PRESSEMITTEILUNG

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Aktuelle Meldung

# Die beliebtesten deutschen Passwörter 2020 - Platz 6 diesmal: ichliebedich

16. Dezember 2020

Vom plötzlichen Wechsel Hunderttausender Mitarbeiter ins Homeoffice haben Cyberkriminelle im Corona-Jahr 2020 stark profitiert. Seit Ausbruch der Pandemie sind neue Angriffsmöglichkeiten entstanden, die vielen Unternehmen zu recht Sorge bereiten. Ein großer Risikofaktor bleibt der viel zu laxe Umgang mit Passwörtern. Noch immer verlassen sich viele Internetnutzer auf simple Zahlenreihen wie „123456", die keinen adäquaten Schutz bieten.

„Die Corona-Pandemie hat die Angriffsfläche für Cyberangriffe in den letzten Monaten stark vergrößert und die IT-Abteilungen vieler Unternehmen vor große Herausforderungen gestellt. Ein Risikofaktor, der angesichts des Homeoffice-Trends nochmals an Bedeutung gewinnt, ist die weit verbreitete Verwendung schwacher Passwörter. Mit einem Passwort wie „ichliebedich" oder „123456" werden die eigenen Daten oder die eines Unternehmens nicht wirksam geschützt," so Professor Christoph Meinel, Direktor des Hasso-Plattner-Instituts.

Das Hasso-Plattner-Institut (HPI) veröffentlicht jedes Jahr die meistgenutzten Passwörter der Deutschen – Datengrundlage sind dieses Jahr 3,1 Millionen Zugangsdaten aus dem Datenbestand des HPI Identity Leak Checkers, die auf E-Mail-Adressen mit .de-Domäne registriert sind und 2020 geleakt wurden. Insgesamt wurden dieses Jahr 172 Datenlecks in den Identity Leak Checker eingepflegt, das sind rund 2 Milliarden Identitäten - 97 davon wurden von den Diensteanbietern selbst bestätigt.

Das Hasso-Plattner-Institut (HPI) weist seit vielen Jahren auf die Notwendigkeit sicherer Passwörter hin. Der Blick auf die Top Twenty der in Deutschland meistgenutzten Passwörter 2020 zeigt jedoch, dass schwache und unsichere Zahlenreihen weiterhin Spitzenplätze belegen.

**Top Twenty deutscher Passwörter:**

| | |
|---|---|
| **1. 123456** | **11. qwertz** |
| **2. 123456789** | **12. michael** |
| **3. passwort** | **13. killer** |
| **4. hallo123** | **14. michelle** |
| **5. 12345678** | **15. hallo** |
| **6. ichliebedich** | **16. sonnenschein** |
| **7. 1234567** | **17. alexander** |
| **8. 1234567890** | **18. Passwort** |
| **9. lol123** | **19. abc123** |
| **10. 12345** | **20. daniel** |

## Tipps zur Passwortwahl

Bei der Passwortwahl empfiehlt das Hasso-Plattner-Institut daher:

- Lange Passwörter (> 15 Zeichen)
- Alle Zeichenklassen verwenden (Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen)
- Keine Wörter aus dem Wörterbuch
- Keine Wiederverwendung von gleichen oder ähnlichen Passwörtern bei unterschiedlichen Diensten
- Verwendung von Passwortmanagern
- Passwortwechsel bei Sicherheitsvorfällen und bei Passwörtern, die die obigen Regeln nicht erfüllen
- Zwei-Faktor-Authentifizierung aktivieren, wenn möglich

## Der Identity Leak Checker

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 12 Milliarden gestohlener und im Internet verfügbarer Identitätsdaten. Dabei liegt der Fokus auf Leaks bei denen deutsche Nutzer betroffen sind. Das Angebot ist in Deutschland einzigartig.

Insgesamt haben mehr als 15,3 Millionen Nutzer mithilfe des Identity Leak Checkers die Sicherheit ihrer Daten in den letzten fünf Jahren überprüfen lassen. In mehr als 3,6 Millionen Fällen mussten Nutzer darüber informiert werden, dass ihre E-Mail-Adresse in Verbindung mit anderen persönlichen Daten im Internet offen zugänglich war.

**Spezialangebot für Unternehmen und Organisationen: Identity Leak Checker Desktop Client**

Der Identity Leak Checker Desktop Client ist ein kostenpflichtiges Angebot für Unternehmen und Organisationen, das sie bei der kontinuierlichen Überwachung der eigenen Domäne(n) unterstützt. Werden neue Datenlecks in den ILC importiert, prüft der Desktop Client automatisch, ob E-Mail-Adressen der überwachten Domäne(n) betroffen sind. Die betroffene(n) E-Mail-Adresse(n) können dann sofort gewarnt werden. Weitere Informationen zum Angebot unter: https://sec.hpi.de/ilc/

**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 650 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 21 Professorinnen und Professoren sowie über 50 weitere Gastprofessoren, Lehrbeauftragte und Dozenten tätig. Es betreibt exzellente universitäre Forschung in seinen IT-Fachgebieten, dem HPI Digital Health Center und seinen HPI Research Schools für Doktoranden mit Forschungsaußenstellen in Kapstadt, Haifa, Irvine 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.

Pressekontakt: presse@hpi.de
Christiane Rosenbach, Tel. 0331 5509-119, christiane.rosenbach@hpi.de und
Carina Kretzschmar-Weidmann, Tel. 0331 5509-177, carina.kretzschmar@hpi.de