Ergebnis der Steuerungsgruppe* zur Untersuchung einer möglichen Schwachstelle bei eHealth-BCS-Kartenterminals

Ausgangslage und Hintergrund

Im Rahmen von regelmäßigen Qualitätssicherungsmaßnahmen zur Einführung der elektronischen Gesundheitskarte wurde durch die gematik eine mögliche Schwachstelle bei eHealth-BCS-Kartenterminals festgestellt. Die Ursache der Schwachstelle ist darin begründet, dass die Kartenterminals zwei unterschiedliche Eingabeschnittstellen aufweisen:

- eine gesicherte Eingabeschnittstelle für die Eingabe von PINs
  --> der hierbei verwendete „sichere Eingabemodus“ stellt sicher, dass die PIN das Kartenterminal nicht verlässt
- eine ungesicherte Eingabeschnittstelle für beliebige, sicherheitsunkritische Dialoge
  --> über diese Schnittstelle könnte ein Angreifer missbräuchlich zu einer PIN-Eingabe auffordern.

Die Verwendung des sicheren Eingabemodus und das Verhalten der Kartenterminals sind in den Bedienungsanleitungen der jeweiligen Hersteller – wie vom BSI gefordert – beschrieben. Die Kartenterminals selber verdeutlichen über eine Signalisierung, dass sie sich im sicheren Eingabemodus befinden. Dies geschieht beispielsweise durch LED-Anzeigen oder Schlosssymbole im Display. Im sicheren Eingabemodus kann eine PIN eingegeben werden, ohne dass diese das Kartenterminal verlässt. Eine Manipulation des sicheren Eingabemodus, zum Beispiel durch Schadsoftware, ist nicht möglich.

Über die ungesicherte Eingabeschnittstelle kann eine Nutzsoftware eine Eingabeaufforderung generieren, damit die Eingabedaten an diese Software übergeben werden. Die ungesicherte Eingabeschnittstelle wurde nach einem allgemeinen Standard für Kartenterminals umgesetzt, findet aber nach derzeitigen Erkenntnissen im Gesundheitswesen keine Verwendung.

Die ungesicherte Eingabeschnittstelle könnte durch eine Schadsoftware zu einer missbräuchlichen PIN-Abfrage genutzt werden – sog. „Phishing-Angriff“. Ein solcher Angriff ist für den Anwender dadurch erkennbar, dass er zur Eingabe beliebiger Daten, u. a. auch PINs, über das Kartenterminal aufgefordert wird, obwohl der sichere Eingabemodus nicht angezeigt wird.

Der derzeitige Einsatz der eHealth-BCS-Kartenterminals im Basis-Rollout – also im Zusammenhang mit der elektronischen Gesundheitskarte (eGK) – verlangt weder die Eingabe einer PIN noch die Eingabe von sonstigen Daten zur Anwendungssteuerung.

Unabhängig davon können die Kartenterminals in den Leistungserbringerumgebungen auch im Zusammenhang mit elektronischen Heilberufsausweisen verwendet werden, z. B. für die Authentisierung an Abrechnungsportalen oder für die Erstellung von qualifizierten elektronischen Signaturen. Die dafür jeweils notwendigen PIN-Eingaben erfolgen im sicheren Eingabemodus, der über das Kartenterminal signalisiert wird. Solange der sichere Eingabemodus nicht signalisiert wird, darf keine PIN eingegeben werden. Andernfalls könnte diese PIN von einer Schadsoftware „gephisht" werden.

Bewertung und Maßnahmen

Unter Beachtung des sicheren Eingabemodus des Kartenterminals ist ein PIN-Phishing ausgeschlossen. Die Leistungserbringer müssen für den sicheren Umgang mit den Kartenterminals sensibilisiert werden.

Um zusätzlich auszuschließen, dass bei Fehlbedienung ein Phishing-Angriff erfolgen kann, wird eine Vorgabe für die Kartenterminalhersteller entwickelt, die die Grundlage künftiger Zulassungen darstellt. Diese Vorgabe wird die Eingabemöglichkeit über die ungesicherte Eingabeschnittstelle künftig auch technisch unterbinden.

Für die Hersteller hat das zur Konsequenz, dass in künftigen Versionen der Kartenterminals diese Vorgabe als Zulassungsgrundlage zu berücksichtigen ist. Bestehende Zulassungen bleiben jedoch erhalten. Für bereits im Feld befindliche Kartenterminals wird die Vorgabe mit dem nächsten Update umgesetzt.

Dies bedeutet, dass aktuell angebotene Kartenterminals im Rahmen des Basis-Rollout weiterhin angeschafft werden können.

* Die Steuerungsgruppe wurde von der 33. Gesellschafterversammlung am 26.05.2011 eingesetzt. Ihr gehören Vertreter/innen der Gesellschafter, des BMG, des BSI und der gematik an.

- - - - - -

23. Juni 2011

Quelle: http://www.gematik.de/cms/de/header_navigation/presse/informationsmaterial/informationsmaterial_1.jsp