Hackerkollektiv deckt Sicherheitslücken bei Corona-Testzentren auf – Schwache Passwörter und lückenhafte Verschlüsselung sind schuld

Ein Kommentar von Jörg Horn, Chief Product Officer bei uniscon

München, 25.06.2021 – Das Hackerkollektiv „Zerforschung“ hat erneut eine gravierende Sicherheitslücke bei Corona-Testzentren aufgedeckt. Die Spezialisten hatten nach eigenen Angaben keine Mühe, sich Zugriff auf 174.000 Datensätze zu verschaffen, darunter Buchungsbestätigungen sowie streng vertrauliche, personenbezogene Daten wie Name, Anschrift, Telefonnummer, E-Mailadresse und Geburtsdatum der Patienten. Selbst Testergebnisse und in einigen Fällen sogar die Ausweisnummer lagen den Angreifern vor.

Wie konnte das passieren?

Die Passwörter der Accounts wurden geradezu schlampig generiert und ungesichert übermittelt: In Aufsteigender Reihenfolge wurden von der im Einsatz befindlichen Software Passwörter aus den Zahlen 0-9 sowie aus den Buchstaben A-F zusammengesetzt. Die Hacker hatten somit leichtes Spiel, massenhaft Patientendaten einsehen zu können.

Das BSI bezeichnete den Vorfall als „gravierendes IT-Sicherheits- und Datenschutzproblem“. Betroffen sind 34 Testzentren des Betreibers PAS Solutions in vier Bundesländern. „Zerforschung“ vermutet hinter der Sicherheitslücke mangelndes Personal in den für die Aufsicht zuständigen Behörden.

Die Lösung: Konsequente Verschlüsselung, starke Passwörter und Zwei-Faktor-Authentifizierung

Die Bewertung eines Vorfalls im Nachgang ist eine vermeintlich einfache Disziplin. Mit Kenntnis der genauen Vorgangsweise der Hacker und der Schwachstellen in der betroffenen IT-Struktur können Sicherheitsexperten schnell eine Strategie mit Gegenmaßnahmen formulieren.

Doch in diesem Fall ist es nicht dem Einfallsreichtum der Angreifer zuzurechnen, dass die Patientendaten entwendet werden konnten. Hier fehlte es an der Einhaltung grundlegender Prinzipien der Datensicherheit – vor allem die unbedachte Generierung simpler Passwörter machten es den Angreifern leicht, die Passwörter mit Hilfe von Brute Force zu „erraten“. Abgesehen davon sollten sensible digitale Informationen niemals im Klartext kommuniziert werden. Ansonsten sind sie Cyberkriminellen schutzlos ausgeliefert.

Geschäftsfelder wie das Gesundheitssystem, die mit besonders sensiblen Daten operieren, sollten daher unter allen Umständen auf eine lückenlose Verschlüsselung ihrer Daten setzen. Ausnahmslos! Denn der damit verbundene zusätzliche Aufwand steht in keinem Verhältnis zu dem Risiko, das ohne sie eingegangen wird. Und das meist ohne Kenntnis der betroffenen Patienten oder Kunden. So wurden laut „Zerforschung“ selbst eine Woche nach Bekanntwerden der Sicherheitslücke die Betroffenen nicht vom Betreiber informiert.

Die Digitalisierung steht und fällt mit dem Datenschutz

Um der Digitalisierung des öffentlichen Lebens – einschließlich Behördengänge, Arztbesuche oder zukünftig auch Wahlen – zum Erfolg zu verhelfen, benötigt es die Akzeptanz aller Nutzer. Um auch die letzten Skeptiker von den Vorzügen digitaler Lösungen zu überzeugen, dürfen sich Vorfälle wie dieser nicht wiederholen.

Gerade in Zeiten, da immer mehr Betriebe und sogar streng regulierte Branchen ihre Daten in die Cloud migrieren, sind vertrauensbildende Maßnahmen der IT-Sicherheit von größter Bedeutung. Die grundsätzliche Verschlüsselung bei der Übertragung und Speicherung von sensiblen Daten ist dabei genauso als nicht diskutierbare Grundlage zu sehen wie der flächendeckende Einsatz starker Passwörter und der Zwei-Faktor-Authentifizierung.

Wurde Ihnen diese Pressemeldung weitergeleitet? Hier können Sie sich zu unserem Presseverteiler anmelden.

Aktuelle Artikel zu den Themen Datenschutz und Datensicherheit finden Sie im privacyblog.

uniscon – A member of TÜV SÜD

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons *Sealed Platform®* bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.

uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).

Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten *Sealed Cloud Technologie*, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design“ entwickelt.

Uniscon wurde 2009 gegründet und ist seit 2017 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Pressekontakt
uniscon GmbH, Wilhelm Würmseer
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20