30.01.2020 – 11:31 Uhr

"Change Your Password Day" am 1. Februar: HPI gibt Tipps für starke Passwörter

Potsdam (ots) -

Anlässlich des "Change Your Password Days" am Samstag, dem 1. Februar, erinnert das Hasso-Plattner-Institut (HPI) an die wichtigsten Regeln zur Erstellung starker Passwörter. "Schwache Zahlenreihen wie etwa "123456" werden weltweit weiterhin viel zu häufig genutzt", kritisiert HPI-Direktor, Professor Christoph Meinel. "Viele Internetnutzer verwalten bereits mehr als hundert Online-Konten - da fällt die Wahl viel zu oft auf Passwörter, die man sich leicht merken kann", sagt Meinel. Auch die weit verbreitete Mehrfachnutzung von Passwörtern für unterschiedliche Dienste sei extrem leichtsinnig, wenn man bedenke, welche Schäden hierdurch entstehen könnten.

Die wichtigsten Regeln zur Erstellung starker Passwörter:

- Die Länge des Passworts sollte mindestens 15 Zeichen umfassen.
- Das Passwort sollte möglichst viele verschiedene Zeichentypen (Buchstaben, Ziffern, Sonderzeichen) sowie Groß- und Kleinschreibung mit einbeziehen.
- Keine Begriffe aus dem Wörterbuch oder andere "sinnvolle" Zeichenfolgen verwenden. Neben den Brute-Force-Attacken sind vor allem "Wörterbuchangriffe" üblich, um Passworte zu knacken: Hierbei werden Listen mit Wörtern genutzt, um fremde Passwörter zu entschlüsseln.
- Nie dasselbe Passwort für mehrere Konten verwenden. Wird ein Passwort geknackt, ermöglicht es Kriminellen sonst den Zugang zu allen anderen Diensten.
- Niemals persönliche Informationen wie Namen, Geburtsdaten, Haustiernamen, Namen der Partner oder der jeweiligen Anwendung (z.B. "Adobe") verwenden. Diese Daten könnten leicht erraten werden.
- Wenn möglich, die 2-Faktor-Authentifizierung nutzen.
- Passwortmanager helfen bei der Generierung und der sicheren Aufbewahrung starker Passwörter

Ob man selbst Opfer eines Datendiebstahls geworden ist, lässt sich mit dem Identity Leak Checker, einem Online-Sicherheitscheck des Hasso-Plattner-Instituts (HPI), sehr leicht überprüfen. Seit 2014 kann dort jeder Internetnutzer unter https://sec.hpi.de/ilc kostenlos durch Eingabe seiner E-Mail-Adresse prüfen lassen, ob Identitätsdaten von ihm frei im Internet kursieren und missbraucht werden könnten. Die Sicherheitsforscher ermöglichen den Abgleich mit mittlerweile mehr als 10 Milliarden gestohlener und im Internet verfügbarer Identitätsdaten. Dabei liegt der Fokus auf Leaks, bei denen deutsche Nutzer betroffen sind.

Kurzprofil Hasso-Plattner-Institut

Das Hasso-Plattner-Institut (HPI) in Potsdam ist Deutschlands universitäres Exzellenz-Zentrum für Digital Engineering (https://hpi.de). Mit dem Bachelorstudiengang "IT-Systems Engineering" bietet die gemeinsame Digital-Engineering-Fakultät des HPI und der Universität Potsdam ein deutschlandweit einmaliges und besonders praxisnahes ingenieurwissenschaftliches Informatikstudium an, das von derzeit rund 600 Studierenden genutzt wird. In den vier Masterstudiengängen "IT-Systems Engineering", "Digital Health", "Data Engineering" und "Cybersecurity" können darauf aufbauend eigene Forschungsschwerpunkte gesetzt werden. Bei den CHE-Hochschulrankings belegt das HPI stets Spitzenplätze. Die HPI School of Design Thinking, Europas erste Innovationsschule für Studenten nach dem Vorbild der Stanforder d.school, bietet jährlich 240 Plätze für ein Zusatzstudium an. Derzeit sind am HPI 19 Professoren und über 50 weitere Gastprofessoren, Lehrbeauftragte und Dozenten tätig. Es betreibt exzellente universitäre Forschung - in seinen 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.

Kontakt:

presse@hpi.de
Christiane Rosenbach, Tel. 0331 5509-119, christiane.rosenbach@hpi.de
und Friederike Treuer, Tel. 0331 5509-177, friederike.treuer@hpi.de

Diese Meldung kann unter https://www.presseportal.ch/de/pm/100007820/100840886 abgerufen werden.