Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Bundesministerium für Gesundheit
Herrn Dittmar Padeken
Rochusstraße 1
53123 Bonn

Bernd Kowalski

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-5700
FAX +49 (0) 228 99 9582-5700

Bernd. Kowalski@bsi.bund.de
https://www.bsi.bund.de

Betreff: Stellungnahme zum veröffentlichten PIN-Angriff mit Kartenterminals des Basis Rollout der elektronischen Gesundheitskarte

Bezug:
Aktenzeichen:
Datum: 30. Mai 2011

Anlage: -

Sehr geehrter Herr Padeken,

zu dem in verschiedenen Medien und Stellungnahmen beschriebenen PIN-Angriff nimmt das BSI wie folgt Stellung:

Für die für den Basis-Rollout vorgesehene Verarbeitung der auf der elektronischen Gesundheitskarte gespeicherten Versichertendaten durch die Kartenterminals (eHealth-BCS-Terminals) bestehen nach aktueller Kenntnis keine Sicherheitsrisiken. Die Eingabe einer PIN ist in der Basis-Anwendung nicht vorgesehen.

Wenn ein für den Basis-Rollout zugelassenes Kartenterminal für qualifizierte elektronische Signaturen genutzt wird, gelten gemäß SiG/SigV besondere Anforderungen an die Einsatzumgebung. Die Anwendung QES hat in einem „geschützten Bereich" zu erfolgen. Das heißt das Primärsystem ist durch geeignete Maßnahmen schad-SW-frei zu halten. Es besteht dann ein Restrisiko, wenn infolge fehlender Schutzmaßnahmen eine Schadsoftware auf dem Primärsystem des Leistungserbringers installiert wurde. Dieses sich ergebende Restrisiko kann bereits heute

Bundesamt
für Sicherheit in der
Informationstechnik

vermieden werden, wenn bei den für eine qualifizierte Signatur zugelassenen Geräten (BCS-KT mit QES) die entsprechenden Anzeigen der Geräte beachtet werden, dass sich das Gerät in einem sicheren PIN-Eingabe-Modus befindet.

Über mögliche andere Anwendungen, die mit einem zugelassenen BCS-KT mit QES durchgeführt werden können, sind aufgrund SiG/SigV immer auch die Anforderungen der BNetzA zu beachten. Zur Sicherheit dieser Anwendungen selbst kann das BSI keine Aussagen machen. Einige Geräte besitzen z. B. zusätzlich Bezahlfunktionen, die eine PIN-Eingabe erfordern.

Das BSI begrüßt, dass die Organisationen der Selbstverwaltung eine Steuerungsgruppe zur Erarbeitung von Handlungsvorschlägen zum Ausschluss des o. g. Restrisikos gegründet hat und wird diese Steuerungsgruppe mit seiner Expertise - ggf. unter Einbeziehung der BNetzA – selbstverständlich unterstützen.

Mit freundlichen Grüßen
Im Auftrag

Bernd Kowalski