LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/4803**

15.01.2019

Antrag

der Fraktion der AfD

Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern

I. Ausgangslage

Die am 3. Januar 2019 einer breiten Öffentlichkeit bekanntgegebene Veröffentlichung von mitunter über Jahre gesammelten privaten Daten von Politikern und Prominenten hat – entgegen ersten Spekulationen – nichts mit herkömmlichen kriminellen Eingriffen in IT-Systeme zu tun, sondern geschah durch Ausnutzung von teilweise fahrlässigem und unzureichenden Maßnahmen zum Schutz privater Daten in IT-Kommunikationssystemen (Email, Social Media) sowie Cloud-Anwendungen.

Auch Spitzenpolitiker und Regierungsmitglieder aus NRW sind betroffen, so wurden persönliche Telefonnummern von Ministerpräsident Armin Laschet (CDU), Joachim Stamp und Christian Lindner (FDP), Arndt Klocke und Monika Düker (Grüne) sowie von Sebastian Hartmann und Sarah Philipp (SPD) veröffentlicht.

Die AfD war im konkreten Fall nicht betroffen, wurde aber in den Vorjahren bereits mehrfach das Opfer ähnlicher Angriffe. Einbrüche in die parteieigenen IT-Systeme, bzw. die Systeme von Dienstleistern führten dazu, dass tausende Namen, private Anschriften, Emailadressen und weitere Daten 2015 und 2016 veröffentlicht und dadurch betroffene Mitglieder in ihrem persönlichen Lebensbereich bedroht wurden.

Wie die Ermittlungen des BKA ergaben, war im jüngsten Fall ein (zumindest bei Beginn der hier gegenständlichen Taten) jugendlicher Schüler verantwortlich für das Abgreifen und Veröffentlichen der Daten. Er hat durch Ausnutzung von Schwachstellen sowohl bei der IT-Technik als auch durch menschliche Schwachstellen bei seinen Einbrüchen Zugang zu fremden Email- und Social- Media- Konten erhalten.

Besorgniserregend ist nicht die inhaltliche Brisanz der veröffentlichten Daten, sondern wie einfach solche Daten erworben werden konnten. Dieser Vorgang deckt eine wesentliche Sicherheitslücke auf, die durch bereits bestehende Sicherheitsmaßnahmenpakete nicht ausreichend gewürdigt wurde und wird.

Datum des Originals: 15.01.2019/Ausgegeben: 15.01.2019

Wenn sogenannte „Skript-Kiddies“ es schaffen, empfindliche Daten durch die „Schwachstelle Mensch“ zu erbeuten, was bedeutet das dann für die Möglichkeiten von professionellen Hackern, die zielgerichtet sowohl durch Hacking von IT-Systemen als auch durch sogenanntes Social Engineering in bestehende Kommunikationsnetze einbrechen?

Die „Amadeo-Antonio-Stiftung“ äußert über die Gefahren und Konsequenzen solcher „Doxing“-Aktionen: „Wer online die Kontrolle über seine privaten Daten verliere, weil diese veröffentlicht würden ("Doxing"), erlebt anschließend auch in der realen Welt Angst.“ Würden etwa von politisch engagierten Menschen Wohnorte, Familieninformationen und andere Daten veröffentlicht, führe das zu Trollanrufen und unangenehmen bis gefährlichen Posts oder sogar zu „Hausbesuchen“ und physischer Gewalt. Oft würden sich die Angegriffenen gezwungen sehen, ihr persönliches Umfeld zu ändern.“[1]

Waren Datenlecks bisher auch durch Ausnutzung von technischen Unzulänglichkeiten bekannt gemacht worden, so spielt im aktuellen Fall eher der Zugang mit Hilfe menschlicher Unzulänglichkeiten eine wesentliche Rolle.
Eine aktuelle Umfrage von Bitkom ergab: 50% der Internetnutzer waren 2018 Opfer von Cyberkriminalität. (davon 23% durch Illegale Nutzung persönlicher Daten; 11% durch Missbrauch von Kontodaten). Vor diesem Hintergrund ist es nahezu ausgeschlossen, dass Akteure aus Politik und Landesbehörden nicht betroffen waren.[2]

Erkenntnisse aus dem aktuellen Datenleak:

- Seit Anfang Dezember die ersten Datensätze unter den Twitteraccount „@_0rbit“ veröffentlicht wurden, hatte das BSI erste Kenntnisse von Datenleaks, konnte diese aber nicht in einen Gesamtzusammenhang einordnen. Mit den weiteren Veröffentlichungen wurde das Ausmaß dieser Unwissenheit immer größer. Weiterhin gab es Betroffene, die trotz Kenntnis ihrer Datenveröffentlichung nicht durch die entsprechenden behördlichen Stellen unterrichtet wurden.

- Vielfach wurden private Datensätze nicht durch eigenes Verschulden veröffentlicht, sondern durch Kontaktdatensammlungen Dritter, die z.B. den Zugang zu ihren Telefonbüchern nicht ausreichend abgesichert hatten. Hier gab es einerseits Verstöße gegen die Datenschutzgrundverordnung (DSGVO), welche eine Erlaubnis/Kenntnisgabe des Speicherortes der Kontaktdaten von Betroffenen sowie zusätzlich eine hinreichende, nach aktuellem Sicherheitsstand eingerichtete Zugangs-Beschränkung für diesen Speicherort vorsieht (Art. 32 DSGVO), wenn dabei Politiker/Prominente nicht als Privatpersonen agieren.

- Trotz aller Aufklärungskampagnen ist der Faktor Mensch mit seiner Bequemlichkeit und Vertrauensseligkeit immer noch das wesentlichste Schwächeglied in der IT-Sicherheit. So zeigte eine luxemburgisch-deutsche Studie von 2016, dass 50% der teilnehmenden Internetnutzer ihr Passwort gegen eine Tafel Schokolade eintauschen würden.[3]

[1] https://www.neues-deutschland.de/artikel/1109539.datenklau-digitale-herausforderungen.html
[2] https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-von-Cyberkriminalitaet-betroffen
[3] Happ/Melzer/Steffgen: “Trick with treat – Reciprocity increases the willingness to communicate personal data”, in Computers in: Human Behavior 61 (2016), S. 372-377

- Seitens des Landes fließt neben der technischen Absicherung von IT-Systemen auch die Aufklärung der Mitarbeiter und Verantwortlichen in die Arbeit der Verantwortlichen, u.a. des Beauftragten der Landesregierung Nordrhein-Westfalen für Informationstechnik (CIO) in die Planung zur IT-Sicherheit mit ein. Jedoch wird bei den sogenannten regelmäßigen Vulnerabilitätstests, den Penetrations-Tests („Pen-Tests“), nur die technische Infrastruktur auf Lücken getestet. Eine Überprüfung des menschlichen Faktors wird nicht vorgenommen.

- Die Ende November 2018 erfolgte Zertifizierung von IT.NRW nach ISO/IEC 27001-Zertifikat auf der Basis von IT-Grundschutz ist ein wichtiger wenn auch recht später und unzureichender Schritt in die richtige Richtung. Entsprechende ISO/IEC 27001 Zertifikate wurden schon 2012 (Saarland IT) und 2013 (Rechenzentrum Mecklenburg-Vorpommern) ausgestellt. Einzelne Ministerien wurden in NRW bisher nicht zertifiziert, während beispielsweise in Sachsen das Ministerium für Wissenschaft und Kunst (SMWK) schon 2008 das entsprechende Zertifikat erhielt.

- Das ISO/IEC 27001-Zertifikat ist wesentlich, da es auch verbindliche Regelungen zur Überprüfung und Schulung der Mitarbeiter im Hinblick auf Datensicherheitsaspekte voraussetzt. Eine Übertragung des Zertifikats von IT.NRW auf andere, angeschlossene Dienststellen findet aber nicht statt.

-

- Herkömmliche Standard-Penetrationstests berücksichtigen nicht ausreichend den Faktor Mensch, wie das BSI auch zugibt: “Mit IS-Penetrationstests können technische und einige organisatorische Schwachstellen aufgedeckt werden, aber selten personellen Gefährdungen.“[4] Hier müssen verstärkt menschliche Schwachstellen durch Social Engineering Angriffe bei sogenannten White-Hat- Hacks regelmäßig überprüft, aufgedeckt und evaluiert werden.

II. Der Landtag stellt fest:

1. Unvorsichtiger und nachlässiger Umgang mit Daten ist eine verbreitete menschliche Schwäche, die offenbar auch in der politischen Sphäre keine Seltenheit ist. Eine verstärkte Sensibilisierung für Notwendigkeiten zur Verschlüsselung, Datensparsamkeit und zur bewussten Nutzung von Cloud- und Social Media-Diensten dient nicht nur dem Schutz der eigenen Person sondern auch dem Schutz des eigenen Umfeldes und der Bürger, mit denen eine Interaktion erfolgt.

2. Die Speicherung von Daten Dritter unterliegt einer besonderen Verantwortung und darf nur im Einvernehmen mit dem Betroffenen stattfinden. Derart erhobene Daten müssen besonders gesichert werden.

3. Insbesondere die verstärkte private Nutzung mobiler IT-Systeme und der zusätzlichen Einbeziehung einer Cloud-Infrastruktur lassen bisherige Sicherungskonzepte, die vor allem auf stationäre Desktop- und Serverarchitektur basieren, nicht angemessen erscheinen.

---

4 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Beschreibung_Pentest.pdf?__blob=publicationFile&v=5

III. Der Landtag fordert die Landesregierung auf,

1. mit einer erneuten Evaluierung der Informationsflüsse und Kooperationstiefe von IT.NRW, CERT NRW (Computer Emergency Response Team NRW), BSI (Bundesamt für Sicherheit in der Informationstechnik) und allen relevanten IT-Sicherheitseinrichtungen des Bundes und des Landes eine lückenlose Kommunikation zwischen den Betroffenen und den Sicherheitsverantwortlichen zu gewährleisten.

2. neben der bereits erfolgten Zertifizierung von IT.NRW nach ISO/IEC 27001, weitere Behörden und Landeseinrichtungen systematisch vom BSI nach ISO 27001 auf der Basis von IT-Grundschutz zertifizieren zu lassen.

3. regelmäßige sogenannte Penetrationstests durch CERT NRW bei Behörden und Landeseinrichtungen um ein Verfahren zur Aufdeckung von Sicherheitslücken durch sogenanntes Social Engineering standardmäßig ergänzen zu lassen.

4. sich bei Herstellern von Kommunikationssoftware, sowie beim Bundesgesetzgeber für sogenanntes Security by Design, wie etwa einer obligatorischen, standardmäßigen Zwei-Faktor-Authentisierung (2FA), stark zu machen.

5. der verstärkten digitalen Transformation der Verwaltungen Rechnung zu tragen und IT-Compliance-Regelungen obligatorisch für jede Landeseinrichtung schon im Vorfeld eines E-Government-Roll-Outs festzuschreiben sowie die Kommunen bei der Implementierung von grundlegenden IT-Compliance-Regelungen durch z.B. der Gemeindeprüfungsanstalt Nordrhein-Westfalen (gpaNRW) zu unterstützen.

Sven W. Tritschler
Markus Wagner
Andreas Keith

und Fraktion