Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zwei-Faktor-Authentisierung

Bewertungstabellen: IT-Sicherheit

Nutzungsumgebung:

- Verwendung von sicheren Passwörtern
- Einsatz der 2-Faktor-Authentisierung unter Verwendung zweier unterschiedlicher Geräte
- Benutzung vertrauenswürdiger Quellen für Software oder Apps

Legende für Bewertung:

Grün = gut
Gelb = mittel
Rot = schlecht
Grau = nicht relevant

Resilienz gegen Phishing (nicht in Echtzeit)

Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Das heißt: die abgefangenen Anmeldeinformationen werden vom Angreifer nicht unmittelbar an das Zielsystem weitergeleitet.

Verfahren	Erläuterung	Bewertung
E-Mail	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Der 2. Faktor verliert seine Gültigkeit nach einer vorgegebenen Zeit (z. B. 10 min).	Gut
SMS-TAN[1]	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Der 2. Faktor verliert seine Gültigkeit nach einer vorgegebenen Zeit (z. B. 10 min).	Gut
softwarebasierte Verfahren, teilweise mit Hardwarebindung: PushTAN Apps	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Der 2. Faktor verliert seine Gültigkeit nach einer vorgegebenen Zeit (z. B. 10 min). **ABER:** In einigen Fällen (Bestätigungsbutton statt TAN) könnten Verbraucher zu einem späteren Zeitpunkt leicht zu Bestätigungen unabhängig vom Anmeldeprozess verleitet werden.	Mittel
softwarebasierte Verfahren, teilweise mit Hardwarebindung: TOTP Apps	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Es können keine einzelnen Transaktions-TANs gewinnbringend gestohlen werden. **ABER:** Allerdings kann, mit erhöhtem Schwierigkeitsgrad, der Nutzer u. U. dazu verleitet werden, sein TOTP Geheimnis preiszugeben (abhängig von konkreter App und mit Auswirkungen auf weitere Bewertungskriterien).	Mittel
hardwarebasierte Verfahren: Fido2[2]	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Das Verfahren ist an Domäne gebunden.	Gut
hardwarebasierte Verfahren: ChipTAN	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: Die TAN ist nur auf bestimmte Transaktionen/Prozesse bezogen.	Gut
hardwarebasiertes Verfahren: Personalausweis[3]	Der 2. Faktor schützt vor Phishing-Angriffen, die nicht in Echtzeit erfolgen. Begründung: - Daten nur abrufbar, wenn Nutzer den Anwender bestätigt - komplette Verschlüsselung zwischen eID und eID-Server (Diensteanbieter) - gegenseitige Authentisierung zwischen eID und eID-Server - Zertifikat für den eID-Server nur durch das BVA Security by Design und Security by Default; Transport-PIN verpflichtet den Nutzer eine eigene Pin zu setzen.	Gut

Tabelle 1: Resilienz gegen Phishing-Angriffe, die nicht in Echtzeit erfolgen.

[1] Annahme: physische SIM-Karte

[2] Bewertet wurde der Einsatz (Verfahren) und die Hardware eines typischen in DE erhältlichen Fido2 Tokens in der aktuellsten Version; Sicherheitslevel 3 spielt in dieser Betrachtung auf Grund fehlender Verbraucherrelevanz keine Rolle. Davon abzugrenzen sind softwarebasierte Fido2-Umsetzungen unter den gängigen Betriebssystemen (Microsoft Windows, Android, iOS). Diese wurden in der vorliegenden Gegenüberstellung nicht betrachtet, nicht alle Aussagen sind 1:1 übertragbar.

[3] Nutzung über Ausweis-App auf einem mobilen Endgerät mit NFC-Schnittstelle

Resilienz gegen Real-Time-Phishing

Der 2. Faktor schützt vor Phishing-Angriffen, die in Echtzeit erfolgen. Schutz heißt hier: die abgefangenen Anmeldeinformationen werden vom Angreifer unmittelbar an das Zielsystem weitergeleitet, führen aber nicht zu einer erfolgreichen Authentisierung des Angreifers am Zielsystem.

Der Verbraucher wird durch transparente Informationen zu der Transaktion befähigt, Angriffe zu erkennen.

Verfahren	**Erläuterung**	**Bewer-tung**
E-Mail	Der 2. Faktor schützt nicht vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: Der über E-Mail zugestellte 2. Faktor kann bei einem Phishing-Angriff durch einen Realtime-Proxy des Angreifers gesendet werden. (Die E-Mail-Zustellung erfolgt in der Regel nicht Ende-zu-Ende verschlüsselt.) Prüfung der Informationen zur Transaktion möglich, da Informationen mitgeliefert werden können, die der Verbraucher prüfen kann.	Schlecht
SMS-TAN	Der 2. Faktor schützt nicht vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: Der über SMS zugestellte 2. Faktor kann bei einem Phishing-Angriff durch einen Realtime-Proxy des Angreifers gesendet werden. Abhängig von der Umsetzung des Verfahrens ist eine Prüfung der Informationen zur Transaktion möglich, da Informationen mitgeliefert werden können, die der Verbraucher prüfen kann. Wird aber nur der Code übermittelt, ist eine Information zur Authentisierung schwieriger prüfbar. Weiterhin sind verschiedene Angriffe bekannt, die ein Ausspähen der übermittelten SMS ermöglichen: - Bei einer Angriffsvariante wird dem heimischen Netz der Aufenthalt des Endgeräts in einem ausländischen Partnernetz suggeriert - mit dem Effekt, dass die SMS in das Fremdnetz zugestellt werden. - Der Transport von SMS ist einem starken Wettbewerb ausgesetzt. Aufgrund von Schwächen im Übertragungsprotokoll kann nicht ausgeschlossen werden, dass SMS auf dem Transportweg abgefischt werden. - Ein Täter kann sich Zugriff auf die Mailbox verschaffen. Anbieter unterstützten teilweise auch die Sprachübermittlung von Codes anstelle der Übermittlung einer textuellen SMS.	Schlecht
softwarebasierte Verfahren, teilweise mit Hardwarebindung: PushTAN Apps	Der 2. Faktor schützt begrenzt vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: Prüfung der Informationen zur Transaktion je nach Implementierung möglich, da Informationen mitgeliefert werden können, die der Verbraucher prüfen kann. **ABER**: Die Sicherheit ist nicht zertifiziert und prüfbar, da in der Regel proprietäre Lösungen zum Einsatz kommen.	Mittel
softwarebasierte Verfahren, teilweise mit Hardwarebindung: TOTP Apps	Der 2. Faktor schützt nicht vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: MitM-Angriffe sind möglich. In der Regel besteht kein Schutz des Nutzers, der MitM Angriffe erkennbar macht.	Schlecht
hardwarebasierte Verfahren: Fido2	Der 2. Faktor schützt vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: Das Verfahren ist resistent gegen Real-Time-Phishing-Angriffe, sofern der Standard korrekt implementiert wurde. (Besondere Sicherheitsrelevanz hat hierbei die Verwendung des Token Binding.)	Gut

Verfahren	Erläuterung	Bewer-tung
hardwarebasierte Verfahren: ChipTAN	Der 2. Faktor schützt vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: Die TAN ist nur auf bestimmte Transaktionen/Prozesse bezogen. Bei der Nutzung von Flicker Codes müssen Verbraucher auf dem Display die Transaktionsinformationen überprüfen. Anmerkung: Sammelüberweisungen sind nicht betrachtet worden.	Gut
hardwarebasiertes Verfahren: Personalausweis	Der 2. Faktor schützt vor Phishing-Angriffen, die in Echtzeit erfolgen. Begründung: - Daten nur abrufbar, wenn Nutzer den Anwender bestätigt - komplette Verschlüsselung zwischen eID und eID-Server (Diensteanbieter) - gegenseitige Authentisierung zwischen eID und eID-Server - Zertifikat für den eID-Server nur durch das BVA Security by Design und Security by Default; Transport-PIN verpflichtet den Nutzer eine eigene Pin zu setzen.	Gut

Tabelle 2: Resilienz gegen Phishing-Angriffe, die in Echtzeit erfolgen.

Resilienz gegen Angriffe aus der Ferne auf den 2. Faktor

Zur Bewertung werden Angriffsmöglichkeiten aus der Ferne auf den 2. Faktor herangezogen.

Verfahren	Erläuterung	Bewer-tung
E-Mail	Denkbare Angriffsszenarien aus der Ferne: - Angriff auf Software(-lieferkette), z. B. des Mail-Servers möglich Es ist nicht sichergestellt, dass - E-Mail-Adressen lebenslang der gleichen Person zugeordnet bleiben ("Use-after-free" Problematik). So kann ein Angreifer freigewordene E-Mail-Adressen neu registrieren und sich Zugriff auf mit dieser E-Mail in der Vergangenheit gekoppelte Dienste verschaffen. - Passwörter für den Zugriff auf E-Mail-Konten sind häufig auf vielen Endgeräten gespeichert, es besteht ein Risiko, dass Angreifer sich Zugriff auf E-Mail-Postfächer verschaffen können. **Angriffsfläche:** Leak der Anmeldedaten aus dem E-Mail-Account möglich oder Abgreifen der Anmeldeinformationen über Phishing-Angriffe auf das E-Mailkonto.	Mittel
SMS-TAN	Denkbare Angriffsszenarien aus der Ferne: - Lieferkettenangriff durch SIM-Swapping möglich - Es ist nicht sichergestellt, dass Telefonnummern lebenslang der gleichen Person zugeordnet bleiben ("Use-after-free" Problematik). Telefonnummern werden nach kurzer Sperrzeit erneut vergeben. Angreifer erhalten so ggf. Zugriff auf mit der Telefonnummer in der Vergangenheit gekoppelte Dienste, z. B. via "Wunschrufnummer". - Auf den Mobilfunkgeräten werden die SMS als Benachrichtigung dargestellt. Hier können maliziöse Drittapps ansetzen und die Inhalte der SMS ausspähen. **SIM-Swapping:** Tätern gelingt es hierbei, aufgrund von schlechten Authentifizierungsverfahren von TK-Anbietern eine Ersatz-SIM für eine Opfertelefonnummer zu erlangen.	Mittel
softwarebasierte Verfahren, teilweise mit Hardwarebindung: PushTAN Apps	Denkbare Angriffsszenarien aus der Ferne: - Angriff auf Software(-lieferkette) möglich - Angriff des Gerätes mit der PushTan App - Angriff auf den Account mit anderem Login Verfahren	Mittel
softwarebasierte Verfahren, teilweise mit Hardwarebindung: TOTP Apps	Denkbare Angriffsszenarien aus der Ferne: - Angriff auf Software(-lieferkette) möglich, aber schwierig unentdeckt durchzuführen - Angriff des Gerätes mit der TOTP App - Angriff auf das Backup	Mittel

Verfahren	Erläuterung	Bewer-tung
hardwarebasierte Verfahren: Fido2	Denkbare Angriffsszenarien aus der Ferne: - Lieferkettenangriff z. B. auf den Microcontroller möglich, sofern nicht vom Hersteller bezogen - Wenn auf dem Token kein vertrauenswürdiger "Sicherheitscontroller" verwendet wird, ist ein Angriff auf den Token über eine Schnittstelle (USB durch Kompromittierung des Rechners, Bluetooth, NFC) möglich. - Angriff auf das Gerät, an dem der FIDO2-Token genutzt wird (bspw. Watering Hole Angriff, Speer Phishing).	Mittel
hardwarebasierte Verfahren: ChipTAN	Denkbare Angriffsszenarien aus der Ferne: - durch organisatorische Maßnahmen gegen Lieferkettenangriffe resistent - Angriffe aus der Ferne sind nicht möglich.	Gut
hardwarebasiertes Verfahren: Personalausweis	Denkbare Angriffsszenarien aus der Ferne: - gegen Lieferkettenangriffe geschützt - Da 2. Faktor auf dem Chip lokal verifiziert, ist ein Angriff aus der Ferne nicht möglich.	Gut

Tabelle 3: Resilienz gegen Angriffe aus der Ferne auf den 2. Faktor

Resilienz gegen "Leaks des Dienstes"

Existiert ein Leak der Anmeldeinformationen beim Dienst, kann ein weiterer Angreifer, der nicht den Leak herbeigeführt hat, sondern nur die Leak-Daten erlangt, mit den Informationen keine Authentisierung mit dem 2. Faktor an diesem Dienst durchführen

Verfahren	Erläuterung	Bewer-tung
E-Mail	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen. Annahme: Im Leak sind keine oder keine verwertbaren Informationen über die TAN-Erzeugung des 2FA-Verfahrens enthalten, da die TAN nicht von einem Secret abgeleitet, sondern mittels Zufallszahl erzeugt wird.	Gut
SMS-TAN	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen Annahme: Im Leak sind keine oder keine verwertbaren Informationen über die TAN-Erzeugung des 2FA-Verfahrens enthalten, da die TAN nicht von einem Secret abgeleitet, sondern mittels Zufallszahl erzeugt wird.	Gut
softwarebasierte Verfahren, teilweise mit Hardwarebindung: PushTAN Apps	**Implementierungsabhängig,** welche Secrets im Leak enthalten sein können, die es einem Angreifer ermöglicht sich eigene PushTans zu erzeugen oder die Angreifenden geben sich als PushTAN App aus (= PushTAN App zu impersonifizieren). Annahme: Unter den Anmeldeinfornationen befindet sich auch das Secret.	Schlecht
softwarebasierte Verfahren, teilweise mit Hardwarebindung: TOTP Apps	**TOTP bietet keinen Schutz** gegen Exfiltration des Shared Secrets beim Diensteanbieter. (Es ist SCHLECHTER als ein starkes, gesalted und gehasht gespeichertes Passwort.)	Schlecht
hardwarebasierte Verfahren: Fido2	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen.	Gut
hardwarebasierte Verfahren: ChipTAN	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen.	Gut
hardwarebasiertes Verfahren: Personalausweis	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen.	Gut

Tabelle 4: Resilienz gegen Leaks des Dienstes

Resilienz gegen "Leaks von Diensten, die diesen Faktor auch verwenden"

Wird der 2. Faktor sowohl bei Dienst A als auch bei Dienst B verwendet und wird Dienst B kompromittiert, so dass es zu Leaks der Anmeldeinformationen von Dienst B kommt, haben die Informationen in diesem Leak keinen Mehrwert für einen Angreifer für den Einsatz des 2. Faktors bei Dienst A.

Verfahren	Erläuterung	Bewertung
E-Mail	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen. Annahme: Im Leak sind keine oder keine verwertbaren Informationen über die TAN-Erzeugung des 2FA-Verfahrens enthalten, da die TAN nicht von einem Secret abgeleitet, sondern mittels Zufallszahl erzeugt wird.	Gut
SMS-TAN	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen. Annahme: Im Leak sind keine oder keine verwertbaren Informationen über die TAN-Erzeugung des 2FA-Verfahrens enthalten, da die TAN nicht von einem Secret abgeleitet, sondern mittels Zufallszahl erzeugt wird.	Gut
softwarebasierte Verfahren, teilweise mit Hardwarebindung: PushTAN Apps	Nicht relevant, da die proprietären Apps i.d.R. einzigartig pro (Meta)Dienst sind. Abhängig davon, ob der Dienst mit anderen Diensten beim gleichen Hosting-Dienstleister angeboten/mit Push-TAN gesichert wird (bspw. IT-Dienstleister eines übergreifenden Sparkassenverbundes).	n. relevant
softwarebasierte Verfahren, teilweise mit Hardwarebindung: TOTP Apps	Abhängig davon, ob für jeden Dienst ein einzigartiges Shared Secret genutzt wird.	Mittel
hardwarebasierte Verfahren: Fido2	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen.	Gut
hardwarebasierte Verfahren: ChipTAN	Nicht relevant, da keine weiteren Dienste.	n. relevant
hardwarebasiertes Verfahren: Personalausweis	Angreifer kann auf Grundlage der Leak-Infos keine 2FA durchführen	Gut

Tabelle 5: Resilienz gegen "Leaks von Diensten, die diesen Faktor auch verwenden"