LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/311**

08.08.2017

Antwort

der Landesregierung

auf die Kleine Anfrage 28 vom 30. Juni 2017
des Abgeordneten Matthi Bolte-Richter BÜNDNIS 90/DIE GRÜNEN
Drucksache 17/61

Angriffe auf IT-Systeme der Landesregierung

Vorbemerkung der Kleinen Anfrage

Die informationstechnische Infrastruktur der öffentlichen Hand ist ein bekanntes Ziel von Angriffen mit unterschiedlichsten Motiven. Vor dem Hintergrund der fortschreitenden Digitalisierung aller Verwaltungsabläufe steigt der Bedarf nach einer sicheren und vor Angriffen bestmöglich geschützten Systemarchitektur.

Die Angriffe – und damit auch die durch verschiedene Behörden geführten Statistiken – unterscheiden sich stark. Angriffe reichen von einfachen Spam-Mails mit kompromittierten Anhängen bis zu professionellen und schwerwiegenden Attacken. Je nach Definition weisen öffentliche Stellen teils eklatant unterschiedliche Zahlen hinsichtlich der Angriffe aus.

Mit der Kleinen Anfrage 2092 der 16. Wahlperiode (Drucksache 16/5580) wurden insbesondere Penetrationstests, also umfangreiche Sicherheitstests möglichst aller Systembestandteile und Anwendungen eines IT-Systems, abgefragt. Über derartige Tests seit der Antwort auf die besagte Anfrage (11.04.2014) liegen jedoch keine Informationen vor.

IT-Sicherheit erwächst jedoch nicht allein aus konsequenten Tests, sondern erfordert auch technische, organisatorische und insbesondere personelle (z.B. durch Fortbildung der Mitarbeiter*innen) Maßnahmen.

Der Minister für Wirtschaft, Innovation, Digitalisierung und Energie hat die Kleine Anfrage 28 mit Schreiben vom 4. August 2017 namens der Landesregierung im Einvernehmen mit dem Ministerpräsidenten und allen übrigen Mitgliedern der Landesregierung beantwortet.

Datum des Originals: 04.08.2017/Ausgegeben: 11.08.2017

Vorbemerkung der Landesregierung

Detaillierte Auskünfte zu den abgefragten Erkenntnissen lassen Rückschlüsse auf die in der Landesverwaltung eingesetzten Systeme und Methoden zu. Daher sind die Antworten so gefasst, dass die Fragen soweit wie möglich beantwortet werden, ohne jedoch schützenswerte Informationen preiszugeben, die einem Angreifer Hilfestellung geben würden.

1. Wie viele Angriffe auf IT-Systeme des Landes, der Ministerien, Landesbehörden und Landeseigenen Betriebe gab es seit dem 01.01.2014? (bitte monatlich, hilfsweise nach Quartalen aufschlüsseln)

Die Darstellung der Anzahl der Angriffe erfolgt jeweils ab der Verfügbarkeit entsprechender Daten. Bei den Zahlen sind eine hohe Volatilität der SPAM- und Angriffswellen sowie Effekte durch die ständige Optimierung von Regelwerken zu berücksichtigen. Die Netzbetreiber IT.NRW, LZPD und RZF erheben unterschiedliche Kennzahlen in Ihrem Verantwortungsbereich.

1) Spam-E-Mails

a. IT.NRW, LZPD

Quartal	Anzahl E-Mails gesamt (in Millionen)	davon Spam (in Prozent)
1/2016	20,6	57
2/2016	17,8	49
3/2016	18,7	55
4/2016	22,1	60
1/2017	16,8	45
2/2017	22,7	63

b. RZF

Quartal	Anzahl E-Mails gesamt (in Millionen)	davon Spam (in Prozent)
1/2014	2,3	44
2/2014	3,2	61
3/2014	2,6	52
4/2014	2,5	48
1/2015	2,1	43
2/2015	1,9	45
3/2015	2,3	55
4/2015	2,6	59
1/2016	2,7	62
2/2016	2,9	63
3/2016	4,4	76
4/2016	3,6	71
1/2017	3,0	64
2/2017	4,0	71

2) Ermittelte Alarme

a. IT.NRW, LVN IDS

Quartal	Anzahl Alarme	davon hohe Kritikalität
3/2015	578.153	182.830
4/2015	644.336	178.938
1/2016	788.844	192.533
2/2016	592.698	176.717
3/2016	652.310	229.458
4/2016	1.427.915	143.364
1/2017	132.865	70.960
2/2017	166.408	49.341

b. LZPD, CN-Pol (Corporate Network Polizei)

Derzeit sind in dem betreffenden Zeitraum keine erfolgreichen „Angriffe“ auf die IT-Systeme der Polizei NRW bekannt, alle getroffenen Sicherheitsvorkehrungen haben dies nach bislang vorliegenden Informationen verhindern können. Täglich werden verdächtige Internetzugriffe oder E-Mails im Rahmen eines übergreifenden IT-Sicherheitsmanagements auf Basis der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik entsprechend geprüft und abgefangen.

c. RZF, Sondernetz der Finanzverwaltung, Firewall-Alarme

Quartal	Summe der Zugriffe	Blockiert in %
1/2015	83.994.102	3,0
2/2015	68.030.592	3,3
3/2015	65.593.604	3,3
4/2015	70.133.728	2,3
1/2016	83.534.164	1,7
2/2016	89.328.975	1,0
3/2016	85.689.449	3,3
4/2016	73.413.298	4,0
1/2017	74.967.416	4,3
2/2017	52.216.029	5,3

3) sonstige Angriffe, die durch das CERT NRW untersucht und behandelt wurden:

Im Jahr 2014:

- Insgesamt 46 Fälle bestätigter Schadsoftwareinfektionen.
- Insgesamt 112 ernstzunehmende Angriffe untersucht.
- 56 E-Mailadressen aus der Landesverwaltung waren Teil einer großen Datei gestohlener Identitäten.
- Ein erfolgreicher Angriff auf ein Webangebot der Landesverwaltung wurde bemerkt. Die Schwachstelle war zum Zeitpunkt der Feststellung des Angriffs bereits geschlossen.
- Behandlung kompromittierter Benutzerkonten einer Behörde der Landesverwaltung im Zusammenhang mit der so genannten "Pony"-Schadsoftware.
- Ein Server der Landesverwaltung wurde für eine DDoS-Amplification Attacke missbraucht.
- DoS-Angriff auf ein Webangebot der Landesverwaltung.

- Angriff auf einige Systeme der Landesverwaltung zum Missbrauch in einem Botnetz.

Im Jahr 2015
- Insgesamt 117 Fälle von Schadsoftwareinfektionen.
- Insgesamt 236 ernstzunehmende Angriffe untersucht.
- Mehr als 60 Infektionen im Zuge einer massiven Welle mit gefälschten DHL- und UPS-Paket-Zustellbenachrichtigungen.
- Infektion mehrerer Terminalserver-Accounts mit einem Verschlüsselungstrojaner (ohne Schadensauswirkung).
- Teslacrypt-Infektionen (siehe Vorlage 16/3631, Strafanzeige)

Im Jahr 2016
- Insgesamt 61 Fälle von Schadsoftwareinfektionen.
- Insgesamt 201 ernstzunehmende Angriffe untersucht.
- Einbruchsversuch in einen Webserver detektiert. Die Einbrecher versuchten erfolglos den Server, anscheinend für den Versand von Spam und Phishingmails bzw. Bankingtrojaner, zu missbrauchen.
- Unautorisierte Zugriffe und Vandalismus bei einer Datenbank (Strafanzeige).

Im Jahr 2017 (Stichtag 1.7.2017)
- Bisher insgesamt 58 ernstzunehmende Angriffe untersucht.
- Ein Einbruch in 3 Webangebote auf einem Sammelserver (mit insg. ca. 200 Webangeboten) wurde festgestellt.

2. Welche Definition eines Angriffs legt die Landesregierung dabei zugrunde?

Als Maßstab für die Beantwortung der Frage 1 wurde jede nicht bestimmungsgemäße Nutzung eines IT-Systems angelegt.

3. Welche Qualität – sowohl hinsichtlich der Integrität der Einzel- wie der Gesamtsysteme als auch hinsichtlich möglicher strafrechtlicher Relevanz – hatten die in Frage 1 erfragten Angriffe jeweils?

Die vorliegenden Informationen sind bereits in die Beantwortung der Frage 1 eingeflossen.

4. Welche Penetrationstests wurden seit 2014 bei den Behörden und Einrichtungen des Landes durchgeführt (bitte einzeln aufschlüsseln unter Angabe des Datums, der überprüften Stelle und – soweit unter Sicherheitsaspekten möglich – der Ergebnisse)

Penetrationstests werden über unterschiedlich lange Zeiträume durchgeführt, da diese abhängig von der Komplexität des Betrachtungsgegenstandes sind. Die Dokumentation des Zeitpunktes hat keinen besonderen Nutzwert und wird daher nicht zentral erhoben. Eine nachträgliche Erhebung ist innerhalb des zur Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Zeitrahmens nicht leistbar.

Für das Landesverwaltungsnetz (IT.NRW):

Im Jahr 2014
Alle Systeme von IT.NRW, die öffentliche IP-Adressen verwenden, wurden mehrfach auf bekannte Schwachstellen überprüft. Neben bekannten Schwachstellen in Standardsoftware, die turnusmäßig gepatcht und abgesichert werden, wurden 230 Schwachstellen in Webanwendungen erkannt und einer Risikobehandlung zugeführt, davon 12 der Kategorie "kritisch" und 85 der Kategorie "hoch".
Zusätzlich wurden 10 anlassbezogene Sicherheitstests von IT-Systemen oder Verfahren durchgeführt und die erkannten Probleme beseitigt. (Kritisch: 4, Hoch: 5, Mittel: 4 , Niedrig: 1)

Im Jahr 2015
Alle Systeme von IT.NRW, die öffentliche IP-Adressen verwenden, wurden mehrfach auf bekannte Schwachstellen hin überprüft. Neben bekannten Schwachstellen in Standardsoftware, die turnusmäßig gepatcht und abgesichert werden, wurden 188 Schwachstellen in Webanwendungen erkannt und einer Risikobehandlung zugeführt, davon 14 der Kategorie "kritisch" und 116 der Kategorie "hoch".
Zusätzlich wurden 9 anlassbezogene Sicherheitstests von IT-Systemen oder Verfahren durchgeführt und die erkannten Probleme beseitigt. Zwei PEN-Tests waren dabei ohne Auffälligkeiten. (Kritisch: 3, Hoch: 4, Mittel: 3 , Niedrig: 6)

Im Jahr 2016
Alle Systeme von IT.NRW, die öffentliche IP-Adressen verwenden, wurden mehrfach auf bekannte Schwachstellen hin überprüft. Im Jahresverlauf identifizierte und meldete das CERT NRW darüber hinaus 83 Schwachstellen, die sodann einer Risikobehandlung zugeführt wurden, davon 18 der Kategorie "kritisch" und 31 der Kategorie "hoch".
Zusätzlich wurden 11 anlassbezogene Sicherheitstests von IT-Systemen oder Verfahren durchgeführt und die erkannten Probleme beseitigt. Zwei PEN-Tests waren dabei ohne Auffälligkeiten. (Kritisch: 2, Hoch: 11, Mittel: 7 , Niedrig: 3)

Im Jahr 2017
Alle Systeme von IT.NRW, die öffentliche IP-Adressen verwenden, werden mehrfach auf bekannte Schwachstellen hin überprüft. In 2017 wurden bis zum 5.7.2017 darüber hinaus 29 Schwachstellen vom CERT NRW gefunden und gemeldet, davon 11 der Kategorie "hoch" und keine der Kategorie "kritisch".
Bislang wurden 13 anlassbezogene Sicherheitstests von IT-Systemen oder Verfahren durchgeführt und die erkannten Probleme beseitigt. Zwei PEN-Tests waren dabei ohne Auffälligkeiten.

Für das Sondernetz der Finanzverwaltung:
Der komplette Internet-IP-Bereich der Finanzverwaltung wird seit 2009 jährlich geprüft. Zwischen den Intervallen einzusetzende Web-Lösungen werden ebenfalls durch Penetrationstests abgesichert. Die Beseitigung von schwerwiegenden Schwachstelle wird in einem Nachtest überprüft.

Für das Corporate Network der Polizei:
Das LZPD NRW beauftragt regelmäßig Penetrationstests für die Polizei NRW und begleitet diese. Penetrationsziele sind hierbei sowohl polizeiliche IT-Infrastruktur-Komponenten als auch zentrale polizeiliche Fachverfahren. Aufgrund datenschutzrechtlicher und sicherheitsrelevanter Aspekte werden die im Einzelnen penetrierten Verfahren und IT-Systeme sowie die hieraus resultierenden Ergebnisse nicht weiter erläutert.

5. Welche technischen, personellen und organisatorischen Maßnahmen zur Risikominimierung wurden seit 01.01.2014 geplant und umgesetzt?

Die Anzahl der technischen Maßnahmen ist nicht zu beziffern, da Informationssicherheit als Prozess die rasante Fortentwicklung der Informationstechnik stets begleitet. Prinzipiell sind alle in der Landesverwaltung betriebenen Verfahren unter kontinuierlicher Weiterentwicklung. Bzgl. einer Beschreibung einzelner Maßnahmen wird auf die Vorbemerkung verwiesen.

IT.NRW errichtet eine zentrale Betriebsinfrastruktur, die standardmäßig Schutzbedarfe „Normal“ und „Hoch“ für Verfahren nach BSI-IT-Grundschutz erfüllt. Eine Zertifizierung ist vorgesehen.

Die Landesverwaltung hat aktuell ein Lead-Buyer-Verfahren abgeschlossen, dass die Beschaffung einer Lösung zum virtualisierten Surfen eröffnet.

Bzgl. der personellen und organisatorischen Maßnahmen incl. der Sensibilisierungsmaßnahmen für die Beschäftigten der Landesverwaltung wird auf den Sachstandsbericht über die Arbeit des CIO (Zf. II.3), Vorlage 16/4742, vom 6.2.2017 verwiesen.

Gegenwärtig stehen insgesamt 68 Stellen in der Landesverwaltung für die Umsetzung des Informationssicherheitsmanagementsystems zur Verfügung. Davon sind 46 Stellen bereits besetzt, für weitere 5 Stellen ist das Besetzungsverfahren abgeschlossen. Die restlichen 17 Stellen befinden sich im Ausschreibungs- bzw. Auswahlverfahren.