# Digitaler Impfnachweis
## Reichlich Lücken im System

**[12.5.2022] Der digitale Impfnachweis wurde in Deutschland mit allzu heißer Nadel gestrickt – und zeigt daher in puncto Sicherheit und Zuverlässigkeit erschreckend viele Mängel. Die Sicherheitslücken nachträglich zu stopfen, ist schwierig bis unmöglich.**

Eigentlich kümmert sich Thomas Siebert bei der G DATA CyberDefense AG um die Entwicklung neuer Schutztechnologien für Computernetzwerke in Unternehmen und Behörden. Am Thema Corona und damit am digitalen Impfnachweis kam aber auch er nicht vorbei. Hier fielen ihm immer wieder einige lose Enden auf. Die erste Ungereimtheit zeigte sich im privaten Umfeld. Ein Bekannter hatte sich direkt nach der zweiten Impfung seinen QR-Code mit dem digitalen Impfnachweis in der Apotheke besorgt und eingescannt. Zu seiner und Sieberts Überraschung zeigte jede App, dass er vollständig geimpft sei. Dabei sollte der Impfstatus erst zwei Wochen nach der Impfung auf "vollständig geimpft" umschalten. Ein genauerer Blick auf die Daten zeigte: Aus Versehen stand beim Datum der Zweitimpfung der Tag der Erstimpfung. Und die lag ja bereits deutlich mehr als zwei Wochen zurück.
Ein harmlos anmutender Fehler, der jedem passieren kann. Wer täglich so viele Impfnachweise erstellt, kann schon mal in der Zeile verrutschen. Aber hätte das System so etwas nicht automatisch anmahnen müssen, um eine Korrektur zu ermöglichen? Die Neugier war geweckt. Wenn ein harmloses Versehen bereits dazu führen kann, dass ein Mensch vorzeitig als geimpft gilt – was ist dann erst mit krimineller Energie möglich?

**Mit heißer Nadel gestrickt**

Und so begann eine Suche, die wenig Ermutigendes zutage fördern sollte. Ausgangsbasis war die Spezifikation der EU, die die technische Umsetzung vorgab. Nach einem umfassenden Blick in die Spezifikationen und die tatsächliche Umsetzung stand fest: Es mangelt dabei an allen Ecken und Enden. Vieles, was die Sicherheit und Zuverlässigkeit hätte erhöhen können, ist entweder ganz ausgeblieben oder wurde nur halbherzig umgesetzt. Vieles deutet darauf hin, dass der digitale Impfnachweis in Deutschland mit heißer Nadel gestrickt wurde, wohl nicht zuletzt durch politischen Druck.
Da ist zum einen die Ausstellung der Impfnachweise und die Art und Weise, wie diese digital signiert sind. In Deutschland werden

alle Impfnachweise in letzter Konsequenz vom Robert Koch-Institut (RKI) ausgestellt. Für die Ausgabe und Signierung sind unter anderem die Apotheken zuständig. Der Deutsche Apothekenverband bietet allen angeschlossenen Apotheken die Möglichkeit, sich in einem Web-Portal anzumelden, dort die Daten der Person einzugeben, die einen Impfausweis vorlegt, und den digitalen Impfnachweis herunterzuladen. Auch hier zeigten sich schnell gravierende Versäumnisse. So sind die entsprechenden Portale nur mit einer Kombination aus Benutzernamen und Passwort gesichert, wobei jede Apotheke einen einzigen Zugang erhält.

**Mehr Impfnachweise als Impfungen**

Insgesamt gibt es 42 Millionen mehr Impfnachweise als es überhaupt Impfungen gab – teilweise wurden Zertifikate mehrfach ausgestellt, weil das Impfzentrum erst im Nachhinein ein solches generiert hat, die Geimpften sich aber bereits vorher in der Apotheke ihren Nachweis abgeholt haben. Möglicherweise wurden Zertifikate auch mehrfach ausgestellt, weil einem Apotheker ein Fehler bei der Dateneingabe unterlaufen ist. Zudem sind hunderttausende Impfnachweise in Deutschland mit derselben digitalen Unterschrift signiert, etwa der des Apothekerverbands. Im Missbrauchsfall wäre es praktisch unmöglich, die ausgestellten Zertifikate durch ein Widerrufen der digitalen Unterschrift nachträglich ungültig zu machen. Denn damit müssten auch alle legitim ausgestellten Impfnachweise neu ausgestellt werden. Theoretisch hätte jeder und jede Mitarbeitende in einer Apotheke eine eigene Signatur bekommen müssen, um den Impfnachweis digital zu "stempeln". Das wäre technisch ohne weiteres möglich, allerdings mit Mehraufwand verbunden.
Darüber hinaus sind einige wichtige Daten im digitalen Impfnachweis gar nicht hinterlegt, die im gelben Impfbuch enthalten sind. Dazu gehören beispielsweise der Ort der Impfung oder die Chargenbezeichnung des verimpften Wirkstoffs.
Apotheken haben keine technische Möglichkeit, die Echtheit der Daten zu verifizieren. Sie müssen also zunächst davon ausgehen, dass die vorgelegten Impfpässe echt sind. So überrascht es nicht, dass Menschen Wege suchten, einen Impfnachweis auch ohne Impfung zu erhalten. Schnell tauchten im Internet Web-Seiten auf, auf denen Betrüger gefälschte gelbe Impfpässe zum Kauf anboten, die "garantiert anerkannt würden". Selbst digitale Impfnachweise wurden gehandelt. Bittere Ironie: In einigen dieser kriminellen Webshops war auch ein TV-Interview mit Thomas Siebert zum Thema verlinkt, mit dem Hinweis "Seht ihr – unsere Nachweise

funktionieren wirklich!"

**Auch die Corona-Apps lassen zu wünschen übrig**

Auch die Systeme – vor allem die Apps – und die Prozesse, welche die Bürger nutzen sollen, lassen zu wünschen übrig. Die ansonsten zurecht vielgelobte Corona-Warn-App (CWA) bot die Möglichkeit, den digitalen Impfnachweis einzuscannen, um ihn bei Bedarf vorzuzeigen. Das funktionierte auch – allerdings erkannte die App anfangs keine gefälschten Impfzertifikate. Auch die CovPass-App erkannte ein erfundenes Zertifikat als gültig an. Aus rein technischer Sicht ergibt das sogar Sinn, denn der Prozess sieht vor, dass zum Scannen und Validieren die CovPassCheck-App zum Einsatz kommt und dass die angezeigten Daten mit einem vorgelegten Ausweis abgeglichen werden. Allerdings war die CovPassCheck-App gerade am Anfang kaum verbreitet. Eine korrekte Prüfung hatte daher lange Seltenheitswert.
Hinzu kommt, dass es keine großen Programmierkenntnisse erfordert, um sich zu Hause einen digitalen Impfnachweis selbst zu basteln. Vielmehr geht dies innerhalb von Sekunden, wie es auch Siebert vor laufender Kamera demonstrierte. Die Umsetzung des digitalen Impfnachweises stellt so praktisch eine offene Einladung zum Missbrauch dar und Siebert ließ keinen Zweifel daran, dass es diesen im großen Maßstab geben werde. Diese Voraussage sollte sich mehr als bewahrheiten. So schätzte vor Kurzem der Präsident der Apothekerkammer Baden-Württemberg, Martin Braun, dass sich die Anzahl der im Umlauf befindlichen gefälschten Nachweise im sechsstelligen Bereich bewegen dürfte. Mittlerweile wurde technisch zwar die Möglichkeit zum Blockieren einzelner Impfnachweise geschaffen, sodass diese dann nicht mehr als gültig anerkannt werden. Praktisch wird diese Möglichkeit in Deutschland aber kaum genutzt. Die Corona-Warn-App etwa blockiert nur die Impfnachweise einer einzigen Münchner Apotheke, die beim Erstellen von Fälschungen erwischt wurde. Andere Länder haben vergleichbare Möglichkeiten zum Blocken falscher Impfnachweise geschaffen, ein internationaler Abgleich der Listen findet aber nicht statt. Ein falscher Impfnachweis, der in einem Land als ungültig markiert ist, könnte in einem anderen Land also nach wie vor den begehrten grünen Haken tragen.

**Nachträglich Sicherheit einbauen? Schwierig bis unmöglich**

Zurück bleibt die ernüchternde Erkenntnis, dass es schwer bis unmöglich ist, nachträglich Sicherheit in ein bestehendes System einzubauen. Das resultiert nur in einer unsäglichen Flickschusterei, bei der bloß Lücken gestopft werden, die es bei besserer Planung

gar nicht erst gegeben hätte. Ein so kritisches System mit heißer Nadel zu stricken, schadet nicht nur der Sicherheit als Ganzes. Es ist auch enorm schädlich für das Vertrauen von Menschen in ein System, das sie eigentlich schützen sollte. Konsequenz: Zwischenzeitlich weigerten sich einige Händler und Restaurants, den gelben Impfpass als Nachweis einer Impfung anzuerkennen – weil der ja gefälscht sein könnte.

*Tim Berghoff ist Security Evangelist bei der G DATA CyberDefense AG, Bochum.*

https://www.gdata.de
Dieser Beitrag ist in der Ausgabe Mai 2022 von Kommune21 im Schwerpunkt Gesundheitswesen erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren. (Deep Link)

Stichwörter: IT-Sicherheit, Corona, Impfnachweis, Corona-Warn-App, G DATA

*Bildquelle: janvier/stock.adobe.com*

---

**Quelle:** www.move-online.de