehr Betriebsgeheimnisse offenlegt. Wenn beispielsweise die Entwicklungsabteilung auf Herstellerseiten nach bestimmten Produkten sucht oder in Suchmaschinen bestimmte Begriffskombinationen eingibt, dann wird diesen Onlinemarketing-Unternehmen, die die Beobachtungssoftware am Laufen haben, gezeigt, an welchen Projekten man gerade arbeitet. Man kann aus vielen kleinen, belanglos erscheinenden Informationen sehr genau herausfinden, an welchem Forschungsprojekt gearbeitet wird. Das Gleiche gilt für Mergers & Acquisitions-Abteilungen, die nachforschen, welche Firmen zugekauft und welche Betriebsteile abgestoßen werden sollen. Sehr sensible Informationen werden allein durch den Internetverkehr der

Linke Seite: Dr. Hubert Jäger ist einer der Geschäftsfürher von Uniscon. Das Unternehmen entwickelt Sicherheitslösungen für Internetnutzer.



Dr. Arnold Monitzer demonstriert, wie IDGARD funktioniert. Neben ihm stehen Prototypen der Cloud-Server. Sobald ein unerlaubter Zugriff erfolgt, werden sämtliche Daten auf diesen Rechnern automatisch gelöscht.

entsprechenden Abteilungen offenbart. So funktioniert heute Wirtschaftsspionage.

Sobald ein Mitarbeiter im Netz surft, kann er Opfer von Beobachtung werden?

Dr. Jäger: Über 70 Prozent aller Webseiten setzen aktiv Beobachtungssoftware ein. Bei jeder Recherche im Netz werden damit unbemerkt Informationen gesammelt. Unternehmen haben aber noch andere Probleme mit der Internetnutzung. Das Trennen der privaten Nutzung des Internets und der geschäftlichen ist sehr schwierig. Es gibt im Grunde für die Unternehmen nur zwei Möglichkeiten: entweder private Nutzung strikt zu verbieten oder sie völlig freizustellen. Wenn man die Nutzung völlig freistellt, hat man Haftungsrisiken in Kauf zu nehmen. Wenn man sie verbietet, muss man das sehr konsequent kontrollieren. Wir entwickeln daher auch Software, die es möglich macht, Privatnutzung und Unternehmensnutzung vernünftig zu trennen. Ein weiteres Problemfeld sind die E-Mails. Eine E-Mail ist wie eine Postkarte – kein verschlossener Brief! Der Inhalt ist für den Netzbetreiber und für vermittelnde Netzknoten lesbar.

Ihre Firma hat kürzlich den Technologiewettbewerb des Bundeswirtschaftministerium gewonnen …?

Dr. Jäger: … wir bieten einen Web-Privacy-Service, um die Privatsphäre im Netz wieder herzustellen. Damit schützen wir vor den »Big Brothern«, von denen ich gesprochen habe, ohne dass wir selber ein neuer Big Brother werden. Die Prämierung und Förderung bezieht sich auf die diesem Dienst zugrunde liegende neue Basistechnologie »Sealed Cloud«. Selbständige, Unternehmen, aber auch Privatpersonen können damit unsichere E-Mails durch versiegelten Datenaustausch ergänzen. Ein weiterer Dienst, IDGARD genannt, ermöglicht es, unerkannt zu surfen. Man ist im Internet aber nicht nur zu Recherchezwecken unterwegs, sondern meldet sich immer wieder auch mit Namen und persönlichen Daten an. In diesem Fall bietet der Privacy-Service die Möglichkeit, als Pseudonym aufzutreten. Unter Pseudonym aufzutreten ist nichts Verwerfliches. Schon 1999 wurde in den Telemediengesetzen festgeschrieben, dass es ein grundsätzliches Recht auf pseudonymes Auftreten im Internet gibt.

Wo setzt diese Software an?

Dr. Jäger: Die persönliche IP-Adresse wird durch eine pseudonyme IP-Adresse ersetzt. Header, also die Informationen, die im Seitenaufruf sofort mitgeschickt werden, werden standardisiert und die Ausspähsoftwarepakete blockiert. Die Sealed Cloud kombiniert dazu elektronische, kryptographische und mechanische Versiegelung der Cloud-Rechner, über die der Datentransfer abgewickelt wird. Wichtig ist, dass die Cloud-Rechner in Deutschland stehen – nur dann unterliegen sie nämlich deutschem Datenschutzrecht. Alle Rechner, über die wir die Daten unserer Kunden versiegeln, verfügen über diese logische und elektromechanische Zugangssteuerung. Die Daten werden verschlüsselt in die Sealed Cloud übertragen. Unsere Entwicklung, für die wir ausgezeichnet worden sind, sorgt dafür, dass nicht einmal wir den Schlüssel haben, um an die Daten unserer Kunden zu kommen. Ausschließlich der Kunde selbst verfügt über den Schlüssel.

Was geschieht, wenn Strafverfolgungsbehörden einem Verbrechen auf der Spur sind und Zugriff auf den Rechner eines Ihrer Kunden fordern?

Dr. Jäger: Nehmen wir an, jemand surft – geschützt durch IDGARD – auf eine rechtswidrige Seite. Staatsanwaltschaft oder Polizei kommen zu uns und fragen nach der IP-Adresse. Wir selber könnten da gar nichts machen, da wir Betreibersicherheit praktizieren. Wenn der Fall allerdings wichtig genug ist und eine richterliche Anweisung vorliegt, dann wird der Fall einem Notar weitergegeben, der mit seinem Schlüssel die IP-Adresse dechiffrieren kann. Auf diese Weise kann jemand, der den Dienst missbraucht hat, entdeckt werden. Das ist wichtig, um sicherzustellen, dass unser Dienst nur »weißen Schafen« dient. Einerseits garantieren wir das völlig legitime Anliegen, unter einem Pseudonym auftreten zu können, aber unser Sicherheitssystem soll kein Schutz für Kriminelle sein.

Welche Kompetenzen bringen die Mitarbeiter mit, die an der Sealed Cloud arbeiten?

Dr. Jäger: Man braucht zum Betrieb dieser Firma natürlich Menschen, die sich im Internet, aber auch mit Geschäftsmodellen im Internet, sehr gut auskennen, und wir brauchen hervorragende Sicherheits- und Software-Ingenieure. Sehr gut bewährt hat sich eine Mischung aus erfahrenen Software-Ingenieuren und ganz jungen Ingenieuren, die frisch von der Universität kommen. Die drei Gründer und Geschäftsführer von Uniscon haben ihren Überblick und Einblick durch viele Jahre Erfahrung im Kommunikations- und IT-Umfeld gewonnen – sowohl in USA als auch in Deutschland. Das und ein gutes Quantum Mut sowie Kreativität und Freiheit, die Dinge ungewöhnlich bzw. »out-of-the-box« zu denken, sind die Zutaten, um ein neues Unternehmen und, mit diesem, eine so tolle Maschine, wie die Sealed Cloud, zu konstruieren (lacht).

Herr Dr. Jäger, ich danke Ihnen für das Gespräch.

Abbildungen: Heike Geigl