Geschrieben von: Lorenz
Donnerstag, den 20. Mai 2021 um 16:37 Uhr

Der Hinweis kam von einem "Whitehat-Hacker"

Sicherheitslücke im Impfportal Niedersachsen – Ministerium lässt Datenleck schließen

Donnerstag 20. Mai 2021 - **Hannover (wbn). Auch das noch – Sicherheitspanne beim Impfportal Niedersachsen! Das Gesundheitsministerium hat ein Datenleck stopfen lassen, nachdem es einem Computer-Hacker gelungen war, sensible Daten aus dem System einzusehen. Darüber hat die Behörde heute selbst informiert.**

Aufgespürt und gemeldet worden war die Sicherheitslücke durch einen "Whitehat-Hacker". Das Gesundheitsministerium hatte daraufhin Entwickler Majorel mit der unverzüglichen Behebung der Schwachstelle beauftragt.

Fortsetzung von Seite 1

Nachfolgend der detaillierte Bericht des Niedersächsischen Ministeriums für Soziales, Gesundheit und Gleichstellung vom Donnerstagmittag im Wortlaut:

"Dank des anonymen Hinweises eines sogenannten „friendly hackers" (freundlicher Hacker) an das Computer-Notfallteam Niedersachsen-CERT und das Gesundheitsministerium konnte eine Sicherheitslücke im Impfportal unter www.impfportal-niedersachsen.de behoben werden, bevor sie von weiteren Personen ausgenutzt werden konnte."

Freundliche Hacker, auch „whitehats" genannt, suchen Sicherheitslücken in Computersystemen und weisen die Betreiberinnen und Betreiber darauf hin, damit sie frühzeitig geschlossen werden können.

Am 7. Mai 2021 erhielten das Gesundheitsministerium und das Niedersachsen-CERT eine E-Mail der Hinweisgeberin oder des Hinweisgebers unter dem Namen „Impfportal Whitehat". Darin schilderte der Hacker, dass es ihm gelungen sei, über das Impfportal Zugriff auf Namen und Adressen von registrierten impfwilligen Personen zu erhalten. Weiter hieß es in der Mail:

„Eins vorweg: Ich habe nur gute Absichten und möchte dazu beitragen, dass die Lücke schnell geschlossen wird, bevor andere diese ebenfalls entdecken. Ich versichere ihnen hiermit, dass meine bisherigen Abrufe rein zum Aufspüren dieser Sicherheitslücke dienten und ich KEINERLEI Daten hieraus gespeichert habe."

Das Gesundheitsministerium informierte daraufhin unverzüglich den für die Programmierung der Webseite verantwortlichen Dienstleister Majorel, der die geschilderte Sicherheitslücke nachvollziehen und noch am Abend des 7. Mai schließen konnte.

Majorel hat nach eingehender Untersuchung des Vorgangs festgestellt, dass

1. eine Funktion für die Schwachstelle gesorgt habe, die für den Betrieb der Impfzentren ermöglicht, nach Datensätzen von registrierten Impfwilligen zu suchen. Diese Funktion ist für die Arbeit der Mitarbeiterinnen und Mitarbeiter an der Hotline unerlässlich, wenn beispielsweise Personen anrufen, die Ihren Termincode verloren haben und dann anhand ihres Namens identifiziert werden müssen.
2. es insgesamt 50 Zugriffe und Zugriffsversuche auf das System gegeben habe, von denen 37 erfolgreich waren. Alle Zugriffe erfolgten am 6. und 7. Mai, also unmittelbar vor der Warnung des friendly Hackers an das Land. Daher ist mit an Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass alle registrieren Zugriffe dieser Person zuzurechnen sind.
3. bei den Zugriffen die Datensätze von insgesamt 1.258 registrierten Personen abgerufen bzw. angezeigt worden seien.
4. zum Ausnutzen der Schwachstelle Insiderwissen über die Anwendung notwendig sei,
5. die Sicherheitslücke nicht aktiv ausgenutzt worden und
6. eine Manipulation von Datensätzen ausgeschlossen sei.

Im entsprechenden Bericht von Majorel heißt es weiter:

Zusammenfassend kann die Schwachstelle so beschrieben werden, dass für den Betrieb der

Impfzentren nach Datensätzen von Impfwilligen gesucht werden kann. Diese Schnittstelle liefert basierend auf Parametern wie z.B. dem Nachnamen bis zu 500 Suchergebnisse zurück.

Der Informant der diese Schwachstelle entdeckt hat, muss diese Funktion, welche nur aus dem geschützten VPN-Bereich, nach Anmeldung via Benutzername und Passwort zugänglich ist, aufgegriffen und auf dem Bürgerportal angewendet haben. Hierzu hat er sich auf dem Bürgerportal angemeldet und per SMS authentifiziert. Dieser Authentifizierungstoken ist für 120 Sekunden gültig und konnte ungeplant für die Abfrage der Schnittstelle in diesen zwei Minuten genutzt werden.

Eine Analyse der Logfiles ergab insgesamt 50 Zugriffe und Zugriffsversuche am Donnerstag, 6.5.2021 und Freitag, 7.5.2021. Es konnten keine Zugriffe vor dem 6.5.2021 festgestellt werden. Weitere Zugriffsversuche werden engmaschig überwacht.

Gesundheitsstaatssekretär Heiger Scholz erklärt zu dem Vorgang: „Dank der Warnung des friendly Hackers konnte eine bedauerliche Sicherheitslücke im Impfportal geschlossen werden, bevor sie von weiteren Personen ausgenutzt werden konnte. Für diese Warnung sind wir sehr dankbar. Nichtsdestotrotz handelt es sich hierbei um einen Verstoß gegen den Datenschutz. Wir gehen davon aus, dass die Daten vom friendly Hacker nicht gespeichert wurden und den Betroffenen kein Schaden entstanden ist. Dennoch werden wir sie in den nächsten Tagen per Brief über diesen Vorgang informieren, um maximale Transparenz für alle Beteiligten herzustellen."

Das Gesundheitsministerium hat auch die Landesdatenschutzbeauftrage über die vorliegende Datenschutzverletzung nach Artikel 33 DS-GVO informiert."