Sicher und anonym surfen

So werden Sie (fast) unsichtbar im Netz

Sie wollen sicher und anonym surfen? Wir zeigen Ihnen, wie das geht – zumindest bis zu einem gewissen Grad.

Im Unternehmensumfeld sorgt ein Erhalt der Mitarbeiter-Privatsphäre dafür, Risiken von Social-Engineering-Angriffen oder Erpressung zu reduzieren. Denn je mehr kriminell motivierte Angreifer über die Schlüsselpersonen innerhalb einer Organisation in Erfahrung bringen können, desto zielgerichteter und effektiver fallen ihre Attacken aus. Deswegen sollten die Aufklärung und Schulung der Mitarbeiter darüber, wie diese ihre Privatsphäre bestmöglich schützen, grundlegender Bestandteil jedes Security-Awareness-Programms sein. Dabei können Sie konkrete, spezifische Maßnahmen und Vorkehrungen treffen, um Ihre Privatsphäre – und die Ihrer Mitarbeiter – zu schützen. Das kostet Sie Energie und Zeit – und erfordert darüber hinaus auch ein wenig technisches Knowhow. Wir sagen Ihnen, wie Sie sich in acht Schritten (fast) anonym und sicher durch das weltweite Netz bewegen. Dabei noch ein Hinweis: Privatsphäre und Anonymität sind nicht synonym. Machen Sie sich keine Illusionen – einhundertprozentige Anonymität im Netz gibt es in der digitalisierten Welt nicht. Alles, was Sie tun können ist, Ihre Privatsphäre so gut wie möglich zu schützen.

Signal: Verschlüsselte Kommunikation

Signal (*www.signal.org/de/*) ist eine Messaging App für verschlüsselte Kommunikation. Text- und Sprachnachrichten können hiermit genauso gesendet und empfangen werden wie Video- und Audioanrufe. Dabei fühlt sich Signal genauso an wie jede andere Messaging App – nutzt aber Verschlüsselung, die (zumindest nach aktuellem Stand) nicht einmal die NSA knacken kann. Was die Metadaten angeht: Jeder Widersacher kann auf Netzwerkebene sehen, dass Sie Signal nutzen. Wenn es sich bei diesen Widersachern um Geheimdienste handelt, können diese sehr wahrscheinlich auch ermitteln, mit wem, wann und wie lange sie kommunizieren.

Die Macher von Signal sind sich dieser technischen Limitationen durchaus bewusst und forschen an Mitteln und Wegen, um das Problem zu lösen. Bislang bleibt eine Metadaten-resistente Kommunikation allerdings ein schöner Traum. Nichtsdestotrotz ist Signal die sicherste und benutzerfreundlichste Messaging App, die derzeit zur Verfügung steht und bietet deutlich mehr Privatsphäre als jedes ihrer populäreren Pendants. Anonym kommunizieren Sie jedoch auch mit Signal nicht – wobei das, wie bereits erwähnt, heutzutage generell kaum möglich ist.

Tor: Anonymität beim Surfen im Netz

Das größte und effektivste Metadaten-resistente Softwareprojekt ist immer noch Tor (*www.torproject.org*). Doch auch hier bestehen technische Limitationen, die bislang trotz ausufernder Security-Forschung noch nicht beseitigt werden konnten. Tor ist für Webbrowsing mit niedriger Latenz optimiert und unterstützt lediglich TCP. Beim Versuch, diverse bekannte Webseiten aufzurufen, wird Tor zudem nicht funktionieren, da die meisten dieser Seiten den Zugang via Tor grundsätzlich blockieren.

Zwar garantiert auch Tor keine hundertprozentige Anonymität beim Surfen im Netz – aber es ist in dieser Hinsicht das beste verfügbare Werkzeug. Wie so viele Dinge im Leben ist auch das Tor-Projekt ein zweischneidiges Schwert: Einerseits wird es von Journalisten und Bloggern genutzt, um anonym zu recherchieren oder zu publizieren, andererseits wird es auch von kriminellen Hackern für diverse böswillige Zwecke eingesetzt. Sollten Sie mal wieder jemandem begegnen, der sich über das „böse Darkweb" beschwert, gegen das endlich jemand etwas unternehmen sollte – erinnern Sie diesen Jemand gerne daran, dass Bankräuber nach getaner „Arbeit" auch vom Tatort flüchten, jedoch niemand auf die Idee kommt, Autos und Straßen verbieten zu wollen.

Vor allem für die mobile Nutzung sollten Sie auf den Tor-Browser setzen. Es gibt eine offizielle Android-App (*https://play.google.com/store/apps/details?id=org.torproject.android*) und eine vom Tor-Projekt autorisierte, aber inoffizielle App für iOS.

VPNs bieten keine Anonymität

Virtual Private Networks bieten keine Anonymität. Weil aber jeder VPNs in einem Artikel wie diesem erwartet, räumen wir an dieser Stelle direkt mit diesem Mythos auf. Alles, was ein VPN tut, ist, den Traffic von Ihrem Internet-Anbieter – oder, falls Sie unterwegs sind, dem Hotel- oder Flughafen-WiFi – über einen anderen Server zu leiten – allerdings verschlüsselt. So gibt es viele legitime Gründe, VPNs zu nutzen – Anonymität gehört jedoch nicht dazu. Nicht einmal ansatzweise. Im Gegensatz zu Tor – das Ihren Traffic über drei verschiedene, im weltweiten Netz verteilte Knotenpunkte leitet und es potenziellen Widersachern dadurch schwer (wenn auch nicht unmöglich) macht, zu sehen, was Sie da tun – tunnelt ein Virtual Private Network lediglich den Verkehr. Nutzen Sie dabei einen VPN-Provider, ist dieser also in der Lage, Ihre Aktivitäten jederzeit nachzuvollziehen. Das bedeutet auf der anderen Seite, dass böswillige oder staatliche Akteure, die sich Zugang zu den VPN-Servern verschaffen – sei es per Hack oder Gerichtsbeschluss – das ebenso gut können.

Damit wir uns richtig verstehen: VPNs sind eine gute Sache. Nutzen Sie sie, wann immer Sie können. Erwarten Sie aber keine Anonymität.

Zero Knowledge Services

Google kann jede E-Mail, die Sie schreiben und erhalten, einsehen. Microsoft 365 scannt jede Zeile, die Sie verfassen. DropBox analysiert jeden Ihrer Uploads. Jedes dieser Unternehmen – und viele andere – sind PRISM Provider, kooperieren im Rahmen von Massenüberwachungsprogrammen mit staatlichen Akteuren. Wenn Sie die Services dieser Unternehmen nutzen, fällt Privatsphäre also grundsätzlich aus.

Gegensteuern könnten Sie natürlich, indem Sie Ihre Daten vor dem Upload verschlüsseln. Dazu könnten Sie sich zum Beispiel Kenntnisse im Umgang mit PGP aneignen. Oder Sie entscheiden sich für Provider, die sich dem Zero-Knowledge-Prinzip verpflichten. Dabei können Sie sich allerdings auch nie sicher sein, dass entsprechende staatliche Akteure auch in diesen Fällen über entsprechende Hintertürchen verfügen.

Mögliche Alternativen bieten beispielsweise Firmen wie **SpiderOak** (*https://spideroak.com*) in den USA, die Zero Knowledge File Storage anbieten oder der Schweizer Anbieter **Protonmail** (*https://protonmail.com*), der damit wirbt, dass es für Dritte rein mathematisch unmöglich sei, die Inhalte Ihrer E-Mails einzusehen. Wir wollen Ihnen keinen der genannten Services empfehlen – es handelt sich lediglich um Beispiele für Zero-Knowledge-Anbieter und entbindet Sie nicht von der Pflicht, vor der Nutzung solcher Services Hintergrundrecherchen über die Anbieter zu betreiben.

Privatsphäre in sozialen Netzwerken

Online-Privatsphäre heißt auch, dass Sie selbst darüber entscheiden, was Sie mit der Welt teilen wollen und was nicht. Wenn sich in Ihrem (Arbeits-)Leben Dinge abspielen, die nicht dazu geeignet sind, mit einer breiten Öffentlichkeit geteilt zu werden, sollten Sie folglich auch vermeiden, diese über Social-Media-Plattformen zu verbreiten.

Dieser Themenkomplex ist ohne Zweifel auch eine Generationenfrage: Während ältere Menschen im Regelfall beim Gedanken daran erschaudern, ihr Privatleben auf Social-Media-Kanälen mit der Welt zu teilen, hält das Gros der Generation Smartphone es für völlig normal, jeden Aspekt ihres Lebens „share-bar" zu machen. Sie sollten vor jedem Posting auf sozialen Kanälen das große Ganze im Auge behalten: Ein einzelner Post mag unbedeutend erscheinen – aber tut er das in Kombination mit den übrigen verfügbaren Informationen über Ihr Leben immer noch? Überlegen Sie sich vor dem Klick auf den Button ganz genau, welches Gesamtbild Ihr Beitrag erzeugen könnte.

App-Berechtigungen: Weniger ist mehr

Mobile Apps – egal ob auf Android- oder iOS-Geräten – tendieren generell dazu, weit mehr Berechtigungen als nötig „einzufordern". Die Folge ist, dass persönliche Daten ganz regelmäßig extrahiert und an den App-Hersteller übertragen werden. Braucht jede App wirklich Zugriff auf das Mikrofon Ihres Smartphones, Ihren Aufenthaltsort oder Ihr Adressbuch? Auch wenn es sowohl unter Android als auch unter iOS etwas umständlich und kompliziert ist: Wühlen Sie sich durch die entsprechenden Einstellungen und schalten Sie unnötige App-Berechtigungen ganz konsequent ab. Dabei gilt: Lieber eine Berechtigung zu viel als zu wenig verwehren.

AdBlocker: Schutz vor Werbe-Trackern

Heutiges Online Advertising ist mit dem der frühen Online-Jahre nicht mehr zu vergleichen: Statt einer Anzeige für alle Nutzer überwachen heutige Advertising-Netzwerke Ihr Nutzungsverhalten und liefern gezielt auf Ihre Interessen zugeschnittene Werbeanzeigen aus. Das ist das maßgebliche Geschäftsmodell der Silicon-Valley-Giganten. Google und Facebook etwa verfolgen jeden Ihrer Schritte im World Wide Web – auch wenn Sie keinen Account dort haben, beziehungsweise nicht eingeloggt sind.

Die Installation eines AdBlockers ist dagegen zwar auch kein Allheilmittel – aber ein Holzschwert ist immer noch besser, als gar keine Waffe zur Verteidigung am Start zu haben. Es gibt einige Webbrowser, die Werbeanzeigen und Tracker standardmäßig blockieren – auch Browser-Erweiterungen stehen zu diesem Zweck zur Verfügung. Eine andere Möglichkeit: Sie nehmen den DNS-Requests der Werbenetzwerke bereits auf lokalem Router-Level den Wind aus den Segeln.

J.M. Porup und Florian Maier

J.M. Porup schreibt als Senior Security Reporter für unsere US-Schwesterpublikation CSO Online. Er beschäftigt sich seit dem Jahr 2002 mit dem Themenbereich IT Security.

Florian Maier beschäftigt sich mit vielen Themen rund um Technologie und Management. Daneben betätigt er sich auch in sozialen Netzen.