Der Feind in meinem Netz

SPIONAGE | Amerikanische und britische Geheimdienste werten in ungeahntem Ausmaß deutsche Mails, Telefongespräche und Kurznachrichten aus. Unternehmen fürchten bereits eine neue Qualität der Wirtschaftsspionage. Wo die Schnüffler ansetzen und mit welchen Techniken Sie Ihre Daten schützen können.

Noch tippe ich allein. Ich sitze beim Frühstück und schreibe den Einstieg für diesen Text auf meinem privaten Laptop. Aber in wenigen Minuten schon werde ich einige Hundert Leser haben. Dann schicke ich den Text via Google-Mail an mein elektronisches Postfach im Büro. Unterwegs werden diese Zeilen dann von britischen Spionen, vom US-Geheimdienst NSA oder von noch viel unangenehmeren Zeitgenossen gescannt.

Für den Versand zerlegt mein Rechner die formulierten Gedanken in kleine Datenpakete, leitet sie über armdicke Leitungen durch den Atlantik zu Googles Serverparks in die USA und von dort schließlich an meinen dienstlichen Mail-Account in Düsseldorf. In Sekundenbruchteilen rast der Text Tausende Kilometer durchs Netz. Und weil die Mail unverschlüsselt ist, können Geheimdienste und Hacker aus den dunkelsten Winkeln unserer Welt mitlesen.

Das ist nicht neu. Normale E-Mails schützen ihren Inhalt etwa so gut wie Postkarten unsere Urlaubsgrüße. Viele Nutzer denken aber, dass ihre Daten so unbedeutend seien, dass die Datenschnipsel im globalen Nachrichtenstrom untergehen.

Lange war das auch so. Doch wir stehen am Beginn eines neuen Datenzeitalters. So wie Menschen beim Ausatmen CO_2 abgeben, produzieren wir ständig Bits und Bytes: mit unseren Smartphones, bei Internet-Recherchen, ja, sogar mit Restaurantbesuchen. Diese Informationsflut zu speichern ist heute nahezu kostenlos.

Mithilfe von Analyseprogrammen lassen sich aus diesem Datenmeer Verhaltensmuster herauslesen – und Entscheidungen von Menschen und Unternehmen vorhersagen. Handyprovider etwa können anhand der Positionsdaten ihrer Kunden auf deren Hobbys, sozialen Status oder beruflichen Erfolg schließen.

Weil es so billig geworden ist, Daten abzufangen und zu analysieren, ist die Verlockung so groß, dies auch zu tun – auch für Geheimdienste: Großbritannien fängt offenbar in ungeahntem Ausmaß Internet-Daten von Unternehmen und Privatleuten ab – darunter E-Mails, Kurznachrichten und Telefonanrufe, auch aus Deutschland.

Viele Programme haben ab Werk einen Staatstrojaner eingebaut

Mit großer Wahrscheinlichkeit gerät auch dieser Text in die Fangnetze des Tempora genannten Projekts der Briten. Um an die Daten zu gelangen, zapfen sie Untersee-Datenkabel an – die Schlagadern unserer Wissensgesellschaft, die Kontinente und Kulturen miteinander verbinden.

Eine dieser Adern heißt TAT-14. Sie transportiert Daten von Europa in die USA. Bevor sie in den Atlantik taucht, führt sie von Deutschland aber zunächst nach Bude im englischen Cornwall. Dort fangen die Schnüffler des britischen Geheimdienstes GCHQ laut der Tageszeitung „Guardian“ noch mehr Daten ab als ihre US-Kollegen im Rahmen des Spionageprojekts Prism. Ohne demokratische Kontrolle, ohne eine öffentliche Debatte und ohne begründeten Verdacht.

ANGST VOR GEHEIMNISVERRAT

Es trifft jeden. Denn es geht nicht um die gezielte Beschattung Verdächtiger. Auf einmal sind alle verdächtig: Die Briten sammeln einfach so viele Daten wie möglich. „Über Jahre haben sich Geheimdienste fremder Staaten hemmungslos an den Daten deutscher Bürger bedient“, klagt der Bundesverband IT-Mittelstand.

Zu Recht wächst mit dieser Erkenntnis auch die Sorge vor einer neuen Qualität der Wirtschaftsspionage.

Denn sowohl bei Prism als auch bei Tempora kooperieren die Geheimdienste offenbar mit Privatunternehmen: mit Telekommunikationsanbietern, die Zugang zu ihren Leitungen gewähren, mit sozialen Netzwerken, die die Kommunikation ihrer Nutzer offenlegen, und mit Softwareherstellern, die vorab über Sicherheitslücken ihrer Programme informieren. Im Tausch, zitiert die Nachrichtenagentur Bloomberg Insider, erhalten die Unternehmen „nützliche Daten“.

Kenner der Szene wundert das nicht. Immerhin hat Großbritannien schon vor Jahren eingeräumt, bei Spionage gehe es nicht nur um Sicherheit, sondern auch um nationale Prosperität. Die deutsche Regierung, für die das Internet ohnehin „Neuland“ ist, ahnte von alledem bislang nichts.

Vielleicht hat die ganze Debatte aber auch ihr Gutes: Vielleicht erhält das Thema IT-Sicherheit endlich die Aufmerksamkeit, die es braucht. Denn der Umgang vieler Privatleu-

FOTO: PR

te und Unternehmen mit dem Internet ist grenzenlos naiv: „Wenn wir Unternehmen auf Sicherheitslücken scannen, gibt es fast keinen Fall, bei dem wir nicht auf ein oder mehrere Schadprogramme stoßen – von Trojanern bis zu übernommenen Datenbanken“, sagt Matthias Rosche, Mitglied der Geschäftsleitung beim IT-Sicherheitsdienstleister Integralis. Inzwischen bietet er manchen Kunden sogar die Wette an, den Sicherheitscheck gratis zu machen, falls sein Team keine gravierende Lücke findet.

Das größte Risiko sind dabei die Übertragungsnetze, die auch die britischen Spione anzapfen. Sie lassen sich durch verschlüsselte Verbindungen sichern. Gleiches gilt für Daten, die im Netz bei sogenannten Cloud-Diensten wie Dropbox oder Microsoft Skydrive liegen.

Auch sie sollten „vor dem Versand verschlüsselt werden“, empfiehlt Sebastian Schreiber Hackerabwehrexperte und Gründer des Tübinger IT-Security-Unternehmens SySS. Schwieriger sei die Lage bei Computern und Smartphones. Windows, Android und iOS lassen sich kaum schützen. „Die Betriebssysteme“, sagt Schreiber, „haben den Staatstrojaner quasi ab Werk eingebaut.“ Sicherer sei das Betriebssystem Linux – allerdings für viele Unternehmen, die Standardsoftware einsetzen, keine Alternative zu Windows oder Apples Mac OS X: „Da hilft dann nur Verschlüsselung der Daten und ein guter Zugriffsschutz.“

Wie Sie Ihre Daten schützen und sicherer kommunizieren können, lesen Sie auf den nächsten Seiten. »

sebastian.matthes@wiwo.de

Platten-Sperre

Wer verhindern will, dass Spionagesoftware die Passworteingabe für die verschlüsselte Festplatte aufzeichnet, sollte externe Speicher mit eigener Entsperrtechnik einsetzen – wie die **DataLocker-**Festplatte von Origin. Das Modell Enterprise 2.0 besitzt ein Tastenfeld für die Code-Eingabe und ist von der US-Technologiebehörde NIST unter anderem für den militärischen Einsatz zertifiziert.
Preis: ab 390 Euro

Passwörter-Buch

Wer kann sich noch die Passwörter merken, die er auf Hunderten Web-Seiten eingibt? Der **MyIDkey** des US-Start-ups Arkami hilft da weiter: Der USB-Stick, der sich nur über den eingebauten Fingerabdruck-Scanner aktivieren lässt, merkt sich sämtliche Benutzernamen und Passwörter, die der Nutzer in Web-Seiten eingibt – und füllt die Zugangsdaten bereits besuchter Web-Seiten automatisch in die vorgegebenen Eingabefelder ein. Via Bluetooth-Funk funktioniert das auch mit Smartphones.
Preis: 170 Dollar

Merkel-Berry

Private Daten und Unternehmensinformationen hält die Spezialversion des Blackberry Z10 vom deutschen Sicherheitsspezialisten Secusmart strikt getrennt. Möglich macht das, neben Sicherungen im Betriebssystem, die Zusatzverschlüsselung per Smartcard, die der Technik **Secusuite** gerade die Freigabe als Regierungshandy beschert hat.
Preis: 2500 Euro

Sprech-Stelle

Abhörsicher telefonieren, unabhängig von Handy oder Notebook, das ermöglicht das Sprachverschlüsselungssystem **Topsec mobile** des Berliner Spezialisten Rohde&Schwarz SIT. Die Krypto-Box mit eigenem Headset wird per Bluetooth mit internetfähigen Handys oder Computern gekoppelt und baut hochverschlüsselte Sprachverbindungen zu baugleichen Topsec-Modulen auf. **Preis: 1260 Euro**

Abdruck-Analyst

Nicht ganz so sicher wie ein komplexes Passwort, aber deutlich komfortabler – und allemal besser als kein Zugriffscode: Das sind Fingerabdruckleser, die viele Business-Notebooks eingebaut haben, wie etwa das **Thinkpad X1 Carbon** von Lenovo.
Preis: 1470 Euro

Post-Geheimnis

Mit den Verschlüsselungsverfahren PGP und S/Mime gibt es wirksame Technologien, um elektronische Post gegen unerwünschte Mitleser zu sichern. Nur ist die Konfiguration gerade für Laien teils recht aufwendig. Einfacher und für den Unternehmenseinsatz geeignet sind Programme wie **gpg4o** des Softwarehauses Giegerich&Partner. Das Paket gibt's als Erweiterung für Microsofts Outlook 2010 und 2013.
Preis: ab 94 Euro

Blick-Fänger

Längst nicht immer kommen Spione übers Netz. Oft genug – etwa im Zug oder am Flughafen – lesen sie einfach von der Seite mit, was Geschäftsleute auf dem Laptop-Display anschauen. Abhilfe schafft der **Vikuiti** Blickschutzfilter von 3M, der nur direkt von vorne freie Sicht aufs Display von Smartphone, Tablet oder PC ermöglicht. Neugierige Späher von der Seite sehen dagegen Schwarz. **Preis: ab 30 Euro**

Gesichts-Login

Auch das eigene Gesicht kann den PC-Zugriff freigeben. Programme wie **KeyLemon** des gleichnamigen Schweizer Unternehmens nutzen dafür die in fast allen neuen Laptops integrierte Webcam. Die Software erkennt den rechtmäßigen Nutzer an dessen Gesichtsproportionen.
Experten warnen aber grundsätzlich, dass sich derartige biometrische Sicherungen leichter knacken lassen als gute Passwörter.
Preis: kostenlos

Spion-Späher

WLAN-Kameras als Wächter für daheim oder im Büro sind Bestseller. Dumm nur, dass viele Nutzer die Bilderströme offen ins Netz stellen und damit fast jedem Einblick auf ihren Schreibtisch ermöglichen. Die Überwachungskamera **In.Sight** von Philips dagegen verschlüsselt die Aufnahmen, bevor sie die per WLAN und Internet zur passenden Smartphone-App überspielt. **Preis: 130 Euro**

Bundes-Fon

Den Komfort eines modernen Smartphones, gepaart mit vom Bundesamt für Sicherheit in der Informationstechnik zertifizierten Sicherheitsfunktionen, das bietet auch die **Simko3**-Softwareplattform. T-Systems und der Softwareanbieter Trust2Core haben sie gemeinsam entwickelt und vertreiben sie unter anderem für Galaxy-Handys von Samsung.
Preis: ab 1700 Euro

Funk-Fresser

Smartphones sind nicht nur Datenspeicher ersten Ranges, sondern auch ein Paradies für Datendiebe: Sie lassen sich per GPS orten oder über WLAN-Funk attackieren. Spitzel-Apps täuschen sogar vor, dass das Telefon ausgeschaltet ist, und durchsuchen das Gerät dann heimlich. Die Handytasche **Rapp It Up** unterbindet solche Zugriffe rustikal: Ein eingenähtes Drahtgitter soll jede Funkverbindung unterbinden.
Preis: 37,50 Dollar

Software-Safe

Informationen gegen fremde Zugriffe zu schützen ist viel leichter als gedacht, denn bei den Profi-Versionen von Windows liefert Microsoft die Festplattenverschlüsselung **Bitlocker** gleich mit. Auf Mausklick wandern die Daten in den Software-Safe. Neue Versionen des Apple-Betriebssystems Mac OS X kommen mit einer ähnlichen Software namens **Filevault.** Sicherheitsexperten vermuten, dass die Hersteller Schlupflöcher für US-Geheimdienste offen lassen, doch Wirtschaftsspione oder Kriminelle müssen draußen bleiben. **Preis: Teil des Betriebssystems**

FOTOS: PR

Geheimnis-Träger

Die Smartphone-App **oneSafe** verschlüsselt Zugangscodes: Benutzernamen und Passwörter, Kreditkarten- und Pin-Nummern, Texte oder Fotos. Via Apples Online-Service iCloud lassen sich die Daten zwischen iPhones, iPads und Mac-Rechnern synchronisieren. Um die App zu öffnen, gibt der Nutzer ein Passwort ein. Wer ein falsches Passwort eingibt, den fotografiert die Frontkamera des Handys.
Preis: 5,49 Euro

Zweit-Schlüssel

Doppelt hält besser – das gilt auch für die Absicherung von Rechnern und Datennetzen. Experten empfehlen daher, bei der Anmeldung am PC oder für den Zugriff auf gesicherte Datenbanken eine Kombination aus Passwort und digitalem Sicherheitsmedium zu nutzen. Der **SecurID 800 Hybrid Authenticator** des US-Sicherheitsunternehmens RSA Security speichert solche Signaturen und dient so bei der sicheren Anmeldung als zweite Sicherheitsstufe. **Preis: 60 Dollar**

Daten-Tunnel

Sicherheitsexperten staunen immer wieder, wie schlecht Unternehmen ihre Netze absichern. Der IT-Spezialist Lancom Systems bietet jetzt als erster Anbieter Übertragungsrechner an, deren Verschlüsselung vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert ist; wie den Router **1781A-4G CC.** Über so gesicherte Daten-Tunnel dürfen nun selbst Behörden und Militärs Dokumente abhörsicher austauschen und Telefonate führen. **Preis: 1100 Euro**

Wolken-Schloss

Was nützt die sicherste Internet-Verbindung, wenn sensible Daten auf den Cloud-Servern von Google bis Microsoft unverschlüsselt für Hacker oder Geheimdienste erreichbar sind? Die Software **Boxcryptor** des Augsburger Startups Secomba ändert das, indem sie Dokumente vor der Ablage im Netz verschlüsselt. Beim Öffnen auf PC, Tablet oder Smartphone werden die Dateien wieder entschlüsselt.
Preis: Basisversion gratis

Sicherheits-Glas

Strategiemeetings, vertrauliche Projektbesprechungen: In vielen Situationen sind Zuschauer unerwünscht. Nun lassen sich ganze Fensterfronten, etwa die Glaswände von Konferenzräumen, blitzschnell gegen neugierige Blicke absichern: Die Klebefolie **Sonte** wird per WLAN-Funk vom Smartphone aktiviert und verwandelt sie in Milchglasscheiben. **Preis: 280 Dollar**

Taschen-Tresor

Das **iWallet** des gleichnamigen US-Startups besitzt ein Karbongehäuse, das Geld, Kreditkarten oder Zugangsausweise fest umschließt. Wer es öffnen will, muss es über den eingebauten Fingerabdruck-Sensor öffnen. **Preis: ab 459 Dollar**

FOTOS: PR

Redaktion: thomas.kuhn@wiwo.de, andreas menn, patrick schultz