BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Frau
[redacted]
[redacted] Karlsruhe

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-[redacted]
E-MAIL Referat24@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 17.03.2023
GESCHÄFTSZ. 24-191 II#5163

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Datenschutz in der Telekommunikation**

Sehr geehrte Frau [redacted],

In Ihrer Akte ist kein weiterer Schriftverkehr mit der Telekom gespeichert. Ich habe entsprechend Ihrem Hilfsantrag die vollständige Akte als Kopie beigefügt und betrachte damit Ihren Antrag nach Art. 15 Abs. 1 DSGVO als erfüllt.

Im Sinne einer transparenten und serviceorientierten Bearbeitung übersende ich zudem die Anlage 5 aus dem Jour Fixe Telekommunikation vom 3. März 2022, aus der sich die wesentlichen Grundsätze der Validierung von E-Mails ergeben.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 302

Beglaubi[redacted]

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Validierung von E-Mail-Adressen

- Jour fixe Telekommunikation, 3. März 2022

- Dipl.-Ing. BfDI, Ref. 24

Warum Validieren?

- Problemfeld

- Neukunden erhalten Informationen per E-Mail, ohne dass die Korrektheit der E-Mail-Adresse geprüft wurde. Bei der Erfassung einer E-Mail-Adresse können jedoch Fehler gemacht werden.

- Die E-Mail-Adressen von Altkunden sind oft nicht überprüft worden. Wenn es einen Anlass gibt, einem Kunden eine E-Mail zu übersenden, könnte ein Dritter die E-Mail erhalten.

- Die Übermittlung personenbezogener Daten an Dritte durch fehlerhafte E-Mail-Adressen soll verhindert werden.

Was sollte bei der Validierung verhindert werden?

- Risiken

- Eine fehlerhaft erfasste E-Mail-Adresse wird erfolgreich validiert.

- Ein unberechtigter Dritter kann seine eigene E-Mail-Adresse erfolgreich validieren lassen, eventuell mit Kenntnis einiger Daten des Kunden.

- Der Validierungsprozess ist so gestaltet, dass sich Kunden an eine unsichere Eingabe von Daten oder Passwörtern in verlinkte Webseiten gewöhnen und damit Angriffe durch Phishing-Mails begünstigt werden.

BfDI

Wie soll die Validierung durchgeführt werden?

- Umsetzung

- 1. Schritt: Nennung/Eingabe der E-Mail-Adresse durch Kunden nach Authentifikation (z.B. Neukunde bei Vertragsabschluss, Kunde im Online-Kundencenter, verifizierter Kunde bei Hotline,..) -> E-Mail-Adresse ist entweder korrekt oder fehlerhaft, nicht aber manipuliert.
- 2. Schritt: Versenden einer Test-Mail an die E-Mail-Adresse mit einem Geheimnis.
- 3. Schritt: Eingabe oder Nennung des übermittelten Geheimnisses im Online-Kundencenter, Gespräch mit Kundenhotline (nach Authentifikation) o.ä.

oder

- 2. Schritt: Versenden einer Test-Mail an die E-Mail-Adresse mit einem speziellen Link zu einem Internetformular zur Eingabe eines Geheimnisses.
- 3. Schritt: Eingabe des Geheimnisses, das von der Kundenhotline (nach Authentifikation) genannt wurde, per Brief oder SMS übermittelt wurde, im Online-Kundencenter angezeigt wird o.ä. in das verlinkte Internetformular.

BfDI

Wie soll die Validierung durchgeführt werden?

- Umsetzung (Fortsetzung)

- Es ist darauf zu achten, dass
  - bei einem fehlerhaften Versand ein Dritter keine Bestätigung erteilen kann,
  - im 3. Schritt keine Manipulation möglich ist,
  - die Gültigkeit von Links oder TANs möglichst kurz gewählt wird,
  - ein Link zur Verifikation der zu prüfenden E-Mail-Adresse eindeutig zuzuordnen ist,
  - keine sensiblen Daten in einem Link abgefragt werden und
  - der Vorgang für den Kunden transparent ist.

Wie soll die Validierung nicht umgesetzt werden?

- Verfahren, die nicht empfohlen werden.

- Ein direkter Link in einer E-Mail in das Online-Kundencenter:
  - Link könnte auch gefälscht sein (Phishing). Kunden sollen sich nicht daran gewöhnen, einen Link aus einer E-Mail anzuklicken und dann Benutzernamen und Passwort einzugeben.
- Eine Übernahme einer nicht verifizierten, aber in der Vergangenheit genutzten E-Mail-Adresse:
  - Es würde eine umfangreiche manuelle Analyse erfordern, um zu prüfen, ob diese sicher dem Kunden zugeordnet werden kann. Eine ausreichende Prüfung mit automatisierten Regeln erscheint nicht praktikabel.

Was kann nicht erreicht werden?

- Die Grenzen des Verfahrens

- E-Mails werden im günstigsten Fall mit einer Transport-Verschlüsselung gesichert. Für besonders sensible Informationen wäre eine Ende-zu-Ende Verschlüsselung erforderlich.[1]
- Die Absende-Adresse einer E-Mail kann gefälscht werden.
- Ein Kunde kann seine E-Mail-Adresse wechseln, ohne darüber zu informieren.
- E-Mail-Accounts könnten auch mehreren Personen zugänglich sein (Urlaubsvertretung, Familie).

[1] Siehe: Orientierungshilfe der DSK „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail"

BfDI

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0

poststelle@bfdi.bund.de
www.bfdi.bund.de