LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/Drnr**

datum

Antrag

der Fraktion der PIRATEN

Kernschmelze der Datensicherheit im Bundestag ist übertragbar: NRW muss Konsequenzen ziehen!

I. Sachverhalt

Die IT-Infrastruktur des Deutschen Bundestags ist von einem schweren Angriff betroffen. Seit einigen Wochen kommen immer neue, alarmierende Details dieses Angriffs ans Licht. Am Donnerstag, den 11. Juni 2015 hat BSI-Präsident Michael Hange wie zuvor bereits am 21. Mai 2015 die Bundestags-Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und -medien (IuK-Kommission) über den Sachstand informiert. Das Sitzungsprotokoll der 6. Sitzung vom 21. Mai ist durch eine ungeplante Veröffentlichung Ursprung zahlreicher Presseberichte.

Laut des BSI haben die Täter den Verzeichnisdienst (Active Directory) mit vollem Administrationszugriff übernommen, was bedeutet, dass sie auf beliebige Systeme und Accounts samt Zugangsdaten Zugriff haben, und damit einen ungehinderten Zugang zu sämtlichen Daten und den 20.000 PCs des Netzwerks.

Die Experten haben offenbar kein Mittel dagegen gefunden, die Angreifer aus dem System auszusperren. Als kurzfristige Maßnahme wurde lediglich ein Großteil des Datenverkehrs über einen Proxy im Regierungsnetzwerk geleitet, was weder eine absolute Sicherheit noch die vom Bundestag angestrebte Unabhängigkeit verspricht. Überdies sei prinzipiell nicht ausgeschlossen, dass auch Regierungsstellen betroffen seien, berichtet Herr Hange am 21. Mai der IuK-Kommission. In dem genannten Protokoll heißt es weiter, der Schutz vor einem Informationsabfluss könne nicht gewährleistet werden. Bereits im Mai empfahl das BSI eine Neuinstallation des Gesamtnetzes.

Das IT-Netz des Bundestags sei nicht mehr zu retten, ergaben auch Recherchen von NDR, WDR und der Süddeutschen Zeitung. Das Netzwerk mit allen Software-Installationen müsse laut des BSI komplett neu aufgebaut werden. Mitglieder der IuK-Kommission bestätigen dies u.a. dem Tagesspiegel. Zumindest für einen etwaigen Parallelbetrieb würde vermutlich

Datum des Originals: datum/Ausgegeben: datum

zusätzliche Hardware gebraucht. Ob die Hardware – inkl. Firmware – selbst betroffen ist, ist bislang unklar.

Dies stellt ein erhebliches Warnsignal dar, und einen Angriff bislang ungeahnter Tiefe und Qualität auf die Legislative der Bundesrepublik Deutschland.

Die IT-Landschaft des Landtags NRW ist mit der des Bundestags technisch vergleichbar und grundsätzlich nicht besser abgesichert. Ein gleicher Angriffsvektor und ähnliche Angriffsdimensionen sind möglich und ohne zusätzliche Maßnahmen langfristig sehr wahrscheinlich. Es ist auch nicht auszuschließen, dass ähnliche Angriffe auf die IT-Infrastruktur des Landtags NRW bereits erfolgt sind.

Es ist kurzfristig erforderlich, die Landtags-IT nach entsprechenden ähnlichen Sicherheitslücken zu durchsuchen, über die der Angriff auf die Bundestags-IT durchgeführt wurde, und diese zu schließen, um das Risiko eines vergleichbaren Angriffs abzuwenden.

Es ist überdies wichtig, die IT-System-Architektur des Landtags NRW grundsätzlich neu zu überdenken und fortwährend intensiv weiterzuentwickeln, um zukünftige Angriffe deutlich zu erschweren. Es ist sinnvoll, hierbei nicht ausschließlich auf proprietäre Software mit unbekannten Hintertüren und ggf. verschwiegenen Schwachstellen zu setzen.

Quelloffene Software (Open Source) ist zwar nicht grundsätzlich vor Schwachstellen und Angriffen sicher, wird jedoch dynamischer entwickelt und kann absichtlich – z.B. zu Spionagezwecken – implementierte Backdoors nicht auf Dauer verstecken. Schwachstellen können schneller und transparent behoben werden. Investiert die öffentliche Hand darüber hinaus zusätzliche Energie in die Behebung von Schwachstellen in Open Source-Produkten, gewinnen auch Unternehmen und Behörden, die ebenfalls auf diese Software setzen. Auch im Bundestag fordern Abgeordnete, Betriebssystem und Software des Parlaments auf Open Source-Produkte umzustellen.

Zudem muss die Architektur von Netzen dezentraler sein, und unterschiedliche Bereiche müssen stärker voneinander abgeschottet sein, um die Verbreitung von Schadsoftware zu verhindern. Eine absolute Sicherheit der einzelnen mit einem Netz verbundenen Rechner wird sich niemals erzielen lassen, umso wichtiger ist es, dass Anwendungen, Netzbereiche und Systeme voneinander logisch getrennt sind.

Die Mitglieder des Landtages müssen aktiv über alle Schritte und Erkenntnisse informiert werden. Nur so erhält man das Vertrauen in die IT-Infrastruktur des Landtages, welche ein unverzichtbares Arbeitsmittel der Abgeordneten und ihrer Mitarbeiter darstellt. Im Bundestag ist die Verunsicherung, verursacht durch die katastrophale Informationspolitik des dortigen Präsidiums so groß, dass sich Abgeordnete öffentlich beklagen, ihr Vertrauen in die Systeme verloren zu haben und unzureichend informiert zu sein. Sie machen dafür das Bundestagspräsidium verantwortlich. Soweit darf es bei uns nicht kommen.

II. Der Landtag stellt fest:

- Die Integrität und Vertraulichkeit der Kommunikation zwischen der Öffentlichkeit und der Abgeordneten sowie ihrer Mitarbeiter ist von höchster Bedeutung.

- Der Angriff auf das IT-System des Deutschen Bundestags bietet Anlass zu größter Besorgnis.

- Die IT-System-Architektur des Landtags NRW ist ebenfalls gefährdet und verwundbar wie die des Bundestags.

- Vermehrter Einsatz von quelloffener Soft- und Hardware, konsequente Verschlüsselung und die stärkere Abschottung innerhalb des Netzes durch dezentrale Architekturen ist eine bessere Basis, die Sicherheit des Landtags-Netzwerkes zu gewährleisten und zu kontrollieren.

- NRW kann durch entsprechende Förderung quelloffener Software und Hardware sowohl die IT-Sicherheit erhöhen als auch ein Vorzeigeland der Open Source-Wirtschaft und eine Wachstumsregion dieser Branche werden.

III. Der Landtag fordert das Präsidium auf,

- Kontakt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundestagsverwaltung aufzunehmen und sich über die Sicherheitsprobleme der Bundestags-IT zu informieren;

- kurzfristig alles Notwendige zu veranlassen, um solche Angriffe zu verhindern bzw. abzuwehren, bzw. das IT-System des Landtages gegen diese Art von Angriffen zu sichern und anfällige Komponenten und Teilsysteme auszutauschen;

- die IT-Landschaft des Landtags NRW unter diesen Gesichtspunkten neu zu planen, aufzubauen und fortwährend weiterzuentwickeln, um ihre Verwundbarkeit zu senken;

- bei einem Neuaufbau der Landtags-System-Architektur weitgehend auf proprietäre Software zu verzichten und quelloffene Software (Open Source) zu nutzen. Dies betrifft vor allem die Netzwerk-Architektur und die Betriebssysteme;

- den Landtag schnellstmöglich über die eingeleiteten Maßnahmen und Erkenntnisse zu informieren und regelmäßig über den Fortschritt zu berichten.

IV. Der Landtag fordert die Landesregierung auf,

- zu Gunsten der Sicherheit öffentlicher und privater IT-Infrastruktur den Einsatz quelloffener Soft- und Hardware zu fördern und entsprechende Anreize zu schaffen;

- zur Verbesserung der IT-Sicherheit aktiv die Beseitigung von Schwachstellen entsprechender Open Source-Produkte zu unterstützen und zu fördern.

Dr. Joachim Paul

Marc Olejak

Daniel Schwerd

$whoeverelse

und Fraktion