Abgeordnetenhaus BERLIN

Drucksache 17 / 14 864
Schriftliche Anfrage

17. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Alexander Morlang (PIRATEN)

vom 30. Oktober 2014 (Eingang beim Abgeordnetenhaus am 04. November 2014) und **Antwort**

IT-Sicherheit der Berliner Verwaltung – „Drupageddon“

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Wie viele und welche Internetauftritte und Verfahren der Berliner Verwaltung basieren auf Drupal 7 und waren damit von dem sogenannten „Drupageddon“-Bug (DRUPAL-SA-CORE-2014-005) betroffen, der eine gravierende Sicherheitslücke in Drupal 7-Installationen darstellt?

2. Welche dieser Installationen wurden nicht vor dem 16. Oktober 2014 um 1:00 Uhr (nachts) auf die Drupal-Version 7.32 aktualisiert oder gepatcht und wurden deshalb – nach Angaben der Drupal-Entwickler*innen – mit hoher Wahrscheinlichkeit gehackt?

Zu 1. und 2.: Nach den dem Senat vorliegenden Informationen waren zwei von der Berliner Verwaltung verantwortete Internetauftritte von der Sicherheitslücke in der Software Drupal 7 betroffen.

Bei dem Stadtportal berlin.de wird grundsätzlich das Redaktionswerkzeug Imperia eingesetzt. Lediglich für das Datenportal unter daten.berlin.de wird Drupal 7 genutzt. Es wird für keinen weiteren Auftritt unterhalb von berlin.de Drupal in der Version 7 eingesetzt.

Drupal 7 wird für den Internetauftritt von eGovernment@School (www.egovschool-berlin.de) genutzt.

Beide Installationen wurden nicht vor dem 16. Oktober 2014 um 1:00 Uhr (nachts) auf die Drupal-Version 7.32 aktualisiert oder gepatcht.

3. Welche Schritte wurden wann unternommen, um die Sicherheitslücken zu schließen?

4. Welche Schritte wurden wann unternommen, um herauszufinden ob die Installationen gehackt wurden?

5. Welche Schritte wurden wann unternommen, um die Existenz von sogenannte Backdoors in kompromittieren Installationen auszuschließen?

Zu 3. bis 5.: Datenportal unter daten.berlin.de
Das offizielle Sicherheitsupdate wurde am 16.10.2014 eingespielt.

Nach Bekanntwerden des Ausmaßes der Sicherheitslücke wurde über Funktionen der Versionsverwaltung des Projektes sichergestellt, dass es zu keinen Veränderungen an Dateien innerhalb der Drupal-Installation gekommen ist. Dabei wurde keine Kompromittierung festgestellt.

Es ist eingeplant, die Installation auf den Stand von vor dem 14.10.2014 zurückzusetzen. Somit können auch eventuelle direkt in der Datenbank vorgenommene Änderungen rückgängig gemacht werden.

www.egovschool-berlin.de
Die betroffene Drupal-Installation wird bei einem externen Betreiber gehostet. Der Hostingvertrag sieht das kurzfristige Einspielen von Sicherheitspatches vor. Meldungen zu Sicherheitslücken zum Drupal-Produkt werden vom Sicherheitsmanagementteam der Senatsverwaltung für Bildung, Jugend und Wissenschaft analysiert. Es wird davon ausgegangen, dass verfügbare Sicherheitsupdates durch den Betreiber vertragsgemäß eingespielt werden. Am 29.10.2014 stufte das Drupalteam das Sicherheitsrisiko dieser Lücke höher. Beim Betreiber des Portals wurde daraufhin durch die Senatsverwaltung für Bildung, Jugend und Wissenschaft nachgefragt, ob die Installation von diesem Problem betroffen ist. Am 4.11.2014 teilte der Betreiber mit, dass die Installation von der Sicherheitslücke betroffen ist. Daraufhin wurden die in https://www.drupal.org/PSA-2014-003 genannten „Recovery-„Schritte beauftragt und am 6.11.2014 durch den Betreiber durchgeführt, um eine saubere Drupal-Installation sicherzustellen.

Das Inhaltsbackup wurde mit Stand vom 10.10.2014 eingespielt. Die Kennwörter der Drupal-Nutzerinnen und Drupal-Nutzer wurden geändert. Nach dem 10.10.2014 geänderte oder neu hinzugefügte Inhalte werden erneut hinzugefügt.

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

In der Regel wurde nach einem erfolgreichen Angriff der Patch für die Drupal-Version 7.32 durch die Angreifer auf das System eingespielt, um die Kontrolle über das System zu behalten. Bei der Drupal-Installation von www.egovschool-berlin.de ist dieser Patch nicht installiert worden. Dies wird als Indiz gewertet, dass die Seite nicht angegriffen worden ist.

Bei der durchgeführten Prüfung konnten keine veränderten Dateien festgestellt werden.

6. Bei welchen Installationen wurde eine Kompromittierung festgestellt und wurden dabei Daten „entwendet“?

Zu 6.: Bei www.egovschool-berlin.de und beim Datenportal unter daten.berlin.de wurde keine Kompromittierung festgestellt.

7. Lässt sich zweifelsfrei feststellen, dass keine Daten unter Ausnutzung dieser Sicherheitslücke „entwendet“ wurden?

Zu 7.: Nein. Es gibt jedoch keinerlei Anhaltspunkte, die auf eine Entwendung von Daten hindeuten.

Berlin, den 12. November 2014

In Vertretung

Andreas Statzkowski
Senatsverwaltung für Inneres und Sport

(Eingang beim Abgeordnetenhaus am 18. Nov. 2014)