

Aufräumen nach dem Polit-Hack

Mittwoch, 23 Januar 2019

<https://www.datenschutz.de/aufraeumen-nach-dem-polit-hack/>

Das Internet vergisst nichts? Doch.

Pressemitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 22.01.2019

Der Polit-Hack, bei dem offenbar ein Schüler persönliche Informationen von 994 Politikern und Prominenten sowie mehreren zehntausend Bürgern erbeutete und im Internet zum Abruf verteilte, ist keineswegs vorüber. Zwar scheint der Täter ermittelt und geständig – aber die zum Teil höchstpersönlichen Daten wurden so im Netz verbreitet, dass es nahezu aussichtslos erscheint, sie dort wieder einzusammeln und dadurch zu verhindern, dass Journalisten, politische Gegner, Geheimdienste oder auch private Interessierte sie dort finden und herunterladen – aus Neugierde und Schadenfreude, mit Schädigungsabsicht, aus professionellem Interesse, zu Zwecken späterer Erpressung oder Manipulation ...

„Das Internet vergisst nichts!“ heißt es nicht ohne Grund, denn wenn wie in diesem spektakulären Fall die Informationsbeute geschickt über Plattformen weltweit verteilt wird, sind die Betroffenen nahezu machtlos, wenn sie den persönlichen Schaden begrenzen und verhindern wollen, dass ihre Daten „auf ewig“ im Netz zu finden sind.

Das hängt insbesondere damit zusammen, dass die Möglichkeiten anonymer Nutzung internationaler Plattformen nahezu unbegrenzt sind – und viele solcher Anbieter gerade damit prahlen „bullet proof“ zu sein und sich der Regulierung durch staatliche Stellen wie Aufsichts- und Sicherheitsbehörden sowie Gerichten wirksam entziehen – zum Nachteil der in ihren Rechten verletzten Opfer der Hacks.

Aber völlig machtlos sind wir gegenüber den unregulierten Weiten des Internets nicht:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) konnte erste „Takedown-Erfolge“ – auch bei außereuropäischen Plattformen – erzielen. Rund 1000 Download-Adressen sind in der Zwischenzeit gelöscht, bei mehreren hundert weiteren ist der LfDI in Kontakt mit den anderen europäischen Aufsichtsbehörden. Denn auch die Plattformbetreiber müssen ihren Teil der Verantwortung tragen und rechtswidrige Inhalte nach entsprechender Kenntnisnahme löschen.

Datensicherheit tut offensichtlich Not. Nur wer sehr sorgfältig auf den Schutz seiner persönlichen Daten achtet, indem er unseriöse Anbieter im Netz meidet, seine Passwörter gut und differenziert wählt, wer bei seiner eigenen „Informationspolitik“ Privates und Öffentliches klug unterscheidet, der kann das Risiko mindern, selbst Opfer eines Hacks zu werden – ausschließen kann man das allerdings nie ganz, schon weil auch Dritte (Verwandte, Bekannte, Berufskollegen, Behörden etc.) mit unseren Daten arbeiten und deren Nachlässigkeit und Fehler in punkto Datensicherheit uns selbst treffen.

Wie man sich verhält, wenn man selbst Opfer eines Hackerangriffs geworden ist, darüber klärt der LfDI demnächst in einer Handreichung „Gehackt – was tun?“ auf.

Allen, die aus beruflichen oder persönlichen Gründen im Internet nach Daten aus diesem oder anderen Leaks gesucht haben und diese Daten von entsprechenden Plattformen vielleicht sogar heruntergeladen haben, sei gesagt: Die Gefahr, sich beim Hantieren mit den kopierten Daten selbst mit Viren oder Trojanern zu infizieren, ist extrem hoch. Denn auf den unseriösen Plattformen, welche Hacker in aller Regel für die Verteilung ihrer Beute nutzen, wimmelt es nur so von Schadsoftware, die beim Betrachten der Hackerbeute gleich mit heruntergeladen werden. Hierzu der Hinweis: Virenschutz-Programme, ob kostenlos aus dem Netz oder teuer bezahlt, sind immer einen Schritt hinter den Angreifern. Gegen neu entwickelte Schadware hilft Ihr Schutzprogramm erst morgen.

Deshalb sollten sich gerade Journalisten und Redaktionen schnellstmöglich davon überzeugen, welche ungebetenen Besucher sie in ihr Netzwerk gelassen haben und wie sie diese wieder loswerden. Der LfDI berät auch hierzu gerne.

Doxing – Nein Danke!

Anderen Menschen im Netz durch kriminelles Vorgehen persönliche Daten zu entwenden und offenzulegen (sog. Doxing) ist nicht nur strafbar, sondern verletzt auch unsere Privatsphäre, auf die wir alle angewiesen sind, um ein vertrauensvolles, gesundes und selbstbestimmtes Leben führen zu können. Im politischen Raum – wie beim Polit-Hack – vergiften solche geleakten Informationen zudem den gesellschaftlichen Diskurs, machen in der Öffentlichkeit stehende Akteure verächtlich oder erpressbar. Damit legt Doxing die Axt an die Wurzeln unserer freiheitlichen und offenen Gesellschaft.

Jenseits der Reaktionen unserer Sicherheitsbehörden müssen wir als Bürgerinnen und Bürger ebenfalls lernen, wie man mit diesem neuen Phänomen vernünftig umgeht – und da kann die Lektion nur heißen: Ergebnisse der kriminellen Verletzung der Privatsphäre anderer nimmt man nicht zur Kenntnis! Das gilt nicht nur im Netz, sondern eigentlich schon immer: Niemand käme auf die Idee in den Unterlagen zu wühlen, die ein Nachbar notgedrungen auf der Straße abgelegt hat, weil sein Haus in Flammen steht. Es ist ein Gebot des Anstands und des fairen Umgangs miteinander, die Notlage des Betroffenen nicht auszunutzen, um tief und gegen seinen Willen in seine Privatsphäre einzudringen.

Diese moralische Regel sollte nicht nur für Privatleute, sondern auch für Journalisten gelten: Wer Privates zur Kenntnis nimmt, das Kriminelle entwendet haben, macht deren Job und vertieft die Rechtsverletzung. Also Finger weg vom Doxing!

Die Pressemitteilungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg