Landtag von Sachsen-Anhalt

Drucksache 7/2697
11.04.2018

Antwort der Landesregierung auf eine Kleine Anfrage zur schriftlichen Beantwortung

Abgeordnete Eva von Angern (DIE LINKE)

Angriffe auf die Informationstechnik und das Datennetzwerk des Landes Sachsen-Anhalt

Kleine Anfrage - **KA 7/1554**

Vorbemerkung des Fragestellenden:

Ausländische Hacker sind nach Informationen der Deutschen Presse-Agentur in das bislang als sicher geltende Datennetzwerk des Bundes und der Sicherheitsbehörden eingedrungen. Cyberspione der mutmaßlich russischen Gruppe „APT28“ hätten erfolgreich das deutsche Außen- und das Verteidigungsministerium angegriffen, hieß es in Sicherheitskreisen. Es sei Schadsoftware eingeschleust worden, die Angreifer hätten auch Daten erbeutet.

In Sachsen-Anhalt gab es im Jahr 2016 in vier Krankenhäusern, beim Verfassungsschutz, in einer Stadtverwaltung und in vier Polizeidienststellen Fälle von Cyberkriminalität.

Antwort der Landesregierung
erstellt vom Ministerium der Finanzen

Vorbemerkung der Landesregierung:

Ein Angriff ist laut der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Hinweis: Die Drucksache steht vollständig digital im Internet/Intranet zur Verfügung. Die Anlage ist in Word als Objekt beigefügt und öffnet durch Doppelklick den Acrobat Reader.
Bei Bedarf kann Einsichtnahme in der Bibliothek des Landtages von Sachsen-Anhalt erfolgen oder die gedruckte Form abgefordert werden.

(Ausgegeben am 11.04.2018)

Zur Prävention im Vorfeld und für die Unterstützung bei der Abwehr konkreter Angriffe beteiligt sich das Land Sachsen-Anhalt am länderübergreifenden Computer Emergency Response Team (CERT) Nord. Das CERT Nord ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen der Bundesländer Bremen, Hamburg und Sachsen-Anhalt. Das CERT Nord wiederum ist Mitglied im Verwaltungs-CERT-Verbund (VCV).

Dies ist eine Informationsaustauschplattform der CERTs der öffentlichen Verwaltung in Deutschland. Beteiligt am VCV sind neben den CERTs der Bundesländer auch das CERT-Bund sowie das BSI.

1. Wie ist das Datennetz des Landes Sachsen-Anhalt - einschließlich des Datennetzwerks des Landtages - vor derartigen möglichen Angriffen geschützt?

Die Informationstechnik und das Datennetzwerk des Landtages werden durch die Landtagsverwaltung in eigener Zuständigkeit betrieben. Insofern kann hierüber keine Auskunft erteilt werden.

Das Landesdatennetz ITN-LSA ist mit den einschlägigen technischen Schutzeinrichtungen zum Perimeterschutz von Datennetzwerken, wie beispielsweise einer zentralen Firewall, einem SPAM-Filter und Virenscanner nach dem Stand der Technik, ausgerüstet. Darüber hinaus betreiben teilweise die Ressorts, als Teilnehmer am Landesdatennetz, weitere dislozierte technische Schutzeinrichtungen in ihrem Zuständigkeitsbereich.

Bei Betrieb und Erweiterung des Landesdatennetzes ITN-LSA werden die Richtlinien, Konzepte und Empfehlungen des BSI im Rahmen der vorhandenen personellen und finanziellen Ausstattung im Land, soweit möglich, berücksichtigt bzw. umgesetzt.

Durch das CERT Nord erfolgen in regelmäßigen Abständen Prüfungen des Landesdatennetzes auf mögliche von außerhalb ausnutzbare Schwachstellen. Bei Feststellungen werden die hierfür zuständigen Stellen umgehend und unter Nennung von Maßnahmenempfehlungen informiert. Darüber hinaus ist das Landesdatennetz über weitere technische Schutzmaßnahmen vor möglichen Angriffen geschützt.

2. Wie viele Hackerangriffe auf die Informationstechnik und das Datennetzwerk des Landes Sachsen-Anhalt wurden in den letzten 3 Jahren registriert? Bitte nach Jahren und Landesbehörden/Landtag getrennt aufschlüsseln.

Eine große Anzahl an Angriffen wird bereits durch die Firewallkomponente abgewiesen. Hierbei erfolgt jedoch keine unmittelbare Klassifizierung in einer Kategorie wie beispielsweise „Angriff“, da die Firewallkomponente Datenpakete allein anhand eines vorgegebenen Regelwerks weiterleitet oder abweist. Werden Datenpakete abgewiesen, so kann daraus nicht zwangsläufig auf einen abgewehrten Angriff geschlossen werden. Vielmehr kann die Ursache für diese Maßnahme auch in einer definierten Regel liegen, eine bestimmte Kommunikationsverbindung bewusst nicht zuzulassen (z. B. aufgrund von Datenschutzer-

fordernissen). Direkt an der Firewallkomponente können somit nicht unmittelbar abgewiesene Angriffe abgelesen oder registriert werden.

Die unspezifischen und in bestimmten Zeiträumen immer wieder großflächig stattfinden Angriffe per Email (als SPAM, als Phishing oder mit Schadsoftware-Inhalt) können naturgemäß ebenfalls nicht direkt quantitativ gemessen werden. Viele dieser SPAM- Emails werden bereits vom Mail-Gateway des Landes mittels „Grey-Listing“ abgewiesen. Sofern derartige Emails doch in das elektronische Postfach der Anwender gelangten, wurden diese in der überwiegenden Anzahl vom Virenscanner neutralisiert bzw. von den für die Informationssicherheit sensibilisierten Mitarbeitern gelöscht, ohne in jedem konkreten Einzelfall eine Meldung hierüber abzusetzen. Dies wäre, allein schon aufgrund der hohen Anzahl von derartigen Emails, ohne Beeinträchtigung des Dienstbetriebs nicht durchführbar.

Bei neuen und bisher nicht im Rahmen der Sensibilisierung vorgestellten Angriffsmustern (vorgebliche Rechnungen, Benachrichtigungen über Warensendungen, vermeintliche Zahlungserinnerungen usw.) erfolgte ab 2016 in sieben Fällen eine direkte Meldung an das CERT (Anlage 1). Erfolgreiche Angriffe anderer Art wurden dem CERT seit 2016 in acht Fällen gemeldet (Anlage 2). Bei schwerwiegenden Angriffen bzw. auf Veranlassung der jeweils betroffenen Stellen wurden die zuständigen Strafverfolgungsbehörden eingeschaltet.

Dementsprechend wurden der Polizei strafrechtlich relevante Sachverhalte gemeldet. Die Falldaten zur Beantwortung der Fragen wurden im Vorgangsbearbeitungssystem IVOPOL für den Zeitraum vom 01.01.2015 bis 31.12.2017 recherchiert. Hierfür wurden die dem bundeseinheitlich definierten Deliktbereich der Cybercrime im engeren Sinne (i. e. S.) zugeordneten Delikte zugrunde gelegt, da der von der Fragestellerin verwendete Begriff des „Hackerangriffs“ rechtlich nicht definiert und somit nicht recherchierbar ist. Cybercrime i. e. S. umfasst Straftaten, bei denen Elemente der elektronischen Datenverarbeitung (EDV) in den Tatbestandsmerkmalen der jeweiligen Strafnorm genannt sind.

3. Welche Kommunikations- bzw. Informationswege sind bei Angriffen auf die Informationstechnik und das Datennetzwerk des Landes Sachsen-Anhalt einzuhalten?
Wer ist in welchem Umfang zu informieren?

Entsprechend der im Land selbst sowie der zwischen Bund und Ländern abgestimmten Prozesse meldet jedes Ressort der unmittelbaren Landesverwaltung Sachsen-Anhalts bei Eintritt eines meldewürdigen Ereignisses dieses parallel an das CERT Nord und an die/den Informationssicherheitsbeauftragte/n des Landes mittels des hierfür vorgeschriebenen Meldeformulars. Dies kann auf verschiedenen Übertragungswegen erfolgen.

Sofern nach Einschätzung der/des Informationssicherheitsbeauftragten des Landes eine allgemeine Betroffenheit für die Ressorts im Land Sachsen-Anhalt gegeben ist, werden diese über einen vorab festgelegten Verteiler informiert.

Mittels des VCV-Referenz-Meldeprozesses meldet das CERT Nord anhand vorgegebener Bewertungskriterien solche IT-Sicherheitsvorfälle, bei denen Aus-

wirkungen auf die Länder oder den Bund nicht ausgeschlossen werden können oder die auch für andere als relevant eingeschätzt werden, an das Lage- und Analysezentrum des VCV. Dieses informiert im Rahmen der Vorfallsbearbeitung wiederum das CERT Bund und dieses erforderlichenfalls weitere Länder CERTs. Für das Land Sachsen-Anhalt relevante Informationen anderer Länder CERTs oder des CERT Bund erreichen Sachsen-Anhalt entsprechend der definierten Prozesse auf dem umgekehrten Weg.

Bei einer Meldung werden neben den allgemeinen Angaben zur betroffenen Behörde, dem Meldenden sowie den Kontaktdaten für Rückfragen inhaltlich eine Sachverhaltsschilderung sowie eine vorläufige Klassifizierung des Vorfalls durch das meldende Ressort übermittelt.

4. Welche Datenbestände incl. personenbezogener Daten waren aufgrund der unter Ziffer 2 benannten Fälle betroffen?

Es wurden keine Datenbestände erlangt. In allen dargestellten Fällen handelte es sich nicht um zielgerichtete Angriffe auf die geschädigten Institutionen; vielmehr wurden täterseitig Schadsoftwares per Zufallsprinzip über das Internet verteilt.

5. Welche Folgen sowie Schäden und in welcher Höhe wurden durch Cyberangriffe auf das Datennetzwerk des Landes hervorgerufen?

Phänomentypisch beschränken sich die Schäden zumeist auf Arbeitsausfallzeiten bzw. Folgekosten aufgrund der nachfolgenden Beauftragung von IT-Dienstleistern. Ausfallzeiten seitens öffentlicher Bereiche sind regelmäßig nur schwer auszuweisen. Derartige Schäden wurden bei Anzeigenerstattung bisher nicht angegeben und konnten demnach nicht recherchiert werden.

6. Welche Maßnahmen zur Aufklärung und zum Schutz vor möglichen Hackerangriffen wurden bisher realisiert? Welche weiteren Maßnahmen sind geplant?

Der Betrieb, die Pflege und der Schutz des informationstechnischen Netzes der Landesverwaltung Sachsen-Anhalts liegen in der Zuständigkeit des Ministeriums der Finanzen. Die Maßnahmen zum Schutz der landeseigenen Infrastruktur und den Einrichtungen des Landes sowie der im Rahmen des Verwaltungshandelns erhobenen Daten der Bürgerinnen und Bürger (z. B. durch das Steuergeheimnis nach § 30 AO besonders geschützte Daten im Steuerverfahren) vor digitalen Angriffen basieren auf vier Säulen und umfassen technische Schutzmaßnahmen, organisatorische Maßnahmen, Präventionsmaßnahmen und Sensibilisierungsmaßnahmen für die Bediensteten der Landesverwaltung. Der Betrieb von Fachverfahren innerhalb der Landesregierung des Landes Sachsen-Anhalt erfolgt in einem nach den Standards des BSI zertifizierten und vom TÜV Nord mit dem Sicherheitszertifikat Trusted Site Infrastructure ausgezeichneten Rechenzentrum, der Dataport AöR.
Im Rahmen des Betriebs des Rechenzentrums trägt die Dataport AöR auftragsgemäß dafür Sorge, dass die Serversysteme dem aktuellen Stand der Technik entsprechend ausgestattet sind.

Im Rahmen des Aufbaus des neuen Landesdatennetzes ITN-XT werden zentrale schützenswerte IT-Räume in Liegenschaften des Landes baulich und technisch besonders ertüchtigt. Damit soll ein verbessertes Niveau in den Bereichen Zutrittsschutz, baulicher Brandschutz, Energieversorgung und Klimatisierung, mit dem Ziel eine hohe Verfügbarkeit und Widerstandsfähigkeit der darin untergebrachten IT-Komponenten gegen technische Ausfälle, Sabotage und sonstige Bedrohungen sicherzustellen.

Im Ministerium der Finanzen des Landes Sachsen-Anhalt soll ein Kompetenzteam Informationssicherheit aufgebaut werden. Dieses soll neben der Aufgabe „Vorbereitung der BSI-Zertifizierung des Informationsverbundes ITN-XT“ auch allen Ressorts des Landes auf Anforderung mit aufgabenbezogenem Fachwissen und mit Dienstleistungen im Bereich der Informationssicherheit zur Verfügung stehen.

7. Welche konkreten Vorkehrungen wurden getroffen, um zukünftige Hackerangriffe und den unbefugten Zugriff auf Datenbestände zu verhindern?

Da die Netze der Landesverwaltung durch den Einsatz von Sicherheitskomponenten an den jeweiligen Netzübergängen angemessen geschützt werden, dienen als Angriffswege vermehrt die üblicherweise auch in der Verwaltung erforderlichen und daher zugelassenen Internet-Protokolle HTTP (Webzugriff) und SMTP (Email).Die Angriffe bestehen überwiegend in der (wahllosen) Zusendung von SPAM- bzw. Phishing Emails mit gefälschten Absenderadressen. Durch diese Emails sollen Anwender dazu gebracht werden, mit einem Schadprogramm infizierte Anhänge zu öffnen oder eine solche Schadsoftware über in der Email enthaltene Links herunterzuladen. Der wichtigste Erfolgsfaktor für die Erreichung eines angemessenen Sicherheitsniveaus sind daher verantwortungsbewusste und geschulte Mitarbeiter. Die Anzahl der landesweit angebotenen Sensibilisierungsveranstaltungen für Mitarbeiter der Landesverwaltung wurde auf drei Veranstaltungen pro Jahr erhöht.

Weiterhin wird derzeit, als große Maßnahme des Landes Sachsen-Anhalt zur Erneuerung veralteter IT-Infrastruktur, das bisherige informationstechnische Netz der Landesverwaltung Sachsen-Anhalts (ITN-LSA) durch ein leistungsfähigeres und den aktuellen Stand der Sicherheitstechnik berücksichtigendes neues Landesdatennetz (ITN-XT) ersetzt. Innerhalb dieses neuen Datennetzes werden Sicherheitskomponenten nach dem aktuellsten Stand der Technik eingesetzt. So erfolgt beispielsweise die Datenübertragung auf dem Übertragungsweg nunmehr grundsätzlich stark verschlüsselt mit vom BSI zertifizierten Verschlüsselungskomponenten.

Die für die Informationssicherheit im Land zuständigen Stellen stehen in intensivem Kontakt mit den anderen Bundesländern sowie dem BSI und beteiligen sich aktiv an den einschlägigen Bund-Länder-Arbeitsgruppen auf dem Arbeitsgebiet der Informationssicherheit. Alle relevanten Informationen für Maßnahmen zur Abwehr von Bedrohungen - bereits im Vorfeld - und für die Unterstützung bei der Erkennung und Abwehr konkreter Angriffe werden engmaschig ausgewertet und berücksichtigt.

Datum	Behörde / Institution	Angriffsvektor / Art der Bedrohung	Meldeformular CERT Nord
10.05.2016	lgst@npd-sachsen-anhalt.de	Pishingmails	nein
04.05.2017	einzelne Rechner im Ministerium	Virenalarm mit Bereinigung	nein
24.08.2017	Ministerium für Justiz und Gleichstellung	Spammail	nein
24.08.2017	Ministerium für Justiz und Gleichstellung	Spammail	nein
24.08.2017	Finanzgericht LSA	Spammail	nein
18.09.2017	Ministerium für Bildung	Spammail	nein
05.10.2017	Ministerium für Bildung	Spammail	nein

Datum	Behörde / Institution	Angriffsvektor / Art der Bedrohung	Meldeformular CERT Nord
09.02.2016	Ministerium für Bildung	TeslaCrypt 3	nein
03.05.2016	Verfassungsschutz	Angriff: keine weiteren Infos	nein
06.12.2016	Ministerium für Bildung	Verschlüsselung	ja
24.01.2017	Ministerium der Finanzen	Maleware + Verschlüsselung	nein
02.06.2017	Ministerium für Finanzen	Verschlüsselung	nein
30.08.2017	Landtag	Angriff	nein
19.09.2017	LVermGeo	Verschlüsselung	ja
26.09.2017	Ministerium für Justiz und Gleichstellung	Verschlüsselung (Nachmeldung 13.09. / 20.09.)	nein

Anlage 3

Delikttext	Name	nationale Rechtsform	Tatdatum bis	Jahr
Computersabotage	Polizeidirektion Sachsen-Anhalt Ost	Landeseinrichtung	09.04.2015	2015
vorbereitendes Ausspähen/Abfangen von Daten § 202c StGB	Polizeidirektion Sachsen-Anhalt Ost, Polizeirevier Dessau-Roßlau	Landeseinrichtung	14.10.2015	2015
Fälschung beweiserheblicher Daten § 269 StGB	Polizeidirektion Sachsen-Anhalt Ost, Polizeirevier Dessau-Roßlau	Landeseinrichtung	14.10.2015	2015
Computersabotage	Technisches Polizeiamt	Landeseinrichtung	04.04.2016	2016
Computersabotage	Landesamt für Verfassungsschutz	Landeseinrichtung	06.04.2016	2016
Computersabotage	Polizeirevier Harz - Revierkommissariat Wernigerode	Allgemeinheit	17.04.2016	2016
Computersabotage	Landesverfassungsgericht Sachsen-Anhalt	Körperschaft	02.03.2017	2017
Computersabotage	Landtag LSA	Landeseinrichtung	24.08.2017	2017
Computersabotage	Landtag Sachsen-Anhalt	Landeseinrichtung	30.08.2017	2017
Computersabotage	Amtsgericht Stendal	Landeseinrichtung	18.09.2017	2017
Computersabotage	Technisches Polizeiamt Magdeburg	Landeseinrichtung	03.11.2017	2017
Computersabotage	Landeskriminalamt Sachsen-Anhalt	Landeseinrichtung	03.11.2017	2017