LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/5429**

27.03.2014

Antwort

der Landesregierung

auf die Kleine Anfrage 2062 vom 21. Februar 2014
des Abgeordneten Daniel Schwerd PIRATEN
Drucksache 16/5133

BSI-Meldung über 16 Millionen kompromittierte Login-Datensätze: Ist die Landesregierung aktiv?

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 2062 mit Schreiben vom 26. März 2014 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin und allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

"Es ist keine Schande nichts zu wissen, wohl aber, nichts lernen zu wollen." – Sokrates

Laut des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurde im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden 16 Millionen gestohlenen Login-Datensätze für Benutzerkonten im Internet entdeckt.[1]

Logins bestehen aus zwei Teilen: Einem Benutzernamen, oft in Form einer E-Mail-Adresse, und einem Passwort. Im Internet und in Intranets werden solche Logins für eine ganze Reihe unterschiedlichster Dienste verwendet. Wer im Besitz der Login-Daten ist, kann im Namen des registrierten Nutzers die entsprechenden Dienste meist nach Belieben nutzen. Fallen diese Login-Daten in die falschen Hände – wie in den 16 Millionen Fällen, von denen das BSI berichtet - so besteht die akute Gefahr eines Identitätsdiebstahls. Diese Gefahr ist noch größer, wenn Nutzer die gleichen Kombinationen aus E-Mail-Adresse und Passwort für mehrere Dienste verwenden, auf die mögliche Datendiebe dann ebenfalls Zugriff erlangen können.

[1] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html

Datum des Originals: 26.03.2014/Ausgegeben: 01.04.2014

Die Liste mit den gestohlenen Login-Datensätzen liegt dem BSI mindestens seit Dezember, vermutlich sogar seit August 2013 vor. Seit dem 21.01.2014 besteht auf der Webseite des BSI die Möglichkeit, eigene E-Mail-Adressen dahingehend zu prüfen, ob diese in der BSI-Liste kompromittierter Login-Datensätze auftauchen. Liegt ein Treffer vor, so muss davon ausgegangen werden, dass ein Login, in dem die entsprechende E-Mail-Adresse als Benutzername dient, gestohlen wurde.

Die zuständige Staatsanwaltschaft übermittelte bereits im August 2013 über das Bundeskriminalamt einen Datensatz mit ca. 600 betroffenen E-Mail-Adressen der Bundesverwaltung und 17 E-Mail-Adressen des Bundestags an das BSI zur Analyse.[2]

Im Land Nordrhein-Westfalen werden von Regierung, Ministerien und Behörden des Landes sowie landeseigenen Betrieben diverse E-Mail-Adressen verwendet. Diese werden sowohl von zentralen Stellen als auch von einzelnen Mitarbeitern für die unterschiedlichsten Zwecke benutzt.

Mit dieser kleinen Anfrage möchte ich erfahren, inwieweit geprüft wurde, ob E-Mail-Adressen des Landes, der Regierung, von Ministerien, Landesbehörden oder landeseigenen Betrieben bzw. dienstliche Adressen der jeweiligen Mitarbeiter betroffen sind.

1. Wann haben Behörden des Landes NRW erstmals von der BSI-Liste der betroffenen E-Mail-Adressen Kenntnis erlangt? Bitte geben Sie an, auf welchem Wege die Kenntnis erlangt wurde.

Das CERT NRW als zentrale Stelle für IT-Sicherheit in der Landesverwaltung hat am 21. Januar 2014 durch eine entsprechende Meldung in den Medien erstmals Kenntnis von dem Sachverhalt erlangt und die Ansprechpartner in den Behörden und Einrichtungen des Landes am selben Tag darüber informiert. Gleichzeitig wurde auch der Hinweis auf die Webseite https://www.sicherheitstest.bsi.de weitergegeben.

Mit Schreiben vom 24. Januar 2014 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) dem Land eine Übersicht („BSI-Liste“) zugeleitet. Konkrete E-Mail-Adressen waren in der BSI-Liste nicht enthalten. Auf Nachfrage mehrerer Länder hat das BSI mit Schreiben vom 30. Januar 2014 als Grund hierfür angegeben, dass es die E-Mail-Adressen von der Staatsanwaltschaft Verden als Herrin des Verfahrens mit einer konkreten und engen Zweckbestimmung erhalten hat. Diese Zweckbindung machte nach Auskunft des BSI eine Übermittlung der konkreten E-Mail-Adressen an die Länder nicht möglich.

Das Land hat daraufhin am 4. Februar 2014 ein entsprechendes Amtshilfeersuchen für die Domain „.nrw.de“ über das CERT Niedersachsen bei der federführenden Staatsanwaltschaft Verden gestellt. Die konkreten E-Mail-Adressen wurden dem Land daraufhin zur Verfügung gestellt. Ab dem 10. Februar 2014 konnten schließlich die Behörden und Einrichtungen des Landes vom CERT NRW die entsprechenden konkreten E-Mail-Adressen ihres Ressorts anfordern.

Im Rahmen polizeilicher Ermittlungen hatte das ermittlungsführende Landeskriminalamt Niedersachsen dem Landeskriminalamt Nordrhein-Westfalen bereits am 06. August 2013 per E-Mail 17 E-Mail-Adressen und Passwörter sowie am 2. September 2013 vier weitere Datensätze mitgeteilt, die aufgrund der Domain „polizei.nrw.de“ offensichtlich der Polizei Nordrhein-Westfalen zugeordnet werden konnten. Anhaltspunkte dafür, dass auch weitere Stellen der

[2] http://www.spiegel.de/netzwelt/web/bsi-schwieg-angeblich-monate-lang-ueber-identitaetsklau-a-954025.html

Landesverwaltung davon betroffen sein könnten, lagen zu dem damaligen Zeitpunkt nicht vor.

2. Wann hat die Landesregierung bzw. haben zuständige Behörden des Landes vom BSI die Liste der E-Mail-Adressen (vollständig oder in den für die Behörden des Landes relevanten Teilen) angefragt?

Hierzu verweise ich auf meine Antwort zu Frage 1.

3. Welches Ergebnis hatte die systematische Suche nach Übereinstimmungen zwischen der Adressliste des BSI und den E-Mail-Adressen von Regierung, Ministerien und Behörden des Landes sowie landeseigenen Betrieben (bzw. den Dienst-E-Mail-Adressen ihrer Mitarbeiter)? Bitte schlüsseln Sie das Prüfergebnis nach Behörden auf und geben Sie die jeweilige Trefferanzahl und den Zeitpunkt des Tests an.

Die Anzahl der jeweils betroffenen E-Mail-Adressen ergab sich aus der „BSI-Liste“, die als Anlage 1 beigefügt ist. In Verbindung mit der im Rahmen der Amtshilfe bereitgestellten Liste war eine Zuordnung zu einzelnen E-Mail-Adressen möglich. Die Durchführung des BSI-Sicherheitstest durch sämtliche Mitarbeiterinnen und Mitarbeiter der Landesverwaltung wurde damit entbehrlich.

4. Welche der auf der Adressliste des BSI gefundenen E-Mail-Adressen des Landes sind sicherheitsrelevanten Bereichen zuzuordnen? Bitte listen Sie die entsprechenden Fälle (ggf. verkürzt) und das damit verbundene Risiko auf.

Es waren keine sicherheitsrelevanten Bereiche betroffen.

5. Welche Maßnahmen werden bzw. wurden in Bezug auf die in der Adressliste des BSI gefundenen E-Mail-Adressen des Landes ergriffen? Bitte listen Sie jede einzelne Maßnahme mit Zeitpunkt bzw. Zeitplan der Umsetzung auf.

Die von den Ressorts ergriffenen Maßnahmen sind in der anliegenden Übersicht (Anlage 2) dargestellt.

Anlage 1 zur Kleinen Anfrage 2062
Übersicht über die betroffenen E-Mail-Domänen der Landesverwaltung NRW

afao-moenchengladbach.nrw.de	1
ag-bruehl.nrw.de	1
ag-duesseldorf.nrw.de	1
ag-koeln.nrw.de	2
ag-lemgo.nrw.de	1
ag-siegen.nrw.de	1
bergheim.polizei.nrw.de	1
bezreg-arnsberg.nrw.de	1
bezreg-detmold.nrw.de	1
bezreg-muenster.nrw.de	4
blb.nrw.de	11
brar.nrw.de	1
brd.nrw.de	4
brdt.nrw.de	4
brk.nrw.de	1
brms.nrw.de	2
bro.nrw.de	1
duisburg.polizei.nrw.de	1
fc.polizei.nrw.de	1
fm.nrw.de	3
gd.nrw.de	1
ggrz-hagen.nrw.de	1
idf.nrw.de	12
im.nrw.de	4
jak.nrw.de	1
jva-essen.nrw.de	1
jva-gelsenkirchen.nrw.de	1
jva-hamm.nrw.de	1
jva-siegburg.nrw.de	2
jva-werl.nrw.de	1
katho.nrw.de	1
landtag.nrw.de	10
lanuv.nrw.de	2
lbme-k.nrw.de	1
lbv.nrw.de	2
lds.nrw.de	2
lg-koeln.nrw.de	1
lk-wl.nrw.de	2
lk.nrw.de	1
loegd.nrw.de	1
lsg.nrw.de	1
lua.nrw.de	1
lverma.nrw.de	2
lwk.nrw.de	4
lzg.gc.nrw.de	1
mags.nrw.de	1
masqt.nrw.de	1

mbv.nrw.de	3
medienberatung.nrw.de	2
mettmann.polizei.nrw.de	1
mgsff.nrw.de	2
mik.nrw.de	1
msw.nrw.de	6
muenster.polizei.nrw.de	1
munlv.nrw.de	4
mwa.nrw.de	1
nrw.de	8
olg-duesseldorf.nrw.de	1
olg-hamm.nrw.de	1
olg-koeln.nrw.de	1
pa.nrw.de	1
polizei.nrw.de	18
schule.nrw.de	2
sta-dortmund.nrw.de	1
sta-duesseldorf.nrw.de	2
stafa-ar.nrw.de	1
stafa-do.nrw.de	1
stafua-owl.nrw.de	1
stk.nrw.de	3
strassen.nrw.de	7
sts.nrw.de	1
stua-du.nrw.de	1
studienseminare.nrw.de	1
vamt-d.nrw.de	3
vamt-ge.nrw.de	2
vamt-k.nrw.de	1
wald-und-holz.nrw.de	1
wme.nrw.de	1
wss.nrw.de	1
zvs.nrw.de	3

Anlage 2 zur Kleinen Anfrage 2062
Nach Bekanntgabe der E-Mail-Adresssen durchgeführte Maßnahmen der Ressorts

Ressort	Maßnahmen
STK	Die betroffenen Kolleginnen und Kollegen wurden persönlich angesprochen und auf die Empfehlungen des BSI verwiesen (Passwortänderung, unterschiedliche Passwörter bei unterschiedlichen Internet-Instanzen, keine Verwendung der dienstlichen Mail-Adresse für private Zwecke etc.).
MSW	Nach der Bekanntgabe der betroffenen E-Mailadressen durch das CERT NRW Mitte Februar wurden die betroffenen Beschäftigten über den Sachverhalt informiert und aufgefordert, ihre Zugangsdaten zu ändern. Zudem wurden die PCs der Betroffenen im Ministerium eingehend auf mögliche Computerviren überprüft – ohne besondere Auffälligkeiten zu finden. Die Behörden und Einrichtungen im Geschäftsbereich, die ebenfalls von dem Identitätsdiebstahl betroffen waren, wurden gezielt informiert und gebeten, vergleichbare Maßnahmen zu treffen.
FM	Nachfolgende Maßnahmen wurden sofort nach Bekanntgabe der E-Mail-Adressen durchgeführt: - Sicherheitstest des BSI durchgeführt - Belehrung und Einzelgespräche mit den Betroffenen durchgeführt - Passworte der Betroffenen geändert Für eine betroffene E-Mail-Adresse wurde eine Adressänderung beauftragt (Anforderung an IT.NRW am 25.02.2014)
MWEIMH	Beim Geologischen Dienst wurden die Adresse und das Passwort in dem Einzelfall geändert. Beim Landesbetrieb Mess- und Eichwesen war eine Adresse betroffen, der Rechner wurde auf Schadsoftware untersucht und neu installiert.
MBWSV	Im Ressort des MBWSV war der Landesbetrieb Straßenbau mit sieben Email-Adressen betroffen. Ein Zugriff auf die Emailpostfächer ist allerdings nur vom dienstlichen Arbeitsplatz aus möglich und nicht von außerhalb. Ein Risiko des Missbrauchs ist daher als gering anzusehen. Gegenmaßnahmen im Landesbetrieb Straßen NRW: - Veröffentlichungen von Informationen über den Vorfall an alle Benutzer im Intranet des Landesbetriebs am 03.02.2014, inklusive Sicherheitshinweise und Link aufs BSI weitergeleitet; - In Abstimmung mit dem Personalrat hat eine Vertrauensperson die Abfrage der konkreten E-Mail-Adressen für den Landesbetrieb ans CERT.NRW gestellt. Diese Person hat die betroffenen Mitarbeiter darüber informiert, dass ihre Mailaccounts von dem Sicherheitsvorfall betroffen sind und dass sie – wenn noch nicht erfolgt – diesbezüglich tätig werden. Die Vertrauensperson stand und steht für Beratung und Rückfragen zur Verfügung.

Anlage 2 zur Kleinen Anfrage 2062

Nach Bekanntgabe der E-Mail-Adresssen durchgeführte Maßnahmen der Ressorts

Ressort	Maßnahmen
MIK	Der Geschäftsbereich des MIK wurde am 12.02.2014 unter Nennung der jeweiligen betroffenen E-Mail Adressen mit dem Hinweis informiert, dass umgehend Passwörter der betroffenen E-Mail Adressen geändert werden sollten, soweit sie weiterhin zur Registrierung bei Online-Diensten verwendet werden. Die Polizei des Landes Nordrhein-Westfalen traf im Zuge der Erkenntnismitteilung des LKA NI im August 2013 (siehe Antwort auf Frage 1) folgende Maßnahmen: • Information des IT-Sicherheitsbeauftragten des LZPD und Über-mittlung der Datensätze an das LZPD durch das LKA NRW • Verifizierung/Zuordnung der Datensätze • erste Befragungen der betroffenen Bediensteten • Unterrichtung der betroffenen Polizeibehörden mit der Bitte um Maßnahmen zur IT-Sicherheit und Datensicherung sowie Prüfung der strafrechtlichen Relevanz • Strafanzeige durch das LKA NRW wegen des Verdachts des ge-zielten Ausspähens von Daten aus polizeilichen Informationssystemen
MAIS	Eingeleitete Maßnahmen: Löschen der betroffenen E-Mailadresse (März 2014) Information an betroffene Beschäftigte (März 2014) Sensibilisierung aller Beschäftigten (März 2014)
JM	Am 06.03.2014 wurde durch das Technische Betriebszentrum der Justiz (TBZ) geprüft, welche der betroffenen E-Mail-Adressen noch aktiv sind. Es handelt sich um dreizehn dienstliche E-Mail-Adressen. Zusätzlich wurde das TBZ beauftragt, die dreizehn betroffenen Mitarbeiterinnen und Mitarbeiter über den Sachverhalt zu informieren. Gleichzeitig wurde das TBZ gebeten, die Mitarbeiterinnen und Mitarbeiter aufzufordern, sich entsprechend der vom BSI empfohlenen Sicherheitsmaßnahmen zu verhalten.

Anlage 2 zur Kleinen Anfrage 2062

Nach Bekanntgabe der E-Mail-Adresssen durchgeführte Maßnahmen der Ressorts

Ressort	Maßnahmen
MKULNV	Nach der Bekanntgabe der betroffenen E-Mail-Adressen wurden die betroffenen Dienststellen am gleichen Tag über die konkreten Adressen informiert, um die notwendigen Maßnahmen einzuleiten. Schon zuvor hatten einige Dienststellen ihre Beschäftigten gebeten, den Prüfdienst des BSI zu verwenden. Die Windows-Accounts der Mailadresseneigentümer wurden in der Landwirtschaftskammer vorübergehend gesperrt bzw. deaktiviert; alle Personen mit kompromittierten Adressen wurden informiert und gebeten, die Login-Daten (Passwort) unverzüglich zu ändern und alle Logins, die nicht mehr benötigt werden, zu löschen. Am 11.2.14 konnte für den Geschäftsbereich des MKULNV und dem MKULNV selbst Vollzug ge-meldet werden.
MIWF	Im Ressort für Innovation, Wissenschaft und Forschung sind nur drei Emailadressen der Stiftung für Hochschulzulassung (SfH, ehemals ZVS) in der Adressliste enthalten. Sie sind einer alten Subdomain zugeordnet gewesen und dienstlich schon seit geraumer Zeit vor Bekanntwerden der BSI-Meldung nicht mehr aktiv genutzt worden. Als Maßnahmen sind nach dem Bekanntwerden im Februar 2014 die Löschung der Subdomain zvs.nrw.de sowie eine Sonderprüfung aller gefährdeten Rechnersysteme der Stiftung veranlasst und durchgeführt worden. Hinzuweisen ist ferner auf die turnusmäßig stattfindenden Informationsveranstaltun-gen, in denen die Beschäftigten für die Gefährdungen sensibilisiert werden.
MFKJKS	Fehlanzeige
MGEPA	Die Adressliste wurde auf Adressen des MGEPA-Geschäftsbereichs und seiner Rechtsvorgänger überprüft. Die dabei identifizierten zwei Adressen sind bereits seit mehreren Jahren gelöscht und damit auch nicht mehr nutzbar. Weitere Maßnahmen wurden daher nicht ergriffen.