UIMCommunic@tion

04/2020

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Pflicht zum Passwortwechsel nicht voreilig streichen

Die Mails oder Hinweise mit dem Inhalt „Ihr Passwort ist älter als 90 Tage. Bitte ändern Sie es.“ sind bekannt, aber ist das wirklich hilfreich? Rund um den „Ändere-Dein-Passwort-Tag“, der in jedem Jahr am 1. Februar stattfindet, entbrannte eine intensive Diskussion. Schwerpunkt: Wie sinnvoll ist es, sein Passwort regelmäßig zu wechseln? Erhöht dies die Sicherheit meines Accounts oder ist es sogar eine Gefahr? Sogar das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat sich klar positioniert: Die Experten des Bundesamtes rudern von ihrer bisherigen Empfehlung zurück, Passwörter häufig zu wechseln. Demnach könnte ein Passwort auch jahrelang genutzt werden, wenn es die richtigen Kriterien erfüllt. „Die Diskussion als solches sorgt für Aufmerksamkeit und steigert die Sensibilität für das Thema Cybersicherheit“, freut sich der erfahrene Datenschutzfachmann Dr. Jörn Voßbein über die Debatte. ***Eine Zusammenfassung der Diskussion, was macht ein starkes Passwort aus und die fachliche Einschätzung von UIMC erfahren Sie hier:***

Fahrt nahm die Passwörter-Diskussion Anfang Februar auf: Das BSI rückte von seiner bisherigen Position ab, Passwörter regelmäßig zu ändern. In der aktuellen Ausgabe des BSI-Grundschutz-Kompendiums wurde die entsprechende Textpassage gestrichen. Passwortänderungen sind aus BSI-Sicht nur noch für folgende Fälle angeraten: 1. Ein Passwort sollte auf jeden Fall geändert werden, wenn es einen Hinweis gibt, dass es tatsächlich in die Hände von unbefugten Dritten gelangt ist. 2. Wenn festgestellt wird, dass das eigene Gerät mit einem Schadprogramm infiziert ist. 3. Wenn Cyber-Kriminelle bei Anbietern oder direkt bei Nutzerinnen und Nutzern vertrauliche personenbezogene Daten (inklusive Passwörtern) abgegriffen haben.

Die BSI-Experten raten im Kapitel zur Regelung des Passwortgebrauchs nur für den Fall, dass ein Passwort in fremde Hände geraten sein könnte, das Kennwort zu ändern. Auch die dort bisher aufgeführte Verpflichtung, feste Regeln für Länge und Komplexität vorzuschreiben, ist verschwunden. Von Teilen der Fachwelt wurde dieser Kurswechsel begrüßt, aber erhöht er tatsächlich die Sicherheit? Hier muss aus Sicht der Experten von UIMC ein dickes Fragezeichen gemacht werden. Klar ist, dass Passwortänderungen, die über Jahre hinweg nur aus der Addierung der Zahl bestehen, eine Scheinsicherheit suggerieren. Beispiel: Das bestehende Passwort KleineMaus15% wird auf KleineMaus16% verändert. Angreifer können solche Passwörter oftmals schnell erraten und knacken. „Gerade bei kritischen und hochsensiblen Systemen sollte aber weiterhin ein regelmäßiger aber echter Passwortwechsel vorgenommen werden“, empfiehlt UIMC-Geschäftsführer Dr. Jörn Voßbein am bewährten Passwortwechsel festzuhalten. Alles andere ist aus seiner Sicht leichtsinnig, zumal ein entstehender Schaden deutlich größere Probleme hervorrufen kann, als die Mühen sich alle 90 oder 180 Tage ein neues Passwort zu merken. „Der Aufwand für ein neues und sicheres Passwort ist deutlich kleiner, als der Schaden, den Cyberkriminelle anrichten können.“.

„Ein großer Knackpunkt der im Rahmen der Debatte um die Abschaffung des Passwortswechselzwangs immer wieder vergessen wird ist das Social Engineering“ so Dr. Voßbein. „Zum einen könnten umstehende Personen einen immer mal wieder beim Eintippen eines Passworts beobachten und so mit der Zeit das entsprechende Passwort erraten, ohne dass man selbst es merkt. Zum anderen kann durch den stetigen Passwortwechsel ein Dritter, der die Zugangsdaten entwendet hat, wieder aus einen Benutzerkonto ausgesperrt werden“.

Fortsetzung auf der nächsten Seite >>

FAQ: Praxishilfe zum Einsatz von Videokonferenzsystemen

Aus datenschutzrechtlicher Sicht sind bei dem Einsatz von Cloud-basierten Webinar-Anwendungen und Videokonferenzschaltungen einige Punkte zu beachten, sodass ein rechtskonformer Betrieb solcher Systeme gewährleistet ist. Diese finden in unserem eCollege-Kurs „FAQ“: https://www.uimcollege.de > Meine Kurse.

Dieser Kurs ist im **neuen eCollege** für alle User freigeschaltet, die einen Account zu einem Schulungskurs haben. Sie haben noch keinen Zugang? Dann informieren Sie sich unter https://www.uimc.de/seminareschulungen/ecollege.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Wie geht man mit Passwörtern richtig um und erleichtert seinen Alltag? Zum einen kann der Einsatz von Passwort-Managern auf dem Rechner die Kennwörter speichern und deren Einsatz vereinfachen. Zum anderen sollten unterschiedliche Passwörter verwandt werden. Konkret: Für das Online-Banking sollte ein völlig anderes Passwort verwandt werden als für den AmazonPrime-Account. Oftmals setzen viele Nutzer dasselbe Passwort bei mehreren Diensten ein. Die Gefahr: Gelangt ein Angreifer etwa an das AmazonPrime-Passwort, könnte er sich damit auch gleich in das Bankkonto einloggen. Daher sollte jeder Dienst mit einem unterschiedlichen Kennwort geschützt werden. „Jeder sollte bei seinen Passwörtern vorsichtig und aufmerksam vorgehen, um sich vor kriminellen Machenschaften zu schützen. Die Abschaffung des regelmäßigen Passwortwechsels kann dabei nicht das richtige Mittel sein“, hebt Dr. Voßbein hervor.

„So ist summarisch betrachtet das Abrücken von der Forderung nach einem Passwortwechselzwang vor allem unter dem Gesichtspunkt der Informationssicherheit nicht zu empfehlen, da davon ausgegangen werden muss, dass die Offenlegung eines Passwortes häufig unbemerkt bleibt. Jedoch könnte aber eine Ausdehnung des Gültigkeitszeitraums in unkritischen Bereichen eines Unternehmens in Betracht gezogen werden“ resümiert Dr. Voßbein.

Wie sollte ein Passwort gestaltet sein?

Die Passwortgestaltung sollte einen Kompromiss zwischen den Sicherheitszielen darzustellen:

» Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist.

» Die Anzahl der durch das vorgegebene Schema möglicher Passwörter muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.

» Das Passwort darf nicht zu kompliziert sein, damit der Benutzer mit vertretbarem Aufwand in der Lage ist, es sich zu merken.

Wie sage ich es den Mitarbeitern?

Neben der Schaffung transparenter, verbindlicher Regelungen (ergo: Nicht nur die technischen Regeln im System entsprechend der Passwortkonventionen definieren und umsetzen), sondern auch die Schulung und Sensibilisierung der Mitarbeiter ist wichtig. Erst, wenn der Mitarbeiter versteht, warum er diese Regeln einhalten muss (schließlich sind Passworte ja „nervig“), wird er diese auch tatsächlich beachten. Hierzu können Präsenzschulungen oder E-Learning-Kurse genutzt werden.

Updates im Online-Formular-Center

» [neu] Informationspflichten für Videokonferenzsysteme

» [neu] Muster-Schreiben für Auskunftsersuchen eines (ehem.) Mitarbeiters

www.online-formular-center.eu

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

☐ Sichere Passwortregeln

☐ Datenschutzkonformer Einsatz von Videokonferenzsystemen

☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.