C-IAM GmbH: Authentifizierung - Begeistern Sie mit schicken Accessoires Ihre Mitarbeiter und erfüllen Ihre Rechenschaftspflicht!

KW 3: EU Datenschutz Grundverordnung 2018 von Joachim Jakobs (https://blog.c-iam.com)

Passwörter überfordern Nutzer – und lassen sich immer besser von Kriminellen knacken. Die Zwei-Faktor-Authorisierung könnte zur systematischen Bewältigung des Problems beitragen. Sie sind gesetzlich dazu verpflichtet, Ihre Datensicherheit nachweisen zu können. Ihre Mitarbeiter können Ihnen beim Erfüllen Ihrer Pflichten wesentlich helfen!

Mitte Januar meldete *Link* golem.de: „Twitter-Account des Spiegel-Chefs gehackt“ – stundenlang soll das Konto des Chefredakteurs Klaus Brinkbäumer von Dritten übernommen worden sein und in dieser Zeit den türkischen Staatspräsidenten beweihräuchert haben. Die feindliche Übernahme von Brinkbäumers Konto könnte mit einem schlechten Passwort zusammenhängen: Zwei Tage nach Bekanntwerden von Herrn Brinkbäumers Panne wurde eine Studie veröffentlicht *Link* der zufolge bei 81 Prozent aller Datenangriffe schwache Passwörter im Spiel gewesen sein sollen: So wie das WLan der Luther-Bibliothek im sachsen-anhaltinischen Zeitz mit dem Passwort „Martin“ „gesichert“ *Link* sein soll. Womöglich sind sich die Nutzer nicht darüber im Klaren, dass es Passwort-Lexika mit Milliarden Einträgen gibt *Link* .

Die Angegriffenen sind überfordert

Lange Zeit wurde empfohlen *Link* , Passwörter sollten häufig gewechselt werden, mindestens 8 Zeichen lang und „komplex“ sein, also nicht nur Groß- und Kleinbuchstaben, sondern auch noch Zahlen und Sonderzeichen enthalten.

Die Verantwortlichen in den IT-Abteilungen hätten das gegenüber Kunden, Partnern und Mitarbeitern per „Passwort-Politik“ durchsetzen *Link* können; tatsächlich scheinen sie häufig mit ihrer Aufgabe überfordert zu sein: 78 Prozent der „IT-Entscheider“ sollen nicht in der Lage *Link* sein, den Zugang zu cloud-basierten Anwendungen zu kontrollieren, knapp zwei Drittel

würden noch nicht einmal verhindern, dass ein Passwort von mehreren Personen genutzt wird. Was konsequent von den Angreifern ausgenutzt *Link* wird. Da die Chefs bei den IT-Anwendern mittlerweile zu 84 Prozent ihre Einkaufsentscheidungen mit Hilfe „sozialer“ Medien absichern *Link* , sollen Britische Unternehmen gar Gefahr laufen *Link* , auf diese Weise „Millionen“ zu verlieren. Und so manche Nutzer treiben den Unsinn ihrer schlechten Vorbilder auf die Spitze: Sean Spicer – der frühere Pressesprecher von US-Präsident Donald Trump – soll in der Woche seines Amtsantritts sein Passwort getwittert *Link* haben.

Die Cyber-Apokalypse

Die Leistungsfähigkeit der Informationstechnik spielt den Angreifern, nicht den Angegriffenen in die Hände: Die Angegriffenen sind noch genauso naiv wie zu Zeiten des Fax-Geräts, die Qualität der Angriffe befindet sich auf dem jeweiligen Stand der Technik. Und mit den Quantencomputern droht Link uns nach Ansicht von James Butterfill, Head of Research & Investment Strategy beim Britischen Anlageberater ETF Securities Ltd. Link eine „Cyber Apokalypse“: Heute gängige Verschlüsselungsverfahren würden obsolet, weil die Schlüssel „in Sekunden“ errechnet werden könnten. Es wird vermutet Link , dass neue Verschlüsselungsverfahren in zehn Jahren verfügbar sein könnten, doch will niemand seine Hand dafür ins Feuer legen, dass die Verfahren schneller als die Quantencomputer am Markt sind.

Passwort-Manager und Sicherheits-Sätze

Bis dahin sollten wir wenigstens von den heute vorhandenen Möglichkeiten Gebrauch machen: Liese und Otto Normalverbraucher könnten einen Passwortmanager verwenden – die Idee: Der Passwortmanager selbst erstellt ein neues Passwort anhand der Vorgaben des Nutzers (Länge, Groß-/Kleinbuchstaben, Sonderzeichen) und speichert alle Zugangsdaten der verschiedenen Dienste. Hier hat die c‘t vor Jahren solche Werkzeuge geprüft Link . Doch welches Werkzeug ist auch in Zukunft so vertrauenswürdig, dass Sie ihm guten Gewissens intimste Geheimnisse anvertrauen können? Manche Technik ist nicht nur löchrig – die Anbieter streiten auch noch darüber, ob Sie von den Löchern Kenntnis nehmen dürfen: Kurz vor Weihnachten 2017 wurde bekannt Link , dass die Firma Keeper Security den Journalisten Dan Goodin wegen eines Berichts über Sicherheitslücken verklagt hat. Der Vorwurf der Klage: „Ziel und Ergebnis des Artikels waren, Keeper und seine Mitarbeiter zu schädigen und Keeper Produkte schlecht zu machen." Nicht auszuschließen ist, dass sich Journalisten auf diese Weise eingeschüchtert fühlen und nicht über Lücken berichten. Was ebenfalls den Angreifern in die Hände spielt.

Andere mögen Link die „MasterPassword App“: Die Anwendung soll aus dem MasterPassword dieser Anwendung und dem Namen des jeweiligen Dienstes ein einmaliges Passwort generieren. Auch wenn HeiseSecurity-Chefredakteur Jürgen Schmidt und andere Link von der Anwendung begeistert zu sein scheinen, so ist dies noch kein Nachweis der Sicherheit dieses Dienstes – vor einem Jahr hieß Link es bei theregister: „Sicherheitspannen bei 1Password und anderen Passwort-Managern ‚extrem beängstigend‘“. Ich kann weder diese Aussage noch die Sicherheit irgendeiner anderen Anwendung beurteilen; aber solang ich kein Zertifikat von einer unabhängigen Institution gesehen habe, das diesem Werkzeug glaubwürdig Sicherheit bescheinigt, bewahre ich mir mein Misstrauen.

Ich persönlich bilde immer Sätze mit dem Namen des jeweiligen Dienstes – ein solcher Satz könnte für C-IAM zum Beispiel lauten „Ich bin ein Fan von C-IAM!“ – wenn man nur die Initialen der einzelnen Worte aus diesem Satz übriglässt, erhält man das neunstellige „IbeFvC-I!“ – im Vergleich zur Masse der Passwörter schon recht komplex. Wenn Sie da jetzt noch das

„e“ durch die Zahl „1“ ersetzen und dem Passwort zum Beispiel „¹“ und „?“ (Beide Zeichen befinden sich ziemlich an den Rändern der Tastatur und lassen sich damit gut merken!) setzen, sieht das schon richtig gut aus: „¹Ib1FvC-I!?“ – es enthält immerhin 11 Stellen einschließlich Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen. Mit der Veröffentlichung hier ist dieses Passwort jetzt allerdings bekannt und sollte nicht mehr genutzt werden.

DSGVO, BDSG und 2FA

Jetzt die Konsequenzen für Unternehmen, die Mitarbeiter und Kunden identifizieren wollen: § 64 BDSG (neu) – die Präzisierung der DSGVO in Deutschland – verlangt Link , „die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, Link “ Also zuerst einmal zurück auf Los und eben rasch eine Risikoanalyse Link anstellen!

Zum Weiterlesen des gesamten Artikels klicken Sie bitte auf:

https://blog.c-iam.com

Kontakt

Jamshed Kharkan
Geschäftsführer

Tel: +49 228 53459235
E-Mail: blog@c-iam.com

C-IAM GmbH
Ballindamm 39
D-20095 Hamburg

https://www.c-iam.com
https://blog.c-iam.com