Digitaler Selbstmord

Laxer Umgang mit Angaben über Bürger: Mailanbieter Posteo rügt Polizeibehörden. Doch der Angriff auf unser digitale Integrität ist längst in vollem Gange

Joachim Jakobs

Der E-Mail-Service-Anbieter Posteo hat Bundesinnenminister Thomas de Maizière (CDU) Mitte Oktober vorgeworfen, dass Polizeibehörden »Bestandsdaten« wie Namen und Adressen unverschlüsselt abrufen würden. Posteos Problem: Die Kunden sind von dem Verschlüsselungskonzept des Anbieters so überzeugt, dass sie dafür sogar Gebühren zahlen. Wenn Behörden die Kundendaten nun aber unverschlüsselt abrufen, könnten sich die Nutzer das Geld auch sparen.

Das Unternehmen sieht einen Verstoß gegen das Bundesdatenschutzgesetz. Dieses fordert in einer Anlage, »dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können«. Der Bundesinnenminister beschwichtigt nach Angaben des Fachmagazins *Heise online*: Nur im »absoluten Ausnahmefall« würden Daten unverschlüsselt abgerufen. Gegenüber *jW* wies de Maizières Pressestelle außerdem darauf hin, dass »die Art und das Verfahren der Verschlüsselung auch vom Kommunikationspartner abhängig ist«. Posteo bietet hier die Standardverfahren »PGP« und »S/MIME« an. Welches Verfahren die Behörden nutzen, wollte das Ministerium nicht verraten. Solche Bestandsdaten werden nicht nur bei Telekommunikationsunternehmen, sondern auch von Rathäusern und Kfz-Zulassungsstellen abgefragt. Das bayerische Staatsministerium antwortet auf Anfrage: »Wir wissen nicht, wie die kommunalen Behörden (...) ihre E-Mails verschlüsseln.« Das bedeutet: Im Freistaat darf offenbar jede Behörde die Gesetze nach eigenem Gutdünken auslegen. Nicht immer klappt das mit diesem Ermessensspielraum – wie eine Woche nach Posteos Klagen bei *Focus Online* zu lesen war: »Mann besticht Kfz-Mitarbeiterin und bietet Daten im Darknet an.«

Attacken aus den Netz

Findet sich »in« der jeweiligen Organisation niemand, den der Täter für seine Zwecke einspannen kann, kommt der Angriff von »außen« in Betracht. So war die Internetseite des Wirtschaftsmagazins *Forbes* mit der Schadsoftware »Angler« infiziert. Die Folge: Bei jedem Besuch eines Lesers prüft »Angler« dessen System auf Schwächen, um dann einen Schädling auf diesem zu hinterlassen, der es okkupiert. Anschließend werden die Nutzerdaten verschlüsselt, und vom Opfer wird gefordert: »Geld oder Daten.«

In qualitativer Hinsicht kann sich das Ergebnis der Manipulation durchaus sehen lassen: »Die Schadsoftware ist so gut«, sagt Joseph Bonavolonta, Ermittler bei der US-Bundespolizei FBI, »wir empfehlen den Leuten häufig, einfach zu zahlen«. Die Telekom hat das offenbar getan: »Jede Firma, die im Internet agiert, erlebt diese Erpressungsversuche. Bei uns, der Deutschen Telekom, ist der letzte, glaube ich, vier Wochen her. Wir haben übrigens bezahlt. Wir hatten keine andere Möglichkeit«, ließ sich Bernd Eßer, »Head of Cyber Defense«

des Konzerns, kürzlich vom *Deutschlandfunk* zitieren.

Wenn die Telekom nicht damit klarkommt – wer dann? Aktuell warnen die Landeskriminalämter zwischen Kiel und München vor der Schadsoftware namens »Chimera«: Kriminelle durchforsten die elektronischen Stellenmärkte und schicken eine E-Mail mit einem Link zu einer Internetseite, auf der sich scheinbar eine Bewerbung befindet. Statt dessen lädt sich der Personalsachbearbeiter tatsächlich aber die Schadsoftware auf den Rechner. Je nach dessen Ausführung muss damit gerechnet werden, dass sämtliche Geräte infiziert werden, die mit der Personalabteilung verbunden sind.

Eine andere Möglichkeit, Gewinn aus den Daten zu schlagen: Man kann damit drohen, die Informationen im Internet zu veröffentlichen. Wer zahlt, weiß aber nie, ob sich der Erpresser damit zufrieden gibt – oder die Daten einfach an den Gesinnungsgenossen verkauft – der dann seinerseits etwa einen »Identitätsdiebstahl« verübt und im Namen seines Opfers Rechtsgeschäfte abschließt.

Wettrüsten der Sammler

Zu den Angreifern zählen Geheimdienste, Cyberkriminelle und -terroristen. Erstere wollen ihre Regierungen bestmöglich mit Informationen versorgen. Seit Edward Snowden (2013) hat sich das Budget allein der US-amerikanischen NSA verfünffacht. Am digitalen Wettrüsten beteiligen sich neben dem BND, Russland und China auch Syrien, Iran, Nordkorea, Pakistan und die Schweiz. Während Kriminelle vorrangig viel Geld machen wollen, könnte der »Islamische Staat« beispielsweise danach trachten, uns den Strom abzustellen.

Das Bildungsniveau krimineller Angreifer verhält sich umgekehrt zur Sensibilität der Angegriffenen – nicht einmal physisch scheinen wir zu wissen, was wir tun. Beispiele gibt es genug: So lagen Akten des Oberlandesgerichts München in Köln auf der Straße herum, eine Festplatte einer Grundschule wurde mit Zeugnissen auf dem Trödelmarkt verkauft usw.

Der »digitale Graben« zwischen dem Bildungsniveau der Angreifer und dem der Angegriffenen wächst synchron mit der technischen Leistungsfähigkeit. Letztere ermöglicht es den Entscheidern in Politik und Wirtschaft, zahlreiche neue Spielsachen zu bewerben: »Gesundheitstelematik« beispielsweise oder »Verkehrstelematik«. Es werden »intelligente« Gebäude konzipiert, und sogar »intelligente« Stromnetze sollen unser Leben künftig bereichern. Auf Basis dieser Entscheidungen wird dann Software entwickelt, implementiert, administriert oder genutzt, um vernetzte Geräte zu steuern oder personenbezogene Daten zu verarbeiten. Der Gesundheitsminister droht derweil denen, die die Einführung der Gesundheitskarte »blockieren«. Lieber sollte Hermann Gröhe (CDU) dafür sorgen, dass alle Beteiligten über Sicherheits- und Notfallkonzepte, physikalischen Einbruchschutz und rollenspezifisches Wissen verfügen. Sonst kommt das Geplante einem digitalen Harakiri gleich.

---

http://www.jungewelt.de/2015/11-02/068.php