

Aktuelle Meldung

Geraubte Identitäten im Internet: HPI-Service hilft Nutzerdaten zu überprüfen

19. Mai 2014

Potsdamer Sicherheitskonferenz

Potsdam. Forscher des Hasso-Plattner-Instituts (HPI) haben eine Lösung entwickelt, die das Internet nach von Cyberkriminellen erbeuteten und im Internet frei zugänglichen Identitätsdaten durchsucht. Diese auch als digitale Identitäten bezeichneten Informationen – derzeit sind es gut 160 Millionen Datensätze – analysieren die Potsdamer Internetwissenschaftler und bieten Internetnutzern den kostenlosen Dienst „HPI Identity Leak Checker“ an. Das teilte das Institut auf der Potsdamer Konferenz für nationale Cyber-Sicherheit mit. Auf der Webseite <https://sec.hpi.uni-potsdam.de> können Internetnutzer bei Eingabe ihrer E-Mail-Adresse prüfen, ob sie Opfer eines Identitätsdiebstahls sind und ihre Identitätsdaten frei im Internet kursieren.

„Der von uns entwickelte Dienst sendet dem Nutzer einen Hinweis, welche Arten seiner Identitätsdaten, also zum Beispiel Passwörter, Vor- und Zuname, Anschriften oder Geburtstage, gegebenenfalls offenliegen und somit missbraucht werden könnten“, erläuterte HPI-Direktor Prof. Christoph Meinel. Selbstverständlich würden in der Antwortmail die Daten selbst nicht herausgegeben, betonte der Wissenschaftler, der auch das HPI-Fachgebiet Internet-Technologie und -Systeme leitet. Nach Meinels Worten soll der Dienst eine Art Warnsystem für gestohlene und im Internet kursierende Identitätsdaten sein und „die Internetnutzer darauf aufmerksam machen, dass im Umgang mit persönlichen Daten dringend mehr Achtsamkeit geboten ist“.

Kostenloser Sicherheits-Check für Rechner

Zusätzlich ergänzt das HPI seine 2012 vorgestellte Datenbank für IT-Angriffsanalysen (<https://hpi-vdb.de>) ab sofort um einen weiteren Dienst. „So kann jetzt jeder Internetnutzer seinen Rechner bei uns kostenlos auf erkennbare Schwachstellen überprüfen lassen“, kündigte Meinel auf der Potsdamer Sicherheitskonferenz an. Die Schwachstellen zu kennen ist zum Schutz der IT-Systeme zuhause oder im Unternehmen extrem wichtig, weil Cyberangriffe erst durch den geschickten Missbrauch dieser Schwachstellen zum Erfolg kommen. Auf der Selbstdiagnose-Seite der HPI-Datenbank erkennt das System die verwendete Version des Browsers – einschließlich der gängigen Zusatzprogramme (Plugins) und weiter auf dem Rechner installierter Software -, und sucht nach bekannten Schwachstellen. Der

Nutzer bekommt dann eine nach Gefährlichkeitsgrad der bekannten Sicherheitslücken sortierte Liste angezeigt.

Registrierte Nutzer können darüber hinaus eine Liste verwendeter Softwareprogramme zusammenstellen, welche die HPI-Datenbank für IT-Angriffsanalysen permanent auf Schwachstellen überprüft. Sobald neue Sicherheitslücken dieser Programme auftauchen, bekommt der Nutzer auf Wunsch eine automatische E-Mail-Benachrichtigung.

Seit Einrichtung im Vorjahr integriert und kombiniert die HPI-Datenbank für IT-Angriffsanalysen viele im Internet verfügbare Angaben über Software-Sicherheitslücken und -probleme. Derzeit sind dort gut 61.000 Informationen zu Schwachstellen gespeichert, die in fast 158.000 betroffenen Softwareprogrammen von mehr als 13.000 Herstellern vorhanden sind. Dreimal am Tag aktualisiert sich die HPI-Datenbank automatisch. „Dadurch wird unsere Datenbasis täglich um 200 bis 300 Verwundbarkeits-Informationen angereichert. Ziel ist eine zentrale und möglichst vollständige Zusammenstellung aller verfügbaren Informationen über Schwachstellen“, erklärte Internetwissenschaftler Meinel.

Die Datenbank solle ein komfortables Mittel sein, mit dem vor allem IT-Sicherheitsverantwortliche, Administratoren und Programmierer einen schnellen Überblick über alle aktuellen Schwachstellen-Informationen erlangen sollen. Außerdem lassen sich dank der maschinenlesbaren Formate, in denen die Schwachstellen-Informationen gespeichert sind, Sicherheitsanalysen von IT-Systemen erstellen. Trotz des großen Umfangs der zu bewertenden Daten sind solche Systemanalysen sogar sehr schnell möglich, da mit der am HPI erforschten und mitentwickelten Hauptspeicher-Datenbanktechnologie gearbeitet wird. Beim Forschungspartner und Softwarekonzern SAP bekam sie den Produktnamen HANA.

Big Data – auch in der HPI-Sicherheitsforschung

Bei den neuen Diensten und in ihrer gesamten Sicherheitsforschung können sich die HPI-Wissenschaftler für die schnelle Analyse der besonders großen Menge sicherheitsbezogener Daten auf die Infrastruktur des HPI-eigenen Spitzenforschungslabors stützen. Dort stehen für die Projekte modernste Hochleistungssysteme mit sehr vielen Rechenkernen, hoher Arbeitsspeicherkapazität und großem Festplattenspeicher-Volumen zur Verfügung.

Zum Einsatz kommt diese Infrastruktur zum Beispiel auch für das Real-time Event Analytics and Monitoring System (REAMS). Darin sammeln die HPI-Internetwissenschaftler sämtliche Informationen, die über Ereignisse in einem Netzwerk auftreten – egal, ob sie von Servern, Routern oder Arbeitscomputern kommen – und werten diese Daten in Realzeit aus. Das schafft die Voraussetzung dafür, dass auch komplexe Cyberangriffe genau in dem Moment erkannt werden können, in dem sie ausgeführt werden. Aber

auch längst zurückliegende Angriffe lassen sich dadurch nachträglich rekonstruieren und analysieren.

Da die gesammelten Daten über solche Ereignisse in Netzwerken meistens in unterschiedlichen Formaten vorliegen, überführt das von den HPI-Forschern entwickelte System sie zunächst in ein einheitliches Format und speichert sie für den schnellen Zugriff in einer Hauptspeicher-Datenbank (In-Memory), statt auf Festplatten. Dank der Hauptspeicher-Datenbanktechnologie können dann die vereinheitlichten Daten über sicherheitskritische Ereignisse und Vorgänge blitzschnell, flexibel und ausführlich analysiert werden. So lassen sich zum Beispiel sofort typische Angriffsmuster erkennen und die Zusammenhänge einzelner Vorgänge aufdecken, die zusammen auf einen komplexen mehrstufigen Cyberangriff hinweisen. Somit versetzen die am HPI entwickelten Techniken IT-Sicherheitsexperten in die Lage, auch neuartige Angriffe zu erkennen, die in herkömmlichen Lösungen unentdeckt bleiben.

Kurzprofil Hasso-Plattner-Institut

Das Hasso-Plattner-Institut für Softwaresystemtechnik GmbH (HPI) in Potsdam ist Deutschlands universitäres Exzellenz-Zentrum für IT-Systems Engineering. Als einziges Universitäts-Institut in Deutschland bietet es den Bachelor- und Master-Studiengang „IT-Systems Engineering“ an – ein besonders praxisnahes und ingenieurwissenschaftliches Informatik-Studium, das von derzeit 470 Studenten genutzt wird. Die HPI School of Design Thinking, Europas erste Innovationsschule für Studenten nach dem Vorbild der Stanforder d.school, bietet 240 Plätze für ein Zusatzstudium an. Insgesamt zehn HPI-Professoren und über 50 weitere Gastprofessoren, Lehrbeauftragte und Dozenten sind am Institut tätig. Es betreibt exzellente universitäre Forschung – in seinen neun 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. Mit openHPI.de bietet das Institut seit September 2012 ein interaktives Internet-Bildungsnetzwerk an, das jedem offen steht.