Datenschutzbeauftragter (https://www.datenschutzbeauftragter-info.de/) INFO
INFORMATIONEN ZUM DATENSCHUTZ

Passwort – Sicherer mit Hash und Salt

Nach einem Bericht von heise online (http://www.heise.de/newsticker/meldung/Kundendaten-des-deutschen-Avast-Distributors-im-Netz-1820007.html) ist der deutsche avast!-Distributor Avadas Opfer eines Hackerangriffes geworden. Im Netz finden sich nun Auszüge aus Datenbanken mit Geburtsdaten, Anschriften, Bankverbindungen Mailadressen und Passworthashes (http://de.wikipedia.org/wiki/Kryptologische_Hashfunktion) von über 16.000 Personen. Welches Hashverfahren zur Anwendung kam, ist aber unbekannt. Es heißt aber zumindest, dass die Passworthashes gesalzen gewesen seien. Was aber bedeutet das?

Kryptologische Hashverfahren

Immer wieder bestätigen Vorfälle wie im Fall von Avadas, dass auf den Schutz von Passwörtern ein besonderes Augenmerk zu richten ist. Dies fängt bereits bei der Wahl eines sicheren Passwortes an, verlangt darüber hinaus aber auch eine sichere Speicherung des Passwortes für das Authentifizierungsverfahren bei Nutzung einer Anwendung oder Webseite. Das Speichern des Passwortes in unverschlüsselter Form stellt ein beachtliches Sicherheitsrisiko dar.

Um diesem Sicherheitsrisiko entgegenzuwirken, werden Passwörter in der Regel mit einem festen Algorithmus verschlüsselt gespeichert. Man spricht hierbei von einem gehashten Passwort.

Risiko einer Wörterbuchattacke

Jedoch unterliegen auch solche gehashten Passwörter ohne weiteres Sicherheitsmerkmal immer wieder sog. Wörterbuchangriffen (http://de.wikipedia.org/wiki/Wörterbuchangriff). Hierbei werden Listen von Wörtern mit demselben Algorithmus wie das Passwort verschlüsselt und anschließend deren Hashwerte mit dem gespeicherten Wert verglichen. Stimmen die Hashwerte überein, ist hieraus ein Rückschluss auf das verwendete Passwort möglich.

Dem Hacker ordentlich die Suppe versalzen

Um beispielsweise vor Wörterbuchangriffen zum Ausspionieren von Passwörtern, aber auch vor einem Sicherheitsrisiko durch einen böswilligen Systemadministratoren zu schützen, wurde das sog. „Salt“ eingeführt. Das Salt ist ein zufällig generierter Wert, der an das Benutzerpasswort vor der Verschlüsselung angehängt wird.

Allerdings vermeidet auch die Hinzugabe des Zufallswertes zum (Klartext)Passwort das Knacken von Passwörtern nicht, aber erschwert dieses erheblich durch großen Zeitaufwand. Denn der nun vorliegende gehashte Wert aus Passwort und Salt kann nicht einfach in einer Liste von Hashwerten nachgeschlagen, sondern muss aus einer Vielzahl von Kombinationen aus Passwörtern und Saltwerten geprüft werden.

Passwortkreativität ist gefragt

Der Benutzer von Diensten, bei denen eine Authentifizierung mittels Benutzernamen und Passwort erforderlich ist, sollte sich jedoch nie darauf verlassen, dass der Dienstanbieter ein sichereres Verschlüsselungsverfahren für die Passwortspeicherung verwendet. Ist es wie im Fall von Avada zu einem Hackerangriff gekommen und das Schicksal der Benutzerdaten einschließlich Passwort unbekannt, sollte in jedem Fall unverzüglich ein neues Passwort vergeben werden.

Hierbei sollte es sich bestenfalls nicht um dasselbe Passwort handeln, das bereits für andere Dienste verwendet wird. Denn wie hinlänglich bekannt, versuchen Cyber-Kriminelle gerne auch sich mittels der erlangten Daten Zugang zu anderen Diensten zu verschaffen. Welche Kriterien bei der Passwortwahl beachtet werden sollten, haben wir hier (https://www.datenschutzbeauftragter-info.de/wie-man-die-passwort-demenz-bekaempft/) bereits zusammengestellt.

ÜBER DEN AUTOR

REBECCA KIRSCH (HTTPS://WWW.DATENSCHUTZBEAUFTRAGTER-INFO.DE/AUTHOR/RKIRSCH/)
Rechtsanwältin

Als IT-Forensikerin weiß ich, welche Informationen ein IT-System über seine Nutzer sammelt und was eine Auswertung zu Tage bringen kann. Umso wichtiger ist es, in jeder Situation verantwortungsvoll mit Informationen umzugehen. mehr → (https://www.datenschutzbeauftragter-info.de/author/rkirsch/)

Externer Datenschutzbeauftragter (https://www.intersoft-consulting.de/datenschutzbeauftragter/externer-datenschutzbeauftragter/)

Mehr zum Thema: Cyber-Attacke (https://www.datenschutzbeauftragter-info.de/tag/cyber-attacke/), Passwort (https://www.datenschutzbeauftragter-info.de/tag/passwort/), Passwort-Sicherheit (https://www.datenschutzbeauftragter-info.de/tag/passwort-sicherheit/), Verschlüsselung (https://www.datenschutzbeauftragter-info.de/tag/verschluesselung/)