

Landtag Nordrhein-Westfalen
Ausschuss für Digitalisierung und Innovation
Postfach 10 11 43
40002 Düsseldorf

Per E-Mail: anhoerung@landtag.nrw.de

Bonn, 6. Mai 2019

**Drucksachen 17/4803 und 17/5056
Anhörung des Ausschusses für Digitalisierung und Innovation am 16. Mai 2019**

Sehr geehrter Herr Vorsitzender,
sehr geehrte Ausschussmitglieder,

vielen Dank für die Gelegenheit zur Stellungnahme zu den Anträgen der Fraktionen der AfD (Drucksache 17/4803) sowie Bündnis 90/Die Grünen (Drucksache 17/5056) und für die Einladung zur Sitzung des Ausschusses am 16. Mai 2019.

Stellungnahme zum Antrag der Fraktion der AfD:

Zur Ausgangslage:

Der Antrag unterscheidet in der Ausgangslage herkömmliche kriminelle Eingriffe in IT-Systeme und die Ausnutzung fahrlässiger und unzureichender Maßnahmen zum Schutz privater Daten. Insbesondere private Daten stehen, neben anderen Geschäftsgeheimnissen von Unternehmen, auch bei den als herkömmlich bezeichneten kriminellen Eingriffen regelmäßig im Visier der Angreifer. Kriminelle nutzen dabei Verwundbarkeiten in aktueller Software (sogenannte Zero-Day-Schwachstellen), wie auch in veralteter Software (hierbei handelt es sich auch um fahrlässige und unzureichende Maßnahmen) genau so aus, wie unzureichend gesicherte Benutzerkonten durch schwache gewählte Passwörter oder manipuliertes Benutzerverhalten (wie beim Social Engineering). Bei Social Engineering handelt es sich ebenfalls nicht um ein neues Phänomen, vielmehr ist die Verbreitung von Schadsoftware über E-Mails (etwa der Erpressungs-Schadsoftware WannaCry) immer wieder ein gewähltes Mittel der Kriminellen.

Der Antrag formuliert, dass ein jugendlicher Schüler verantwortlich für das Abgreifen und Veröffentlichen der Daten (auch bekannt als Doxing) sei. Er habe durch Ausnutzung von Schwachstellen sowohl bei der IT-Technik als auch durch menschliche Schwachstellen bei

seinen Einbrüchen Zugang zu fremden E-Mail- und Social-Media-Konten erhalten. Insbesondere die Ausnutzung von Schwachstellen bei der IT-Technik durch den Jugendlichen ist so nicht bekannt und es gibt viele Anhaltspunkte dafür, dass die Daten der Schlüsselkonten bereits zuvor in öffentlich verfügbaren Leaksammlungen enthalten waren. Einige der Daten, etwa Scans von Personalausweisen, wurden bereits im April 2018 auf entsprechenden Plattformen hinterlegt. Näher liegt hier, dass der Jugendliche als Trittbrettfahrer die bereits veröffentlichten Daten der Betroffenen verwendet hat, um über kompromittierte E-Mail- und Social-Media-Konten weitere Informationen, etwa Adressbücher, etc. zu sammeln. Wären Betroffene rechtzeitig proaktiv von der Existenz ihrer Daten in solchen öffentlich verfügbaren Leaksammlungen informiert worden, hätten sie durch die zeitnahe Änderung ihrer Passwörter einen Schaden eventuell vermeiden können.

Den Erkenntnissen aus besagtem Doxing-Vorfall lässt sich hinzufügen, dass die Daten nicht erst im Dezember 2018 veröffentlicht wurden, sondern sie a) bereits vorher in Datensammlungen in einschlägigen Kreisen kursierten und b) auch im Dezember zunächst nur einem kleinen Kreis bekannt waren. Erst im Januar 2019 wurde eine große Öffentlichkeit durch die Berichterstattung darauf aufmerksam.

Die im Antrag zitierte luxemburgisch-deutsche Studie von 2016 hat andere als die angegebenen Ergebnisse ermittelt. Tatsächlich hat nicht die Hälfte, sondern lediglich ein Drittel der Befragten _ein_ Passwort gegen eine Tafel Schokolade eingetauscht. Von dem Befragten wurde zwar verlangt, dass es das eigene und tatsächlich genutzte Passwort ist, ob dieser jedoch wahrheitsgetreu den Zettel beschriftete wurde zu keiner Zeit geprüft. Schlussfolgerungen aus dieser Studie lassen sich nicht ohne weiteres verallgemeinern.

Die erwähnten, vom BSI durchgeführten IS-Penetrationstests beinhalten keine Überprüfung des Faktors Mensch. In der Privatwirtschaft angebotene Penetrationstests beinhalten durchaus auch Social Engineering. Aufgrund von hohem manuellen Aufwand und entsprechender Vorbereitungszeit sind diese jedoch kostenintensiv, was eigene Erfahrungen aus dem kürzlich abgeschlossenen von mir geleiteten Forschungsvorhaben ITS.APT (IT-Security Awareness Penetration Testing) bestätigen. Im Gegensatz zu technischen Schwachstellen, die im Anschluss an Penetrationstests durch technische Maßnahmen abgesichert werden können, ist die Umsetzung wirksamer Maßnahmen zur Absicherung gegen Verwundbarkeiten durch Social Engineering deutlich schwieriger. Schulungen als Intervention bei menschlichem Versagen sind nicht immer geeignet. So konnten in einem Feldtest im Rahmen des Projekts ITS.APT auch kontraproduktive Nebeneffekte erzielt werden: Durch eine Schulung, die Probanden nachweislich dazu brachte weniger risikobereites Verhalten zu zeigen (weniger auf Phishing-Links zu klicken und Ähnliches) aber einen potentiellen Sicherheitsvorfall auch seltener zu melden.

Mögliche Erklärungen für ein derartiges Verhalten umfassen ein breites Spektrum, wie zum Beispiel überhöhtes Selbstbewusstsein oder eine Fehleinschätzung der eigenen Kompetenzen. Die Untersuchung der Wirkeffekte von Maßnahmen zur zielgerichteten Beeinflussung des Verhaltens von Menschen zur Abwehr von Bedrohungen durch z.B. Social Engineering ist Gegenstand eines für die Zukunft geplanten Forschungsprojekts meiner Arbeitsgruppe.

Vorfälle in der Vergangenheit haben deutlich demonstriert, dass Verwundbarkeiten durch Social Engineering existieren. Da die Wirkeffekte von Maßnahmen zur Begegnung dieser Bedrohungen aktuell im Allgemeinen nicht klar und möglicherweise nachteilig sind, stellt sich die Frage, mit welchem Ziel regelmäßige Vulnerabilitätstests des Faktors Mensch (wie im Antrag thematisiert) durchgeführt werden sollten. Wie soll mit den unterschiedlichen Testergebnissen umgegangen werden? Da der Antrag eine Antwort auf diese Frage schuldig bleibt, sollte der Bedarf an geeigneter Gestaltung von Systemen und Prozessen die Verwundbarkeit durch Social Engineering verringert (zum Beispiel Zwei-Faktor-Authentifizierung) und die gezielte Entwicklung wirksamer Awareness-Maßnahmen bevorzugt werden. Mithilfe entsprechender Tests kann die Eignung der Gestaltung sowie die Wirksamkeit von Awareness-Maßnahmen überprüft werden.

Zu den Feststellungen des Landtags:

Die Aussage, unvorsichtiger und nachlässiger Umgang mit Daten sei eine verbreitete menschliche Schwäche, die auch in der politischen Sphäre keine Seltenheit sei, lässt sich zum Teil bestätigen. Allerdings muss hierbei der Begriff der Privatsphäre viel deutlicher in den Fokus rücken. Dieser erfährt in der Gesellschaft durch soziale Medien derzeit eine große Veränderung und ist nicht mit dem Begriff in den 70er und 80er Jahren vergleichbar. Die Einschätzung und Wertschätzung der eigenen Privatheit korreliert mutmaßlich unmittelbar mit dem Umgang privater Daten.

Zu den Forderungen:

Es ist davon auszugehen, dass die Punkte 1, 2 und 4 zu einer Erhöhung der IT-Sicherheit führen und aus diesem Grund zu favorisieren sind. Darüber hinaus ist eine mögliche Verbesserung der IT-Sicherheit durch Punkt 3 aus oben dargestellten Gründen zu bezweifeln.

Abschließende Bemerkungen:

Die von mir geleitete Arbeitsgruppe IT-Sicherheit an der Universität Bonn hat in den letzten Jahren den Faktor Mensch in den Fokus verschiedener eigener Arbeiten gestellt. Das BMBF-geförderte Projekt IT-Security Awareness Penetration Testing (ITS.APT) zur Bewertung von IT-Sicherheitsbewusstsein zum Schutz kritischer Infrastrukturen wurde von 2015-2017 durchgeführt und erfolgreich beendet. Eine Anschlussfinanzierung wird derzeit beantragt. Seit Januar 2017 wird im Projekt "Effektive Information nach Digitalem Identitätsdiebstahl" (EIDI) mit Förderung vom BMBF die automatische Suche und Auswertung öffentlich verfügbarer Leaksammlungen mit anschließender Risikobewertung und proaktiver Information Betroffener untersucht. Derzeit befindet sich das System in einem Testbetrieb im Kreis der Projekt-Kooperationspartner.

Die Wissenschaft hat sich bereits frühzeitig mit den kürzlich öffentlich aufgetretenen Phänomenen beschäftigt und mögliche Lösungen im Umgang mit den resultierenden Problemen erarbeitet. Der breite Einsatz benötigt jedoch weitere praxisnahe Forschung in diesen Bereichen.

Stellungnahme zum Antrag der Fraktion Bündnis 90/Die Grünen:

Zur Ausgangslage:

Der Antrag erwähnt die Veröffentlichung zuvor geklauter Daten (Doxing) von rund 1.000 Personen des öffentlichen Lebens. Dabei gilt zu beachten, dass die Daten bereits weit im Vorfeld der öffentlichen Aufmerksamkeit veröffentlicht wurden und weit mehr als 1.000 Personen von diesen Veröffentlichungen betroffen sind. Alle Betroffenen haben, unabhängig von ihrem Status als Person des öffentlichen Lebens, nur eingeschränkte Möglichkeiten, den Umstand der eigenen Betroffenheit zu erfahren. Während für Personen des öffentlichen Lebens die Veröffentlichung privater Daten ein Risiko darstellen mag, werden alle anderen Personen durch den häufig resultierenden klassischen Betrug, etwa Online-Bestellungen in ihrem Namen und entsprechend nicht bezahlte Rechnungen mit allen Folgen, zum Teil in ihrer Existenz bedroht.

Als Betroffene von WannaCry werden Krankenhäuser in Großbritannien erwähnt. Auch deutsche Krankenhäuser und andere kritische Infrastrukturen waren deutlich von WannaCry und verwandter Erpressungs-Schadsoftware betroffen.

Im Hinblick auf die Untersuchung und Beherrschung des Phänomens Identitätsdiebstahl sind Universitäten und Forschungseinrichtungen in NRW aktuell führend. Die Universität Bonn führt in Kooperation mit weiteren Forschungspartnern das Projekt "Effektive Information nach Digitalem Identitätsdiebstahl" (EIDI) bereits seit 2017 durch. Eine weitere Förderung über das Projektende im Dezember 2019 ist für weitere Untersuchungen dringend notwendig.

Die ebenfalls im Antrag erwähnten Angebote zur Aus- und Weiterbildung werden bereits nicht nur an Schulen und Hochschulen geschaffen. Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), für das ich ebenfalls tätig bin, hat etwa in Zusammenarbeit mit der Hochschule Bonn-Rhein-Sieg ein Lernlabor Cybersicherheit entwickelt, das neben Unternehmen und Behörden auch gezielt Tätigen in kleinen und mittelständischen Betrieben Weiterbildung im Bereich IT-Sicherheit anbietet. Ausgehend von meiner Erfahrung aus der Mitwirkung im Lernlabor Cybersicherheit bedarf es zur Erhöhung des Wissenstransfers weniger einer Verbesserung des Weiterbildungsangebots als der Schaffung von Anreizen für KMUs Mitarbeiter (trotz Fachkräftemangel) für die Teilnahme an IT-Sicherheitsweiterbildungen freizustellen.

Zur Beschlussvorlage:

Die in Punkt 6. erwähnte Möglichkeit zur Sperrung von Nutzerprofilen in sozialen Netzwerken und Medien kann ein erster Schritt zu einem Umgang mit der wachsenden Bedrohung sein. Allerdings kann es deutlich zielführender sein, die Plattformen selbst zu verpflichten, Betrugsversuche zu erkennen und einzudämmen und Benutzer proaktiv über mögliche Risiken, etwa durch öffentlich verfügbare Identitätsdaten, zu informieren.

Zu den Forderungen:

Es ist davon auszugehen, dass insbesondere die Forderungen in den Punkten 3 und 6 zu einer Verbesserung der IT-Sicherheit führen.

Abschließende Bemerkungen:

Die Politik ist als Gesetzgeber gefordert, Rahmenbedingungen zu schaffen, die den Betrieb eines Warnsystems im Bereich des Identitätsdiebstahls ermöglichen. Insbesondere sind solche Systeme ja selbst auch datenverarbeitende Systeme, die sich ohne Ausnahme an die rechtlichen Vorgaben halten müssen. Insbesondere ist es erforderlich, einem geeigneten Betreiber eines solchen Systems ein öffentliches Mandat zu erteilen. In Frage kommen dabei unterschiedliche Einrichtungen, sowohl im Bereich des Verbraucherschutzes, der Landesämter für den Datenschutz, dem BSI oder entsprechenden Forschungseinrichtungen.

gez. Prof. Dr. Michael Meier