

Aktuelle Meldung

## Software-Schwachstellen 2016: Zahlen leicht rückläufig

10. Januar 2017

Potsdam. Im Jahr 2016 sind weltweit insgesamt weniger Software-Sicherheitslücken gemeldet worden als im Vorjahr. Nach Analyse des Potsdamer Hasso-Plattner-Instituts (HPI) wurden in den vergangenen zwölf Monaten rund 5.577 Meldungen zu Software-Schwachstellen registriert. Das sind immer noch mehr als in den Jahren von 2009 bis 2013, allerdings waren es 2015 noch 6.354 gewesen.

Die Auswertung der Wissenschaftler zeigt, dass sich die Verteilung der Schwachstellen nach Schweregrad kaum geändert hat: Wie im Vorjahr handelt es sich vorwiegend um Sicherheitslücken mit mittlerem Schweregrad (2016: 52%; 2015: 53%). Über ein Drittel sind Software-Schwachstellen mit hohem Schweregrad (2016: 39%; 2015: 37%). Der Schweregrad basiert auf dem CVSS-Score, die ausführliche Statistik finden Sie unter: <https://hpi-vdb.de/vulndb/statistics/>. Der Großteil der Schwachstellen könnte der HPI-Analyse zufolge „remote“, also aus der Ferne, ausgenutzt werden (2016: 84%; 2015: 86%).

„Es ist erfreulich, dass immer mehr IT-Unternehmen die Bedeutung von Schwachstellen erkannt haben. Viele von ihnen belohnen im Rahmen sogenannter Bug-Bounty-Programme die Aufdeckung und Meldung von Sicherheitslücken“, so HPI-Direktor Professor Christoph Meinel. Die Unternehmen fürchteten zu Recht Imageverluste durch den Verkauf oder das Ausnutzen von Schwachstellen. Weiterhin gelte jedoch: „Computernutzer sollten darauf achten, alle Software-Produkte regelmäßig auf verfügbare Updates zu überprüfen und so immer auf dem aktuellen Stand zu halten“.

Auf der Website <https://hpi-vdb.de> können Nutzer per Selbstdiagnose ihren Browser und Browser-Plugins kostenlos auf erkennbare Schwachstellen überprüfen lassen. Außerdem lassen sich über den Dienst individuelle Listen mit selbst genutzten Programmen erstellen, die dann permanent auf Sicherheitslücken überprüft werden.

### **Die Datengrundlage**

In der HPI-Datenbank sind die wesentlichen im Internet veröffentlichten und frei verfügbaren Angaben über Software-Sicherheitslücken und -Probleme integriert und kombiniert. Die aktuellen Jahres-Statistiken zu Schwachstellen können sich geringfügig ändern, da Informationen über in Vorjahren registrierte Schwachstellen noch nachgereicht bzw. aktualisiert werden. Die

Einstufung der Schwachstellen nach Kritikalität basiert auf dem freien, offenen und stark genutzten Industriestandard CVSS (Common Vulnerability Scoring System).

Die HPI-Datenbank analysiert neben allgemeinen Informationen über eine Schwachstelle wie Schweregrad und Änderungsdatum zusätzlich die Vor- und Nachbedingungen einer Sicherheitslücke. Vorbedingungen beziehen sich auf alle Notwendigkeiten, die erfüllt sein müssen, damit eine Schwachstelle ausgenutzt werden kann (z.B. die Zugriffsart). Nachbedingungen sind die Auswirkungen der Ausnutzung einer Schwachstelle (z.B. die Art des Zugriffs auf das betroffene System). Diese Informationen stellt das HPI in maschinenlesbarem Format bereit, das eine automatische Analyse ermöglicht.

### **Kurzprofil Hasso-Plattner-Institut**

Das Hasso-Plattner-Institut für Softwaresystemtechnik GmbH (<https://hpi.de>) in Potsdam ist Deutschlands universitäres Exzellenz-Zentrum für IT-Systems Engineering. Als einziges Universitäts-Institut in Deutschland bietet das HPI den Bachelor- und Master-Studiengang „IT-Systems Engineering“ an – ein besonders praxisnahes und ingenieurwissenschaftliches Informatik-Studium, das von derzeit von rund 500 Studierenden genutzt wird. Die HPI School of Design Thinking, Europas erste Innovationsschule für Studenten nach dem Vorbild der Stanford d.school, bietet jährlich 240 Plätze für ein Zusatzstudium an. Insgesamt zwölf HPI-Professoren und über 50 weitere Gastprofessoren, Lehrbeauftragte und Dozenten sind am Institut tätig. Es betreibt exzellente universitäre Forschung – in seinen elf IT-Fachgebieten, aber auch in der HPI Research School für Doktoranden mit ihren Forschungsaußenstellen in Kapstadt, Haifa und Nanjing. Schwerpunkt der HPI-Lehre und -Forschung sind die Grundlagen und Anwendungen großer, hoch komplexer und vernetzter IT-Systeme. Hinzu kommt das Entwickeln und Erforschen nutzerorientierter Innovationen für alle Lebensbereiche. Das HPI kommt bei den CHE-Hochschulrankings stets auf Spitzenplätze.

---

Pressekontakt: [presse@hpi.de](mailto:presse@hpi.de)

Christiane Rosenbach, Tel. 0331 5509-119, [christiane.rosenbach@hpi.de](mailto:christiane.rosenbach@hpi.de) und

Felicia Flemming, Tel. 0331 5509-274, [felicia.flemming@hpi.de](mailto:felicia.flemming@hpi.de)