CCC-Warnung zur ePA: Hinweise für Zahnarztpraxen

Ende Dezember hat der Chaos Computer Club (CCC) eine potentielle Sicherheitslücke der ePA für alle demonstriert. In der Zwischenzeit wurden durch die gematik in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits Maßnahmen entwickelt und erste Maßnahmen umgesetzt, welche die Sicherheitslücken schließen sollen. Allerdings hat der CCC auch Punkte aufgezeigt, die von den Praxen selbst berücksichtigt werden müssen. Was Zahnarztpraxen tun können, zeigt dieser Überblick.

Das Angriffsszenario

Grundlage des Angriffs waren zwei verschiedene Angriffsvektoren. Zum einen ein freigeschalteter Praxisausweis (SMC-B) inklusive PIN plus selbst beschaffter TI-Zugangstechnik und zum anderen der vollständige Zugang zur IT einer Praxis. Die SMC-B konnten sich die Sicherheitsforscher des CCC über den Gebrauchtmarkt von eHealth-Kartenterminals beschaffen (mit aufgeklebter PIN der SMC-B), während sie sich den Zugang zur Praxis-IT (inkl. aller Zugangsdaten) durch ein vorgetäuschtes Angebot von IT-Dienstleistungen erschleichen konnten.

Die Sicherheitsforscher hatten damit grundsätzlich die Möglichkeit, die Telematik-Identität und die Konnektor-Schnittstelle der angegriffenen Praxis zu nutzen und somit auf die ePA-Akten zuzugreifen, für die eine ePA-Befugnis für die Telematik-ID der verwendeten SMC-B eingestellt worden ist. Davon wären alle Versicherten mit ePA betroffen gewesen, die in den letzten 90 Tagen in der angegriffenen Praxis vorstellig geworden sind oder die Praxis über ihre ePA-App für den Zugriff berechtigt haben.

Was können Zahnarztpraxen tun?

Mit der Beachtung bestehender Vorgaben und einiger Grundregeln können Zahnarztpraxen das Risiko, Opfer des gezeigten Sicherheitsvorfalls zu werden und damit potentielle Angriffe auf Patientendaten zu ermöglichen, wirksam reduzieren.

Vor allem der regelkonforme Umgang mit der SMC-B und das Bewusstsein für die Gefahren von Social Engineering können helfen, Gefahren abzuwenden.

Verantwortungsvoller Umgang mit der SMC-B und PIN

Die SMC-B ist als praxisbezogene Smartcard eine Sicherheitsmodulkarte und repräsentiert mit ihren Schlüsseln und Zertifikaten die Praxis in der Telematikinfrastruktur (TI). Die SMC-B weist somit die Identität der Praxis in der TI nach und gewährt ihr Zugriff auf medizinische Daten in der TI. Daraus folgt, dass der Verkauf oder Verlust der SMC-B die Gefahr birgt, dass Unbefugte den Ausweis nutzen, um unter der Identität der Praxis Zugang zur TI und zu den dort gespeicherten Daten zu erhalten. Zu beachten ist außerdem, dass zum Beispiel Zugriffe auf die ePA protokolliert werden und damit der jeweiligen Praxis anhand der verwendeten SMC-B zugeordnet werden können.

Eine SMC-B darf aus diesem Grund unter keinen Umständen verkauft werden. Sollte (was nicht zu empfehlen ist) ein eHealth-Kartenterminal verkauft werden, muss unbedingt darauf geachtet werden, dass die SMC-B nicht mehr steckt. Vorsicht: Die SMC-B ist leicht mit der (unkritischen) Gerätekarte des Kartenterminals zu verwechseln. Wo welche Karte im Kartenterminal steckt, kann der Betriebsanleitung des jeweiligen Geräts entnommen werden.

Der Schutz der zugehörigen PIN ist eine weitere wichtige Maßnahme, um eine missbräuchliche Nutzung der SMC-B zu verhindern. Auf keinen Fall darf die PIN auf die Karte oder das Kartenterminal geschrieben oder ungeschützt aufbewahrt werden!

Die wichtigste Grundregel für die Nutzung der SMC-B ist: Die Karte darf nicht in die Hände unbefugter Dritter gelangen und die dazugehörige PIN muss sicher aufbewahrt werden. Andernfalls besteht die Gefahr, dass Angreifer unter Nutzung der Identität der Praxis auf medizinische Daten in der TI zugreifen und damit hohen Schaden anrichten. Weitere Regeln für die Nutzung der SMC-B sind:

- **Persönliche Verantwortung**: Verantwortlich für die Nutzung ist der Inhaber. Inhaber eines Praxisausweises ist die Praxis selbst. Davon zu unterscheiden ist der Kartenverantwortliche, der für die Einhaltung der Sicherheitsvorgaben verantwortlich ist.
- **Unbefugten Einsatz verhindern**: Der Kartenverantwortliche muss die notwendigen Vorsichtsmaßnahmen ergreifen, um einen unbefugten Einsatz der SMC-B zu verhindern. Dazu zählt u. a. die Verwaltung und der Schutz der Zugangsdaten der SMC-B (PIN und PUK).
- **Beschränkte Nutzung**: Die Nutzung der SMC-B ist auf die Orte beschränkt, die sich aus der Zulassung bzw. Ermächtigung ergeben.
- **Dokumentation der Nutzung**: Verfügt der Inhaber über mehrere SMC-Bs, ist er zur Dokumentation des jeweiligen Einsatzortes verpflichtet. Gleiches gilt, wenn der Praxisausweis an mehreren Praxisstandorten eingesetzt wird.
- **Sperrung**: Der Karteninhaber ist zudem verpflichtet, den Verlust der SMC-B bei der zuständigen KZV anzuzeigen und die SMC-B über die Sperr-Hotline des Anbieters sperren zu lassen oder die KZV mit der Sperrung zu beauftragen. Bei einer Praxisaufgabe wird die Sperrung im Rahmen von definierten Prozessen und Vorgaben durch die KZV vorgenommen.

Schutz vor Social Engineering

Für den Zugang zur Praxis-IT haben die Sicherheitsforscher des CCC das Vertrauen eines Praxismitarbeiters ausgenutzt, um ihn gezielt zu manipulieren. Dieses sogenannte Social Engineering ist kein spezielles TI-Thema, sondern findet heute grundsätzlich im Kontext von digitalem Betrug im Internet statt. Die bekannteste Form von Social Engineering ist das Phishing, also das Sammeln von Passwörtern durch echt wirkende E-Mails.

Bei Angriffen mittels Social Engineering täuschen die Täter das Opfer über ihre Identität und ihre Absichten. Im konkreten Fall haben sich die Sicherheitsforscher des CCC als angeblicher IT-Dienstleister ausgegeben. Unter dem Vorwand, ein vermeintliches Sicherheitsproblem mittels Remote-Zugriffs zu lösen, wurden Zugangsdaten und Passwörter erfragt. Das Opfer handelte im Glauben, das Richtige zu tun, und händigte die Daten aus. Dadurch gelangten die Sicherheitsforscher in das ansonsten geschützte Praxisnetz und kamen so auch in den Zugriff auf die Konnektor-Schnittstelle. Abhängig davon, welche Zugangsdaten und Passwörter ausgehändigt werden, können durch Social Engineering erhebliche Schäden entstehen.

Um das Risiko von Social Engineering zu reduzieren, sollten Zahnarztpraxen folgende Regeln beachten:

- **Keine Auskunft am Telefon oder per E-Mail:** Keine Passwörter, Zugangsdaten oder sonstige sensible Daten der Praxis per Telefon oder E-Mail teilen. Seriöse IT-Dienstleister und Firmen fordern ihre Kunden niemals per E-Mail oder Telefon zur Angabe von vertraulichen Informationen auf.
- **Kontaktaufnahme durch IT-Dienstleister:** Ein seriöser Anbieter von IT-Dienstleistungen würde nicht nach sensiblen Daten oder vertraulichen Informationen fragen, schon gar nicht beim Erstkontakt im Rahmen einer Kontaktaufnahme.
- **Umgang mit zweifelhaften Anfragen:** Grundsätzlich immer die Identität und Berechtigung des Anfragenden sicherstellen. Im Zweifelsfall Kolleginnen und Kollegen oder den Praxisinhaber bei der Klärung einbeziehen.
- **Nicht überreden lassen:** Gerade, wenn der Anfragende nicht lockerlässt und versucht, mit Praxiskenntnissen und durch Überredung an die gesuchten Informationen zu gelangen, sollten Praxen sich nicht unter Druck setzen lassen. In diesem Fall geht Sicherheit vor Freundlichkeit.
- **Besondere Vorsicht bei E-Mails von unbekannten Absendern:** Im Zweifelsfall gar nicht auf die E-Mail reagieren oder, falls möglich, durch einen Telefonanruf bei einer bereits zuvor bekannten Rufnummer des vermeintlichen Absenders nachfragen.

- **Schulungen zur IT-Sicherheit:** Für die IT-Sicherheit sind alle Mitarbeitenden verantwortlich. Das gesamte Praxispersonal sollte deshalb regelmäßig für Sicherheitsfragen sensibilisiert werden. Alle Mitarbeitenden sollten regelmäßig zu Informationssicherheitsthemen geschult werden.
- **IT-Dienstleister beaufsichtigen:** Grundsätzlich dürfen IT-Dienstleister nicht unbeaufsichtigt an IT-Systemen arbeiten, wenn potentiell die Möglichkeit besteht, dass dabei Patientendaten eingesehen werden können. Passworteingaben sollten immer durch das Praxispersonal erfolgen.

Gut zu wissen

Grundsätzlich können sich Zahnarztpraxen darauf verlassen, dass die ePA erst dann bundesweit ausgerollt wird, wenn die Umsetzung entsprechender Maßnahmen in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgt ist. Das hat das Bundesministerium für Gesundheit (BMG) zugesichert.