Original-URL des Artikels: https://www.golem.de/news/bundeshack-hack-auf-bundesregierung-erfolgte-ueber-lernplattform-ilias-1803-133227.html **Veröffentlicht:** 08.03.2018 15:56 **Kurz-URL:** https://glm.io/133227

Bundeshack

Hack auf Bundesregierung erfolgte über Lernplattform Ilias

Die Bundesregierung wurde über die Lernplattform Ilias gehackt, die an der Hochschule des Bundes zu Weiterbildungszwecken genutzt wird. Die Einrichtung nutzte eine alte Version mit zahlreichen Sicherheitslücken.

Unter lernplattform-bakoev.bund.de können Mitarbeiter des Bundes Weiterbildungsangebote der Bundesakademie für Öffentliche Verwaltung wahrnehmen - eigentlich. Denn die von der Hochschule des Bundes betriebene Webseite ist derzeit nicht erreichbar. Wer sie besuchen will, bekommt nur die Fehlermeldung: *"Die Lernplattform Ilias ist zurzeit nicht erreichbar. Sie wurde auf Empfehlung des BSI vorsorglich vom Netz genommen."* Über diese Plattform soll der Hack auf die Bundesregierung abgelaufen sein.

Dem BSI (Bundesamt für Sicherheit in der Informationstechnik) sind nach eigener Auskunft keine Sicherheitslücken in der Ilias-Software bekannt, das Bundesministerium des Innern wollte auf Nachfrage keine weiteren Angaben zu dem Angriff machen.

Die Fehlermeldung bestätigt frühere Medienberichte, denen zufolge ein E-Learning-Angebot der Bundesregierung Einfallstor für die Malware war. Über ein mit Schadsoftware präpariertes Kursangebot hätten die Angreifer es geschafft, in 17 Rechner im Auswärtigen Amt einzudringen und von dort mehrere vertrauliche Dokumente zu kopieren, wie die Frankfurter Allgemeine Sonntagszeitung berichtet. Der Angriff wurde intern angeblich im Dezember 2017 entdeckt, soll aber zu diesem Zeitpunkt schon mehrere Monate aktiv gewesen sein. Es heißt, die Bundesregierung sei von einem befreundeten Geheimdienst auf die infizierten Rechner hingewiesen worden.

Der Angriff zielte demnach eher auf einzelne Rechner in Ministerien ab als auf das Netzwerk der Bundesregierung selbst, den Informationsverbund Bonn Berlin. Medienberichten zufolge gehen Sicherheitbehörden von einem russischen Ursprung der Angriffe aus.

Ilias bestätigt Hack der eigenen Software

Ilias ist ein Open-Source-Projekt, es wird an zahlreichen Universitäten und auch an anderen öffentlichen Einrichtungen genutzt. Der Verein hat seinen Sitz in Köln. Auf der Admin-Mailingliste des Vereins schreibt Ilias-Produktmanager Matthias Kunkel am 8. März, dass bei dem Hack auf das Netzwerk der Bundesregierung *"leider auch eine Ilias-Installation involviert gewesen sein"* soll. Genauere Informationen über möglicherweise verwendete Sicherheitslücken habe man allerdings derzeit nicht. Der Verein will die Sicherheitsproblematik bei der Ilias-Entwicklertagung in der kommenden Woche in Halle/Saale besprechen.

Auf Anfrage von Golem.de äußerte sich Matthias Kunkel von Ilias zu der Software. Er sagte: *"Der Verein Ilias Open Source E-Learning e.V. gibt Ilias als Open Source Software heraus und koordiniert deren Softwareentwicklung. Betrieben werden die jeweiligen Ilias-Installationen aber von den Institutionen oder Unternehmen, die Ilias für ihre E-Learning-Zwecke einsetzen."* Die vom Netz genommene Installation der Bundesakademie werde *"von der Hochschule Bund betrieben"*.

Tatsächlich gibt es einige Sicherheitslücken, die Angreifer ausgenutzt haben könnten ...

Hochschule nutzte veraltete Version mit bekannten Sicherheitslücken

Wie genau die Ilias-Installation angegriffen wurde, konnten wir nicht herausfinden, auch weil bislang keiner der Beteiligten für eine Stellungnahme erreichbar war. Doch eine Analyse der Software brachte einige Details zu Tage, die möglicherweise Hinweise geben.

Im Google-Cache war zum Zeitpunkt unserer Recherche noch die zuletzt aktive Version von Ilias unter der betroffenen Webseite abrufbar. Daraus geht hervor, dass diese mit Version 5.1.16 von Ilias betrieben wurde. Diese wurde bereits vor einem Jahr, im März 2017, veröffentlicht. Seither gab es mehrere Sicherheitsupdates, die offenbar nicht installiert wurden.

Der Upload von SVG-Dateien ermöglichte eine Cross-Site-Scripting-(XSS)-Lücke, eine weitere XSS-Lücke gab es aufgrund fehlender Filterung von Formulareingaben. Eine Lücke in der Mailzustellung führte dazu, dass Systemmails manchmal an die falschen Nutzer zugestellt wurden. Im Oktober 2017 wurde eine nicht näher erläuterte Sicherheitslücke bei der Behandlung von Mediendateien gefunden. Und Anfang Februar 2018 fand sich eine weitere Cross-Site-Scripting-Lücke.

Um Schwachstellen dieser Art auszunutzen, ist es in der Regel erforderlich, das Opfer auf eine bestimmte Seite mit Angriffscode zu locken. Das ist meist deutlich umständlicher als andere Klassen von Sicherheitslücken, bei denen man oft direkt Code ausführen oder Daten abgreifen und manipulieren kann. Für professionelle Angreifer wäre das aber ein realistischer Aufwand.

Eine kritischere Lücke wurde in der von der Hochschule verwendeten Version 5.1.6 behoben: Sie ermöglicht laut der Beschreibung das Kopieren von Dateien an beliebige Stellen im Dateisystem. Damit ist es vermutlich relativ einfach möglich, eine Installation komplett zu übernehmen und Code auszuführen. Diese Lücke ist zwar in der vor wenigen Tagen noch genutzten Version von Ilias behoben, doch bisherigen Berichten zufolge soll der Angriff mehrere Monate vor dem vergangenen Dezember begonnen haben.

Adminsitratoraccount mit Standardpasswort "homer"

Bei der Analyse von Ilias ist uns ein weiterer Schwachpunkt aufgefallen. Wenn man das System neu installiert, wird ein Standardaccount mit Administratorrechten angelegt. Dieser hat den Benutzernamen "root" und das Passwort *"homer"*. Nirgendwo wird man dazu aufgefordert, das Passwort umgehend zu ändern. Denkbar wäre es also, dass das Standardpasswort schlicht nicht geändert wurde.

Wir haben keine Möglichkeit gefunden, mit einem Administratoraccount direkt Code auszuführen. aber es ist natürlich nicht auszuschließen, dass es eine solche Möglichkeit gibt und wir sie nicht gefunden haben. Natürlich ist auch denkbar, dass der Angriff über eine bislang unbekannte Lücke erfolgte. Insgesamt ist das Ilias-System sehr umfangreich, es bietet für Nutzer viele Möglichkeiten, zu interagieren. Datei-Uploads von zahlreichen Medienformaten, ein Wiki, ein Pluginsystem und vieles mehr bieten eine große Angriffsfläche.

Von der Nato geprüft

Bei unseren Recherchen sind wir außerdem auf eine Meldung aus dem Jahr 2008 gestoßen. Demnach hat die Nato die Ilias-Software einem dreitägigen Test unterzogen und dabei keine Sicherheitsprobleme gefunden. Ilias kann demnach auch im internen Nato-Netz Chronos eingesetzt werden. Auch soll Ilias bereits vor diesem Test von der Nato zur Vorbereitung von Soldaten auf Isaf-Einsätze in Afghanistan verwendet worden sein.

Hinweis: Eine englischsprachige Version des Textes können Sie hier nachlesen (hg)

Verwandte Artikel:
Fluggastdaten: Regierung dementiert Hackerangriff auf deutsches PNR-System
(10.03.2018, https://glm.io/133261)
Government Hack: Hack on German Government via E-Learning Software Ilias
(08.03.2018, https://glm.io/133231)
Auswärtiges Amt: Bundeshacker kommunizierten per Outlook mit Malware
(06.03.2018, https://glm.io/133177)
Bundeshack: Ausländischer Geheimdienst soll Regierung gewarnt haben

(02.03.2018, https://glm.io/133112)
Spionage: Angriff auf Bundesregierung dauert noch an
(01.03.2018, https://glm.io/133075)
