Bundesversicherungsamt

Bundesversicherungsamt, Friedrich-Ebert-Allee 38, 53113 Bonn

An alle
bundesunmittelbaren
gesetzlichen Krankenkassen
- nur per E-Mail -

HAUSANSCHRIFT
Friedrich-Ebert-Allee 38
53113 Bonn

TEL +49 228 619 1948
FAX +49 228 619 1872

Thorsten.Schlotter@bvamt.bund.de
www.bundesversicherungsamt.de

BEARBEITER(IN) SCHLOTTER

11. April 2016

AZ **116 - 820 - 981/2015**
(bei Antwort bitte angeben)

nachrichtlich per E-Mail:

Bundesministerium für Gesundheit

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

GKV-Spitzenverband

Zugangs- und Zugriffsschutz bei digitalen Anwendungen – Erneuter Identitätsdiebstahl bei den Krankenkassen

Sehr geehrte Damen und Herren,

immer mehr Anwendungen und digitale Dienste werden in das Internet bzw. auf mobile Applikationen verlagert. Dadurch verändert sich auch die allgemeine Gefährdungssituation, insbesondere was den Schutz von Sozial- und Gesundheitsdaten anbelangt. Dies erfordert

gut aufeinander abgestimmte Sicherheitsmaßnahmen, die aus der Gesamtperspektive der jeweiligen Digitalisierungsstrategie analysiert werden müssen.

Vor diesem Hintergrund hatten wir Sie mit Rundschreiben vom 05. September 2014 (vgl. http://www.bundesversicherungsamt.de/aufsicht/datenschutzdatensicherheit.html, letzter Zugriff: 06.04.2016) darauf hingewiesen, dass wir eine Überarbeitung der Sicherheitskonzepte für notwendig halten, die diesen neuen Gefahren auch Rechnung trägt. Wir hatten darauf hingewiesen, dass wir für besonders schutzbedürftige Daten (z. B. Gesundheitsdaten) die herkömmlichen Authentisierungssysteme, bestehend aus Benutzername und Kennwort, für nicht sicher genug halten und hatten in Analogie zu § 36a Abs. 2 SGB I auf einen sicheren Identitätsnachweis mittels elektronischem Personalausweis bzw. elektronischer Gesundheitskarte hingewiesen (sog. Zwei-Faktor-Authentisierung).

Wie aus Presseberichten zu erfahren war (vgl. u. a. Rheinische Post vom 12. März 2016), ist es aber einer Testperson erneut gelungen, sich Zugang zu Gesundheitsdaten eines Redakteurs zu verschaffen. Das Angriffsmuster (u. a. Adressänderung im Callcenter) war mit dem, das auch schon dem ersten Pressebericht in dieser Sache zugrunde lag, identisch. Dies nehmen wir zum Anlass, nochmals auf die Sensibilität des Identitätsdiebstahls und Identitätsmissbrauchs hinzuweisen. Eine sichere elektronische Identität bildet die Grundlage in das Vertrauen digitaler Prozesse.

Insoweit ist ein feinabgestimmtes Maßnahmenbündel von organisatorischen und technischen Maßnahmen zu treffen, das in Abhängigkeit der konkreten Schutzanforderungen ein angemessenes Sicherheitsniveau bieten kann (vgl. § 78a SGB X einschließlich Anlage in Verbindung mit den BSI-Sicherheitsstandards und dem IT-Grundschutzkatalog). Die Sicherheitsanalyse kann nur individuell durchgeführt werden. Vor dem Hintergrund des vorliegenden Identitätsdiebstahls weisen wir insbesondere auf Folgendes hin:

- Die Sicherheitsanalyse ist ganzheitlich auszurichten, d. h. bei den Sicherheitsabwägungen müssen die Ursache-Wirkungs-Beziehungen über die konkreten Anwendungsgrenzen hinaus bedacht werden (z. B. alle Auswirkungen, die mit einer Adressänderung verbunden sein können).

- Vor dem Hintergrund des Spannungsfeldes – einerseits werden immer komplexere und hoch integrierte digitale Lösungen eingesetzt, die ein in allen Bereichen sicheres Identitätsmanagement erfordern, andererseits müssen diese Techniken benutzerfreundlich

und nach Möglichkeit verbreitet sein – sind flexible und anwendungsspezifische Authentifizierungslösungen hilfreich, um verschiedene Schutzniveaus abdecken.

- Ein Hauptaugenmerk ist dabei auf einen sicheren, elektronischen Identitätsnachweis zu legen und zwar sowohl bei der erstmaligen Einrichtung eines digitalen Zugangs (Registrierung) als auch bei den jeweiligen Anmeldungen am System (Authentisierung). Zum Stichwort „elektronischer Identitätsnachweis" verweisen wir auch auf das Gesetz zur Förderung der elektronischen Verwaltung (sog. E-Government-Gesetz) sowie den dazu vom Bundesministerium des Inneren veröffentlichten Minikommentar (vgl. http://www.bmi.bund.de/ DE/Themen/IT-Netzpolitik/E-Government/E-Government-Gesetz/e-government-gesetz_node.html, letzter Zugriff: 06.04.2016).

- Im E-Government-Gesetz wird auf eine sog. Zwei-Faktor-Authentisierung verwiesen (Besitz=elektronische Gesundheitskarte bzw. elektronischer Ausweis, Wissen=PIN bzw. Zugangsdaten). Grundsätzlich sind auch andere sichere Lösungen durch Kombination der Faktoren Wissen, Besitz und Biometrie denkbar. Allerdings sollte dabei berücksichtigt werden, dass beide Faktoren zwingend aus verschiedenen Kategorien stammen und so kombiniert werden, dass diese nicht unabhängig voneinander angegriffen werden können (d. h. beide Faktoren sollten miteinander verknüpft sein). In der Literatur wird aktuell eingeschätzt, dass eine starke Authentisierung immer einen besitzbasierten Faktor einschließen sollte (vgl. hierzu ausführlich J. Bender/D. Kügler: Was ist starke Authentisierung? In: DuD – Datenschutz und Datensicherheit, Heft 4/2016, S. 212-216).

- Bei der Sicherheitskonzeption sind der Faktor Mensch und das sog. Social Engineering besonders zu berücksichtigen. Organisatorische Sicherheitsmaßnahmen müssen in klaren Regeln formuliert zum Ausdruck gebracht werden (z. B. in Dienstanweisungen). Eine Missachtung sollte zudem konsequent sanktioniert werden.

Das Bundesversicherungsamt wird vor dem Hintergrund der wiederholten Sicherheitsvorfälle zukünftig stichprobenmäßig prüfen, ob anwendungsspezifische Sicherheitskonzepte für digitale Lösungen erstellt wurden, ob deren Einhaltung (insbesondere der organisatorischen Regeln) durch die verantwortliche Stelle selbst überwacht wird und ob etwaige Verstöße entsprechend sanktioniert wurden.

Wir weisen in diesem Zusammenhang noch einmal deutlich auf die Informationspflichten bei unrechtmäßiger Kenntniserlangung von Sozialdaten gemäß § 83a SGB X hin und im Fall der

Auftragsdatenverarbeitung auf die besondere Prüfpflicht des § 80 Abs. 2 Satz 4 SGB X sowie auf den korrespondierenden Bußgeldtatbestand im § 85 Abs. 1 Nr. 1b SGB X.

Mit freundlichen Grüßen
Im Auftrag

(Heinz-Peter van Doorn)