Leichtes Spiel für Spione
Cloud & Co. als Gefahrenquellen

Marko Rogge hat als ehemaliger Hacker ein tiefes Verständnis für die Manipulationsmöglichkeiten moderner Technik. Anders als immer wieder dargestellt, sind weder die Cloud noch das Smartphone harmlose Begleiter des beruflichen oder privaten Lebens. Sein Wissen um die Verwundbarkeit dieser Technik stellt Marko Rogge mit seinem Unternehmen ›Omega Defense‹ allen Unternehmen zur Verfügung, die kompetenten Rat in Sachen Datenschutz benötigen.

Sehr geehrter Herr Rogge, Smartphones entwickeln sich zum Renner. Massenweise werden kostenlose Apps darauf installiert, die sich, gut versteckt in den (rasch weggeklickten) Allgemeinen Geschäftsbedingungen, weitreichenden Zugriff auf Funktionen und Daten des Smartphones einräumen lassen. Haben Sie Beispiele, welche Apps besonders lange elektronische Finger machen?

Marko Rogge: Es ist eine Gratwanderung zwischen Nutzbarkeit und Sammelwut an Daten der Anwender. Beispiel hier wären Messengerdienste wie ›Whatsapp‹, die untransparent Userdaten transferieren und das vollständige Adressbuch auslesen, ohne das andere, unbeteiligte User sich dagegen wehren können. Beispiel: Sie haben Whatsapp und ich nicht, jedoch ist meine Nummer bei Ihnen hinterlegt und so gelangt meine Nummer ebenfalls zum Betreiber von Whatsapp. Ein anderes Beispiel wäre hier die App von TV Spielfilm, die einen vollen Zugriff auf die Telefonfunktion (Android) gewährt haben will. Der Sinn für den Zugriff bei einer TV-App ist schlicht nicht einsehbar.

Was machen diese Apps, wovon der Nutzer nichts mitbekommt?

Rogge: Wie im Beispiel voran beschrieben, wird das Adressbuch abgeglichen oder mittels Zugriff auf die Telefonfunktion könnte ein Smartphone zu einer Wanze umfunktioniert werden, ohne dass der User dies mitbekommt.

Ist es generell so, dass bei kostenlosen Apps die Gefahr am größten ist, sich einen Schnüffler einzufangen?

Rogge: Das kann ich so nicht bestätigen. Erst kürzlich hat Google seine Zahlungen zurückgestellt, um betrügerische Entwickler abzuschrecken.

Warum wird zum Schutz des Bürgers nicht von Haus

Marko Rogge ist ein ausgewiesener Fachmann, wenn es um Datensicherheit geht. Den tiefen Einblick in die Welt der EDV erarbeitete er sich als Hacker. Seine Erkenntnisse sollten sich alle Unternehmen zu Eigen machen, die mit sensiblen Daten umgehen. Sein Expertenwissen gibt Marko Rogge auch auf großen Veranstaltungen weiter , die sich eines regen Zuspruchs erfreuen.

aus ein Gesetz erlassen, das solche Umtriebe stoppt? In jedem Vertrag sind überraschende Klauseln, mit denen man nicht rechnen muss, unwirksam. Bei Apps, deren Funktion und Programmzweck keinen Zugriff auf Daten nötig macht, soll dies anders sein?

Rogge: Persönlich bin ich der Meinung, dass man gerade im dem Bereich doch auch auf die Mündigkeit der Benutzer achten sollte. Es gibt hinreichend Beispiele dafür, dass etwa Banking-Trojaner, die über Smartphones eingeschleust werden, Schaden anrichten und das über eine installierte App, die eben nicht gleich als schadhaft erkannt wurde. Dahin gehend, um sich des Betrugs zu wehren, reichen aus meiner Sicht die Gesetze derzeit aus.

Was ist ihr Vorschlag, um schon vor dem Herunterladen zu erkennen, was die APP für Rechte haben will? Schließlich ist es hanebüchen, dass etwa Programmzeitschriften-Apps Zugriff auf die Telefonfunktion des Geräts wünschen. Was geht es eine Programmzeitschrift an, wer angerufen wird? Eine gesetzliche Offenlegungspflicht in informativer Form würde wohl viele Nutzer vor der unbedachten Installation derartiger Software abhalten.

Rogge: Interessanterweise wird dies bei Android vollständig unterstützt und auch dem User angezeigt – er muss es nur noch lesen. Eine Weigerung, die noch so tolle App dann zu installieren, sollte vom User kommen.

Vielfach sind Smartphones kompliziert zu bedienen. Technisch wäre es doch sicher kein Problem, einen Button einzubauen, der jeden unerwünschten Zugriff einer App auf Daten unterbindet. Warum gehen Hersteller diesen Weg nicht, um ihre Produkte sicherer zu machen?

Rogge: Die Smartphones werden immer komplexer in der Bedienung und trotz Sicherheitsbedenken der Experten, wollen die Anwender genau das haben. Es gibt hinreichend Möglichkeiten sich zu schützen, man muss diese auch nutzen. Das Sicherheitskonzept von iOS (iPhone) ist durchdacht und hilft beim Verschlüsseln der Daten. Genutzt wird es immer noch nicht hinreichend. Auch gibt es Software, die entsprechende Zugriffe von Apps überprüfen und notfalls unterbinden. Leider sind dafür oft Expertenkenntnisse erforderlich, sodass der normale Anwender davon unberührt bleibt.

Immer wieder ist davon zu hören, dass in Fernost gefertigte Chips versteckte Funktionen enthalten, die sich bestens dafür eignen, einen PC oder ein Smartphone auch ohne entsprechendes Programm in ein Spionagewerkzeug zu verwandeln. Gibt es da konkrete Beispiele?

Rogge: Ich persönlich möchte mich dazu nicht öffentlich äußern. Gebe allerdings zu bedenken, dass vor vielen Jahren bereits eine kontrollierbare Plattform namens ›Palladium‹ geschaffen wurde. Diese ist dann durch TCPA (jetzt TCG) erweitert worden. Daher gibt es offiziell seitens der Hersteller bereits diese Möglichkeiten. Auch wurden immer wieder Stimmen laut, die chinesischen Herstellern wie Huawei und ZTE solche Möglichkeiten unterstellen und teilweise auch nachweisen konnten.

Es wurde bekannt, dass Regierungsmitglieder spezielle Handys nutzen, die nicht so leicht abzuhören sind. Wie arbeitet diese Technik?

Rogge: Da bekanntlich der momentan genutzte Mobilfunkstandard als unsicher gilt, nutzen viele Regierungsmitglieder Verschlüsselungstechnologien. Es gibt Software, die auf das SRTP- oder ZRTP-Protokoll aufbauen und so verschlüsselte Gespräche von einem zum anderen Teilnehmer ermöglichen. Damit ist das Abhören durch das Netz zunächst einmal mehr als erschwert. Aber auch Hardware gibt es, die man auch als Unternehmer erwerben kann. Als Beispiel sei das Unternehmen Rhode & Schwarz genannt, das entsprechende Technik anbietet.

Warum ist diese Technik nicht Standard, sodass jeder Bürger unbesorgt ein Smartphone nutzen kann?

Rogge: Für die meisten Anwender ist der Standard der, dass er ein Smartphone mit allen Annehmlichkeiten nutzen will. Einhergehend damit verliert sich allerdings eben auch die Sicherheit, die billigend in Kauf genommen wird.

Auch die Navigations-App von Navigon ist ins Gerede gekommen, heimlich Daten auszuspionieren. Was wissen Sie darüber?

Rogge: Leider habe ich darüber keine konkreten Informationen, außer denen, die in den Medien lesbar waren. Abgesehen davon hat auch Apple mit seinen iPhones Positionsdaten gesammelt und sich selbst zugesendet.

Selbst Windows und Outlook stehen im Verdacht, „nach Haus" zu rufen. Gibt es dazu Schutzmaßnahmen?

Rogge: Kein leichtes Thema. Ich denke, dass hier betrachtet werden muss, ob dem in der Tat so ist und wenn dem so ist, wird ein Berater sicherlich dahin gehend helfen können, entsprechende Lösungen zu beschaffen, die den ausgehenden Datentraffic genau analysieren und notfalls unterbinden. Bei einigen Systemen dürfte dies wegen der „Updatemechanismen" durchaus schwerer werden.

Eignet sich Linux nicht besser für sicherheitskritische Arbeitsumgebungen?

Rogge: Linux ist per Default nicht als sicherer zu betrachten. Server arbeiten überwiegend auf Basis von Linux und sind ein sehr begehrtes Angriffsziel. Fast alle Firewallsysteme basieren auf dem Linux-Kernel und arbeiten durchaus sicher und effizient. Für den Arbeitsalltag wäre selbst ich nicht sicher, ob ich Linux empfehlen würde, wenngleich ich durchaus ein Fan von Linux bin.

Welches Betriebssystem für PCs beziehungsweise für Smartphones würden Sie niemals einsetzen, da es zu unsicher für Daten ist?

Rogge: »Sagen Sie niemals nie.« Android, iOS oder auch Windows können durchaus sicher betrieben werden.

1998 wurde der Berliner Hacker ›Tron‹ tot aufgefunden. Er hatte in seiner Diplomarbeit an einem absolut abhörsicheren ISDN-Telefon gearbeitet und wurde eines Tages erhängt an einem Baum gefunden. Jeder, der Tron kannte, äußert, dass es sich hier um Mord handelt. Ist diese Tat eine Bestätigung dafür, dass verschlüsselte Handygespräche für normale Unternehmen und Nutzer unerwünscht sind?

Rogge: Ein schweres Thema, aber eben genau aus dem Grund nicht undenkbar. Man beachte in diesem Zusammenhang vielleicht auch, dass sehr wenig Verschlüsselungstechnologie aus Deutschland kommt. Aber

ob die genannte These wirklich zutrifft, möchte ich nicht sagen. Verschlüsselung ist einsetzbar und sollte genutzt werden. Nicht jeder, der so etwas entwickelt hat, hing danach an einem Baum.

Mittlerweile werden viele Telefonate über das Internet geführt. Vielfach ohne Wissen der Kunden. Insbesondere Dienste wie ›Skype‹ werden hier genutzt. Skype ist kostenlos, doch hat niemand etwas zu verschenken. Was ist das Geschäftsmodell dieses Unternehmens und wie sicher sind hier die Daten beziehungsweise über Skype geführte Gespräche?

Rogge: Ich persönlich habe mich nie mit dem Geschäftsmodell von Skype oder dem von Microsoft auseinander gesetzt, um zu erfahren, wie man damit Geld verdienen will außer, dass man darüber auch normale Festnetz- und Mobilnetznummern erreichen kann und dies als Bezahldienst. Dass hier in Gespräche möglicherweise reingehört werden kann, ist sehr wahrscheinlich. Offiziell wird so etwas stetig dementiert. Allerdings gibt es Software, die genau dies bestätigt. Unternehmenskunden sollten auf andere Lösungen setzen und damit nicht sparen wollen. Microsoft integriert Skype immer mehr in Office-Lösungen, was für die Unternehmenskommunikation durchaus kritisch betrachtet werden kann, sofern man Skype dafür nutzt.

Behörden spielen auf ihre neu angeschafften Laptops alle nötigen Programme auf und versiegeln danach in manchen Fällen alle Schnittstellen, sodass darüber kein Datenaustausch mehr stattfinden kann. Sind diese Maßnahmen geeignet gegen Datenklau?

Rogge: Es gibt sicherlich ausreichend Maßnahmen, um sich zu schützen. In einigen Fällen wird dies in der Tat so durchgeführt, hindert allerdings daran, nachträgliche Wartungen, Patches et cetera aufzuspielen. Es sollte einfach sorgfältig abgewogen werden, welche Maßnahmen sind für welche Fälle erforderlich, um seine Unternehmensdaten zu schützen. Nicht unterschätzen sollte man hier die eher manuelle Form der Spionage und des Datenklaus mittels interner Mitarbeiter. Ein häufig in Vergessenheit gelangter Fakt.

Sollten Unternehmen nicht besser mehrere Techniken einsetzen, um weniger verwundbar zu sein? Denkbar wäre, dass ein einfaches Handy für Telefonate und ein geschützter Laptop mit verschlüsselter Festplatte für den Rest genutzt wird. Auf diese Weise werden kritische Daten nur auf dem Laptop vorgehalten. Schließlich sind Smartphone-Daten etwa von Vertriebsmitarbeitern via Spionage-App leicht mitlesbar, wenn diese mit dem PC abgeglichen werden.

»Ich persönlich rate keinem Unternehmen, nur aus Kostengründen eine Cloud-Lösung zu wählen.«

Rogge: Wird ein Unternehmen, welches sich eben gut absichert schwerer angreifbar, wird der Weg über weniger gesicherte Zulieferer gewählt. Je kleiner ein Unternehmen, umso weniger Budget ist zur Unternehmenssicherheit vorhanden. Wobei es hier auch darauf ankommt, in welchem Bereich ein Unternehmen arbeitet. Ein 20 Mann-Technologieunternehmen, welches mir bekannt ist, hat Sicherheitsmaßnahmen, die an manche Regierungsstelle erinnert.

Konto-PIN, Kreditkartendaten, Zugangscode zur Konstruktionsdatenbank – es gibt nichts, was man dem Smartphone nicht anvertraut, um sich nicht lange Zahlenwüsten merken zu müssen. Spione bekommen so alles auf dem Serviertablett präsentiert. Haben Sie einen Tipp, wie es besser geht, ohne auf moderne Technik verzichten zu müssen?

Rogge: ›Datensparsamkeit‹ ist das Schlagwort. Man sollte sich als Unternehmer fragen, ob und welche Daten mobil transportiert werden müssen und welche nicht. Mobilität setzt nicht zwangsweise voraus, dass man alles am Mann haben muss.

Der Standort von Handys lässt sich problemlos ermitteln. Auf diese Weise können Bewegungsprofile erstellt werden. Gibt es dazu einen praxisgerechten Tipp, um nicht zu viel von seiner Reisetätigkeit preiszugeben?

Rogge: Das ist kaum möglich, wenn man sein Firmensmartphone auch für die Navigation nutzt. Es ist oft genug vorgekommen, dass hier Eingriffe vorgenommen wurden und die Bewegungsprofile zu einer Konfrontation von Arbeitgeber und Arbeitnehmer führten. Es ist sicher fragwürdig, inwiefern hier eine Auswertung vorgenommen werden darf. Der Datenschutz schützt den Arbeitnehmer, sofern dieser nicht ausdrücklich solchen Praktiken zugestimmt hat.

Zum Abhören vertraulicher Gespräche können sogar Fensterscheiben genutzt werden, die durch den Sprechschall in Schwingungen versetzt werden. Diese werden mit einem Laser abgetastet und das Schwingungsmuster, ähnlich wie beim Abspielen einer CD, hörbar gemacht. Wie sieht es denn mit drahtlosen Mäusen und Tastaturen aus. Sind das nicht auch trojanische Pferde, die man sich da ins Haus holt?

Rogge: Man sollte nicht jeden Fortschritt verteufeln, aber dennoch wachsam und informiert sein. Sicher können Laptoptastaturen über ein ähnliches Verfahren belauscht werden und man kann die Eingaben abhören. Drahtlose Technik ist davon ebenso betroffen, solange Technologien, wie etwa Bluetooth, unsicher sind.

Kann es sein, dass über Wireless-LAN drahtlos zum Drucker gesendete Druckaufträge heimlich den Weg ins Internet finden? Immerhin könnte der Router ja durch eine geheime Schaltung dies ermöglichen.

Rogge: Die Angriffsvektoren sind hier sehr vielseitig und ich befürchte, dass diese Ausgabe dafür nicht ausreichend Platz hat. Allerdings ist es in der Tat so, dass selbst verschlüsselte WLANs von Experten recht schnell aufgebrochen werden können, um so Daten abzufangen. Das Framework ›Metasploit‹ bietet dazu ausgefeilte Skripte, die dies ermöglichen. Aber auch ›aircrack-ng‹ bietet dahin gehend sehr viele Angriffsmöglichkeiten, vor denen Unternehmen geschützt sein sollten.

Überhaupt ist der Trend zur Drahtlos-Technik gerade im industriellen Umfeld bedenklich. Was raten Sie Unternehmen und dem sicherheitsbewussten Anwender, wenn er dennoch nicht auf diese Technik verzichten möchte?

Rogge: Man sollte bei jeder Sicherheitsüberlegung in der Tat eine Risikoanalyse durchführen um zu erkennen, ob bestimmte Bereiche der

Technik/Herstellung besser abgetrennt und in gesonderten Netzwerkbereichen arbeiten sollten. Eine möglichst hohe Verschlüsselung bietet Schutz vor Manipulation und weiteren Einfallsmöglichkeiten. Sabotage wäre hier durchaus noch möglich, aber vom Schaden her geringer, als wenn der Übergriff auf das Unternehmensnetzwerk möglich wäre.

Auf öffentlichen Plätzen werden immer mehr Kameras aufgebaut. Heutige Gesichtserkennungssoftware funktioniert schon erschreckend gut. Ist hier nicht unsere Privatsphäre massiv bedroht?

Rogge: Ein schweres Thema muss ich gestehen. Grundsätzlich natürlich, denn was mit den gewonnenen Daten geschieht, ist in Deutschland leider nicht transparent, außer, dass man den Bürger vor Terrorismus bewahren möge. Ich betrachte das Thema durchaus kritisch und halte es für massiv übertrieben. Kriminalität verlagert sich nachweislich dahin, wo keine solchen Maßnahmen greifen.

Nutzer, die in sozialen Netzwerken, wie etwa Facebook, Mitglied sind, gehen sehr freizügig mit ihren Daten um. Wie erklären Sie sich diesen Leichtsinn und was raten Sie dem Nutzer dieser Netzwerke?

Rogge: »Schreibe in Facebook & Co die Daten rein, bei denen Du auch bereit bist, diese morgen in einer Tageszeitung auf Seite 1 zu lesen.« Der Irrglaube, man sei in einem privaten Netzwerk ist enorm groß. Dass dem nicht so ist, zeigt ein Beispiel: Eine Arbeitnehmerin meldet sich krank und postet kurz darauf lustige, aktuelle Fotos von der Sonneninsel Mallorca, wo sie sich köstlich amüsierte. So etwas geht natürlich nicht.

Man hört, dass Facebook auch von der CIA unterstützt wird. Liegt es da nicht auf der Hand, dass die Daten generell mitgelesen werden? Immerhin sind die USA dabei, riesige Abhöranlagen zu errichten, um jede Mail und jedes Telefongespräch auf verdächtige oder interessante Inhalte zu analysieren.

Rogge: Möglich ist vieles und mittels Überwachungsgesetze in den USA auch legitimiert. Es werden und müssen Schnittstellen dafür bereitgestellt werden. Fraglich allerdings, wer diese Flut an Daten wirklich auswerten will und zu welchem Zweck. Für eine gezielte Strafverfolgung ist dies durchaus sinnvoll. Eine normale Überwachung ist hier allerdings schon sehr schwer durchführbar, auch wenn wir von Big Data sprechen.

Momentan werden massive Werbekampagnen bezüglich der Cloud durchgeführt. Gerade Unternehmen sollen auf den Zug aufspringen. Es wird versprochen, dass die Daten garantiert sicher seien und ausschließlich das Unternehmen beziehungsweise der Nutzer darauf Zugriff haben. Ist dieses Versprechen nicht eher dem Bereich der Fabel zuzuordnen?

Rogge: Ich persönlich rate keinem Unternehmen, aus Kostengründen hier eine solche Lösung zu wählen.

Was raten Sie gerade Unternehmen, wenn sie die Cloud trotz aller Gefahren nutzen möchten?

Rogge: Man muss analysieren: Wo ist der Standort der Cloud Server, wo steht das Rechenzentrum, welche Kommunikation geht dahin und zurück, wie sind Daten dort abgelegt, wird deutsches Recht berücksichtigt und vieles mehr. Ein komplexer Prozess, der augenscheinlich von den Anbietern so vereinfacht wird. Selbst Amazon hatte einen Zwischenfall, bei dem Daten in der EC2 (Elastic Cloud) unwiederbringlich weg waren. Wer haftet in diesen Fällen? Welches Gesetzt greift? Mit diesen Themen muss man sich auseinander setzen, möchte man solche Services für sein Unternehmen nutzen.

Das bargeldlose Bezahlen kommt immer mehr in Mode. In Schweden sind sogar Bestrebungen im Gange, das physische Geld komplett abzuschaffen. Die Bürger sollen nur noch via Chipkarte oder Einzugsauftrag bezahlen können. Die zunächst harmlos erscheinende Idee birgt immense Risiken für den Einzelnen. Wie ist ihre Meinung dazu?

Rogge: ›Nur Bares ist Wahres.‹ Ein Ausspruch, der für die heutige Zeit etwas übertrieben sein mag, aber viel aussagt. Mittels elektronischer Zahlungssysteme (RFID, Plastikgeld et cetera) werden auch wieder neue Angriffsmöglichkeiten geöffnet. Es gilt sicherlich nicht alles zu verteufeln, aber mit Bedacht einzusetzen.

Zum Schluss: Wie ist ihre persönliche technische Ausstattung, um am täglichen Leben teilzunehmen und wie schützen sie sich vor zu viel Schnüffelei?

Rogge: Vor der Installation überlegen, was man sich installiert und welche Zugriffe damit ermöglicht werden. Weitere Details möchte ich aus Sicherheitsgründen nicht veröffentlichen.

Herr Rogge, vielen Dank für das Interview.

omega-defense.com