Landesamt für Sicherheit in der Informationstechnik

# Leitfaden des LSI

## Phishing-resistente Multifaktor-Authentifizierung

## DOKUMENTINFORMATIONEN

| | |
|---|---|
| **Version** | 1.1 |
| **Stand** | 07.06.2024 |
| **Herausgeber** | Landesamt für Sicherheit in der Informationstechnik (LSI), Keßlerstraße 1, 90489 Nürnberg |
| **Kontakt** | beratung@lsi.bayern.de |

# VORBEMERKUNG

Das Landesamt für Sicherheit in der Informationstechnik (LSI) ist die IT-Sicherheitsbehörde des Freistaats Bayern. Zu den Aufgaben des LSI gehört u.a. die Beratung der Staatsverwaltung, der Kommunen und öffentlicher Unternehmen als Betreiber kritischer Infrastrukturen in Fragen der IT-Sicherheit. Für diese Zielgruppen wurde der vorliegende Leitfaden konzipiert.

# MANAGEMENT SUMMARY

Kompromittierte Benutzerkonten sind häufig die Eintrittspforte für weitere, schwerwiegende Angriffe auf die IT-Systeme und Daten einer Organisation. Vor allem Systeme mit rein Passwort-basierten Authentifizierungsverfahren sind akut gefährdet durch vielfältige Arten von Phishing-Angriffen.

Schutz bietet eine Absicherung durch eine Multifaktor-Authentifizierung (MFA), bei der Authentifizierungselemente aus den drei Faktoren „Wissen“, „Besitz“ und „Biometrie“ sinnvoll miteinander kombiniert werden.

Jedoch ist nicht jede Form einer MFA gleichermaßen gut für einen beabsichtigten Einsatzzweck geeignet. Zudem existieren weit entwickelte Angriffsformen auf die MFA wie z.B. Echtzeit-Phishing, die eine gewisse Robustheit des MFA-Verfahrens erfordern.

Das LSI empfiehlt vorzugsweise Lösungen, die Standard-basiert, Hardware-basiert und (Echtzeit-)Phishing-resistent sind. Robuste Verfahren verhindern auf technischer Basis, dass überhaupt Zugangsdaten des Benutzers an eine falsche URL (Phishing-Seite) gesendet werden können. Falls aus organisatorischen oder technischen Gründen eine Phishing-resistente Umsetzung nicht möglich ist, gilt der Grundsatz:

**Eine** MFA ist besser als **keine** MFA.

Aktuell empfiehlt das LSI folgende Phishing-resistente Verfahren:

- Einsatz eines Hardware-basierten PKI-Benutzerzertifikats
- Einsatz einer Lösung nach dem FIDO2-Standard

# INHALTSVERZEICHNIS

# 1 Einleitung

## 1.1 Bedrohungslage und Notwendigkeit von sicheren Authentifizierungsverfahren

Die Anzahl aller erfassten Straftaten aus dem Bereich Cyberkriminalität steigt stetig an. Die Angriffe werden immer gezielter und professioneller. Sehr oft dienen **illegal erlangte Zugangsdaten** als Eintrittspforte in die Systeme der Opfer, um dort massive Schäden zu verursachen, beispielsweise durch

- Einschleusen von Schadsoftware, insbesondere Ransomware
- Abfluss und Veröffentlichung vertraulicher Informationen
- Sabotage von Betriebsabläufen
- Identitätsdiebstahl
- Ausbreitung und Kompromittierung weiterer Systeme und Benutzerkonten.

Zunehmende Relevanz gewinnen dabei kriminelle „Initial Access Broker“. Diese handeln in der „Underground Economy“ mit unrechtmäßig erlangten Zugängen, vielfach für Unternehmens- oder Behördennetzwerke [2].

Weitere Informationen zur aktuellen Bedrohungslage finden sich in [1-4].

Historisch gesehen bestanden digitale Identitäten üblicherweise nur aus einer Kombination von Benutzername und Passwort. Der Benutzername gibt die Identität des Benutzers an, die Kenntnis des zugehörigen Passworts bestätigt sie. Dieses einfache Authentifizierungsverfahren weist eine Vielzahl von Sicherheitsproblemen auf und ist aus sicherheitstechnischer Sicht heute in den meisten Anwendungsfällen nicht mehr ausreichend. Leider wird in der Praxis oft noch daran festgehalten, nicht zuletzt aus Gewohnheitsgründen oder wegen den anfallenden Umstellungsaufwänden.

Der Schutz von Benutzerzugängen durch sichere Authentifizierungsverfahren ist eine der zentralen Herausforderungen im Zuge der fortschreitenden Digitalisierung. Sichere Authentifizierungsverfahren müssen in der Lage sein, den jeweils aktuellen Angriffsformen standhalten zu können. Eine der wesentlichen Anforderungen an ein sicheres Authentifizierungsverfahren ist, dass die Sicherheit bereits maßgeblich durch die Architektur sichergestellt wird **(„Security by Design“)**. Das Authentifizierungsverfahren ermöglicht dadurch in hohem Maße Toleranz gegen menschliche und organisatorische Schwächen.

## 1.2 Arten von Phishing

Die momentan am weitesten verbreitete und damit gefährlichste Angriffsform gegen Authentifizierungsverfahren ist Phishing. Unter dem Begriff Phishing versteht man Versuche, über gefälschte Internetseiten, E-Mails oder andere Kommunikationswege eine legitime bzw. vertrauenswürdige Organisation oder Person zu imitieren. Ziel ist, das Opfer zur Preisgabe von sensiblen Informationen wie z.B. Zugangsdaten zu verleiten.

Der Kreativität der Angreifer sind dabei keine Grenzen gesetzt. Ihre Methoden werden inhaltlich und technisch immer raffinierter und entwickeln sich ständig weiter. Im Folgenden werden, beispielhaft und nicht abschließend, einige aktuelle Arten von Phishing kurz vorgestellt.

### E-Mail-Phishing (allgemein)

Die häufigste Form ist das allgemeine E-Mail-Phishing. Der Angreifer versendet große Mengen an E-Mails an eine breite Masse von Empfängern, in der Hoffnung, aufgrund der schieren Masse einige „Treffer“ zu erzielen.

Die E-Mails weisen oft irreführende oder gefälschte Absender auf (E-Mail-Spoofing). Die Absenderadresse einer E-Mail kann hierbei vom Angreifer beliebig gewählt werden, sofern das zum Versand verwendete E-Mail-System die Absenderadressen nicht einschränkt bzw. den Absender nicht korrekt authentifiziert.

Im Inhalt der E-Mail wird dem Empfänger ein legitimes und ggf. dringendes Anliegen vorgetäuscht oder er wird mit einem fiktiven Sachverhalt unter Handlungsdruck gesetzt. Die Kampagnen orientieren sich inhaltlich oft auch an aktuellen gesellschaftlichen oder politischen Ereignissen.

Ziel der E-Mail ist, den Benutzer auf eine gefälschte Internetseite zu leiten, um ihn dort dazu zu bringen, sensible Informationen wie seine Zugangsdaten einzugeben. Die Fälschung ist in der Regel dem erwarteten Original sehr ähnlich und für einen Nutzer nur schwer oder gar nicht als solche erkennbar. Technisch sind die Fälschungen oft ohne großen Aufwand zu erstellen. Sobald der Benutzer seine Zugangsdaten auf der gefälschten Internetseite eingegeben hat, befinden sich diese in den Händen des Angreifers.

### Spear-Phishing

Diese Art des E-Mail-Phishings zielt nicht auf die breite Masse, sondern einen ausgewählten Empfänger oder Empfängerkreis ab. Der Inhalt der E-Mail wird oft durch vorherige Angriffe wie z.B. Social-Engineering oder sonstiges Ausspähen speziell auf das Opfer zugeschnitten. Weitere speziellere Varianten dieser Art sind:

- **Whaling**: Gezieltes Ansprechen einer hochrangigen Führungskraft einer Organisation mit vorher perfekt recherchiertem und plausiblem Inhalt
- **CEO-Fraud**: Gezieltes Ansprechen eines Mitarbeiters einer Organisation mit einer dringenden Handlungsanweisung von einer vermeintlich hochrangigen Führungskraft
- **Clone-Phishing**: Der Angreifer erstellt die Phishing-E-Mail auf Basis einer echten E-Mail, die das Opfer bereits bekommen hat, jedoch werden Links und Anhänge entsprechend ausgetauscht

### Phishing mit real existierenden E-Mail-Inhalten der Benutzer

Im Rahmen verschiedener Schadecode-Kampagnen wie beispielsweise „Emotet“ wurde beobachtet, dass auf infizierten Systemen sowohl Kontakte als auch komplette E-Mail-Verläufe aus dem E-Mail-Postfach des Opfers ausgelesen werden (sog. „Outlook-Harvesting“). Diese Informationen werden genutzt, um E-Mails zu generieren, die für den Empfänger wie eine Antwort auf eine tatsächlich von ihm verfasste E-Mail aussehen, aber in Wirklichkeit der Weiterverbreitung des Schadcodes dienen.

Zudem existiert die Schadcode-Familie der sog. „Information Stealer“, die speziell auf das Auslesen und Ausleiten von sensiblen Informationen wie Zugangsdaten oder E-Mail-Inhalte ausgerichtet ist.

Abgeflossene E-Mail-Inhalte durch Outlook-Harvesting oder Information Stealer können als Basis für äußerst authentisch wirkende und schwer zu erkennende Phishing-Kampagnen verwendet werden.

### Suchmaschinen-Phishing

Beim Suchmaschinen-Phishing versucht der Angreifer, eine gefälschte Internetseite durch SEO-Maßnahmen („Search Engine Optimization“) oder durch Werbeschaltungen auf eine möglichst hohe Position der Trefferliste für bestimmte Suchanfragen zu bekommen.

Ziel ist, das Opfer in den Glauben zu versetzen, beim Aufruf des Suchergebnisses direkt auf die Internetseite bzw. Anmeldeseite der gesuchten Institution zu gelangen. Die falsche URL hinter dem Link wird meist geschickt verschleiert.

### Smishing (SMS-Phishing)

Bei dieser Form bekommt der Benutzer eine SMS zugestellt, die zum Aufruf einer Phishing-URL auffordert. Dies geschieht oft im Kontext eines vermeintlich dringenden Ereignisses wie z.B. der Zustellung eines Paketes.

### Vishing (Voice-Phishing)

Der Angreifer gibt sich am Telefon als vertrauenswürdige Person aus (z.B. Mitarbeiter einer Behörde oder der IuK-Servicestelle) und versucht, das Opfer zur Preisgabe von sensiblen Daten wie Passwörtern oder TANs zu bewegen. Es wird oft das Überraschungsmoment ausgenutzt, emotionaler Druck aufgebaut und in geschickter Art und Weise ein äußerst dringender Handlungsbedarf suggeriert.

### Echtzeit-Phishing

Echtzeit-Phishing kommt vor allem dann zum Einsatz, wenn der Angreifer eine Zwei-Faktor-Authentifizierung überwinden muss. In diesem Fall genügen Benutzername und Passwort nicht für die Anmeldung. Der Dienst verlangt ein weiteres Merkmal (zweiter Faktor) wie z.B. ein dynamisch generiertes Einmalpasswort oder eine dem Benutzer vorab übermittelte TAN, die zeitlich und ggf. auch inhaltlich nur begrenzt gültig ist. Der Ablauf des Echtzeit-Phishings wird in Kapitel 3.2 näher beschrieben.

Alternativ kann Echtzeit-Phishing auch durch Voice-Phishing betrieben werden, indem der Angreifer während des Telefonats die entsprechenden Seiten aufruft und dazu die bereitgestellten Informationen des Opfers verwendet.

# 2 Überblick über Authentifizierungsverfahren und MFA

## 2.1 Allgemeines zur Multifaktor-Authentifizierung

Es gibt drei grundlegende Gruppen von Faktoren, deren Verfahren zur Authentifizierung herangezogen werden können:

- Faktor Wissen
- Faktor Besitz
- Faktor Biometrie

Bei einer Multifaktor-Authentifizierung muss der Benutzer **mindestens zwei** Authentifizierungsmerkmale vorweisen können, die **verschiedenen** Faktoren angehören. Durch eine **sinnvolle Kombination** können die Schwächen eines einzelnen Faktors kompensiert und in Summe ein deutlich höheres Sicherheitsniveau erzielt werden.

So kann zum Beispiel das Passwort (Faktor Wissen) um einen weiteren Faktor ergänzt werden, um sich gegen

- Passwortdiebstahl durch Ausspähen
- Passwortrateversuche mittels Brute-Force oder Wörterbuch

zu schützen. Phishing-Angriffe können je nach gewählter Kombination der Faktoren deutlich erschwert werden.

Die folgenden Abschnitte geben einen kurzen Überblick über die Authentifizierungsverfahren der drei Faktor-Gruppen.

## 2.2 Faktor Wissen

**Passwort**

Ein Passwort ist ein geteiltes Geheimnis zwischen Benutzer und Anbieter in Form einer Zeichenkette, das in der Regel in Verbindung mit einem Benutzernamen zur Authentifizierung verwendet wird.

Passwörter sind als eine der ältesten und schwächsten Formen der Authentifizierung mit folgenden Sicherheitsproblemen behaftet:

- Ein Passwort verleitet den Benutzer (oft aus Komfortbedürfnissen) zu einer leichtfertigen Handhabung wie z.B. der Verwendung von einfachen Passwörtern, Mehrfachbenutzung über verschiedene Anbieter hinweg, unsicheren Aufbewahrung, unachtsamen Eingabe, Teilen des Passworts mit weiteren Benutzern, etc.
- Ein Passwort ist insofern kein richtiges Geheimnis, als dass es naturgemäß auch dem Anbieter bekannt gegeben werden muss. So entsteht zusätzlich eine Gefahr durch unsachgemäße Handhabung bzw. Angriffen auf Anbieterseite.
- Ein Passwort muss bei allen Authentifizierungsvorgängen über ein potentiell unsicheres Medium übermittelt werden, was weitere Angriffsmöglichkeiten (Ausspähen) mit sich bringt.
- Ein Passwort kann durch Schadsoftware auf dem Endgerät (z.B. „Keylogger“ oder „Information Stealer“) aufgezeichnet und von Angreifern ausgelesen werden.
- Ein Passwort kann unbemerkt entwendet und durch Dritte verwendet werden.
- Ein Passwort ist anfällig für Brute-Force-Angriffe, sofern die nötigen Anforderungen an die Passwortkomplexität nicht eingehalten bzw. nicht eingefordert werden.

Die aktuell schwerwiegendste Bedrohung für Passwörter ist jedoch das Phishing.

Beim Einsatz von Passwörtern empfiehlt sich die Verwendung eines **Passwort-Managers**. Dieser unterstützt den Benutzer bei der individuellen Passwortvergabe und der sicheren Passwortverwahrung an zentraler Stelle. Weitere Hinweise zum richtigen Einsatz und zu den Vor- und Nachteilen von Passwort-Managern finden sich unter [5] und [6].

### PIN

Eine PIN („Personal Identification Number“) ist eine Spezialform des Passworts und kommt meist in einem lokalen bzw. gerätegebundenen Kontext zur Anwendung. Sie ist typischerweise kürzer und weniger komplex als ein Passwort, damit sich der Benutzer die PIN ohne weitere Hilfsmittel merken kann. In der Regel wird die PIN-Eingabe nach einer streng limitierten Anzahl von Fehlversuchen gesperrt.

Für sich alleine betrachtet ist die PIN ein sehr schwaches Authentifizierungsmerkmal. Sie wird deshalb niemals alleinstehend eingesetzt, sondern dient dem Schutz eines weiteren Faktors, z.B. dem Besitz einer Chipkarte oder eines Endgeräts, welches an die PIN gebunden ist.

### Sicherheitsfrage

Sicherheitsfragen werden manchmal als zusätzliches Wissensmerkmal verwendet, um Zugangsdaten wie z.B. Passwörter wiederherzustellen, falls diese vergessen oder gesperrt wurden. Die Verwendung birgt ähnliche Sicherheitsprobleme wie die des Passworts. Zudem kann ein Angreifer die Antworten auf gängige, triviale Sicherheitsfragen unter Umständen sehr leicht recherchieren. Das Verfahren wird daher nicht empfohlen.

### Wiederherstellungscode

Auch Wiederherstellungscodes werden verwendet, um Zugangsdaten wiederherzustellen. Im Unterschied zu Sicherheitsfragen und Passwörtern sind diese nicht frei wählbar, sondern werden vom Anbieter generiert und dem Benutzer mitgeteilt. Die Übermittlung und Aufbewahrung bietet einige Angriffsmöglichkeiten. Zudem besteht auch hier ein Phishing-Risiko. Es ist zu beachten, dass Verfahren zur Wiederherstellung von Benutzerzugängen insgesamt nicht schwächer sein dürfen als das Verfahren zur initialen Einrichtung des Zugangs.

## 2.3 Faktor Besitz

Dieser Faktor bezieht sich auf den Besitz eines kryptographischen Geheimnisses, welches zur Authentifizierung mittels kryptographischer Protokolle genutzt wird. Dieses Geheimnis ist entweder in einer **dedizierten Hardwarekomponente**, welche auch als **(Security-)Token** bezeichnet wird, oder in einer **Softwarekomponente** gespeichert.

Zur Authentifizierung muss der Besitz nachgewiesen werden. Dies geschieht durch die entsprechende Verwendung des Tokens während des Authentifizierungsvorgangs. Dazu können unterschiedliche Geräteformen und Verfahren zum Einsatz kommen.

Im Folgenden werden einige zugrunde liegende Verfahren und die in Frage kommenden Geräte und Softwarelösungen vorgestellt.

### Einmalpasswörter (OTP- / TAN-basierte Verfahren)

Sowohl beim OTP (One Time Passwort) als auch bei der TAN (Transaktionsnummer) handelt es sich um **Einmalpasswörter**, die nur für genau einen einzigen Authentifizierungsvorgang verwendet werden können. Es sind drei grundlegende Varianten zu unterscheiden:

- **Variante 1**: Das Einmalpasswort wird vom Benutzer generiert.
- **Variante 2**: Der Anbieter übermittelt dem Benutzer eine transaktionsabhängige Information, mit der der Benutzer ein gültiges Einmalpasswort generieren kann.
- **Variante 3**: Das Einmalpasswort wird vom Anbieter generiert und dem Benutzer auf einem „zweiten Kanal“ übermittelt.

Bei **Variante 1** muss vorab ein geheimer symmetrischer Schlüssel zwischen Benutzer und Anbieter ausgetauscht werden. Mittels diesen Schlüssels und eines entsprechenden Verfahrens (z.B. TOTP oder vergleichbaren proprietären Standards) berechnen sowohl Benutzer als auch Anbieter das Einmalpasswort. Das vom Benutzer berechnete Einmalpasswort wird übermittelt und während der Authentifizierung auf Übereinstimmung geprüft.

Beispiele für in Frage kommende Komponenten:

- Hardwarekomponente: Dedizierte Tokens (ohne Verbindung zum Client-Gerät)
- Softwarekomponente: Smartphone / Tablet mit einer entsprechenden App nach dem im RFC 6238 beschriebenen Standard [9]

Bei **Variante 2** wird dem Benutzer in der Applikation z.B. ein sog. Flicker-Code oder ein QR-Code angezeigt, der durch den TAN-Generator oder das Handy vom Bildschirm abgescannt werden. Mittels dieser individuellen, transaktionsabhängigen Information wird das Einmalpasswort berechnet, dem Benutzer angezeigt und von diesem über eine Eingabemaske zurück an den Anbieter übermittelt.

Beispiele für in Frage kommende Komponenten:

- Hardwarekomponente: Dedizierte TAN-Generatoren, ggf. mit einer entsprechenden Chipkarte, integriertem Chipkartenleser, Zifferntastatur oder optischem Sensor
- Softwarekomponente: Smartphone / Tablet mit einer entsprechenden, meist proprietären App

Beim Einsatz einer Softwarekomponente / App der **Variante 2** wird in einigen Fällen auf die Anzeige des Einmalpassworts und dessen manuelle Rückübermittlung durch den Benutzer verzichtet. Die Apps haben in der Regel eine direkte Verbindung zum Anbieter und erledigen die Rückmeldung der entsprechenden Information nach der Bestätigung durch den Benutzer automatisch (z.B. Authega-App oder diverse Banking-Apps).

Bei **Variante 3** wird das Einmalpasswort ausschließlich vom Anbieter erzeugt, dem Benutzer auf einem zweiten Kanal übermittelt und über eine Eingabemaske der ursprünglichen Anwendung wieder abgefragt. Der Zugang zum Kanal gilt als Nachweis des Merkmals „Besitz“.

Die klassischen Kanäle dieses Verfahrens waren SMS und E-Mail, welche jedoch beide aus sicherheitstechnischen Gründen nicht mehr empfohlen werden.

Alternativ ist die Verwendung von Apps auf dem Smartphone möglich (z.B. PushTAN-Apps wie im Online-Banking). Diese verfügen in der Regel über eine sichere Verbindung zum Anbieter und sind deswegen der Übermittlung durch SMS oder E-Mail vorzuziehen.

Beispiele für in Frage kommende Komponenten:

- Hardwarekomponente: SMS (Besitz der SIM-Karte)
- Softwarekomponente: Smartphone / Tablet mit einer entsprechenden PushTAN-App (vorwiegend proprietäre Verfahren)

**Generelle Empfehlungen für OTP- und TAN-Verfahren:**

- Die Verwendung von Hardwarekomponenten ist grundsätzlich der Nutzung von Softwarekomponenten aus sicherheitstechnischer Sicht vorzuziehen und wird deshalb vom LSI ausdrücklich empfohlen. Dies liegt daran, dass bei Softwarekomponenten grundsätzlich weniger bis kaum Schutzmaßnahmen gegen das Kopieren oder Extrahieren der kryptographischen Geheimnisse vorhanden sind.
- Bei Anmeldungen von mobilen Endgeräten aus ist entscheidend, dass Anmeldung und zweiter Faktor nicht auf dem gleichen Endgerät stattfinden, da es sonst keinen echten zweiten Faktor gibt. Dieser Umstand ist je nach konkretem Anwendungsfall und dem verlangtem Schutzniveau individuell zu beurteilen.
- Der Benutzer sollte am Gerät bzw. in der App Informationen zum Inhalt der Transaktion mitgeteilt bekommen, für die das Einmalpasswort eingesetzt wird, z.B. die genaue Bezeichnung der Aktion, den Zeitpunkt der Ausführung, die IP-Location des zugreifenden Geräts, etc.
- Die Erzeugung bzw. Anzeige von Einmalpasswörtern am entsprechenden Gerät bzw. in der App sollte durch mindestens ein weiteres Authentifizierungsmerkmal abgesichert werden, z.B. PIN-Eingabe, Chipkarte, Fingerabdruck, etc.
- Je kürzer die zeitliche Gültigkeit von OTPs/TANs, desto besser.
- Je granularer die transaktionsbezogene Gültigkeit, desto besser.
- Bei entsprechendem Schutzbedarf sollte nicht nur die Anmeldung mit einem Einmalpasswort abgesichert werden, sondern alle zu schützenden Transaktionen.

Bei der Auswahl des Verfahrens sollte darauf geachtet werden, sog. **MFA-Fatigue-Angriffe** zu erschweren. Dabei ist der Angreifer bereits im Besitz des ersten Faktors (z.B. Passwort) und fordert durch wiederholte und automatisierte Anmeldeversuche eine Vielzahl von MFA-Authentifizierungsanfragen beim Opfer an, bis dieses aus „Ermüdung“ letztendlich eine der Anfragen bestätigt. Gefährdet sind v.a. Verfahren, bei denen der Benutzer nur eine MFA-Push-Notification bekommt, die er am selben Gerät einfach bestätigen muss.

## Zertifikatsbasierte Verfahren

Bei der zertifikatsbasierten Authentifizierung handelt es sich um ein asymmetrisches Verfahren, da es mit einem Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel arbeitet (Public-Key Verfahren). Der private Schlüssel verbleibt stets beim Benutzer und wird niemals dem Anbieter oder sonstigen Dritten übermittelt. Der öffentliche Schlüssel hingegen wird an alle Stellen verteilt, mit denen eine Authentifizierung stattfinden soll.

Die Verteilung geschieht typischerweise in Form eines Zertifikats, in dem der öffentliche Schlüssel an die Identität des Benutzers gekoppelt wird. Dies wird in der Regel durch eine vertrauenswürdige Zertifizierungsstelle beglaubigt. Dafür ist eine **PKI (Publik Key Infrastructure)** notwendig, welche die Zertifikate ausstellt und verwaltet.

Der Zugriff auf den privaten Schlüssel sollte immer mit einem weiteren Faktor, z.B. einer PIN-Abfrage, abgesichert werden.

Nur wenn der private Schlüssel auf **externer kryptographischer Hardware** gespeichert ist, z.B. auf einer Smartcard oder einem entsprechenden USB-Token, ist dies sicherheitstechnisch eine wesentliche Verbesserung. Sollte das technisch nicht möglich sein, kann im Einzelfall alternativ eine geräteinterne Speicherung auf einem TPM-Chip oder in einem dedizierten Zertifikatsspeicher geprüft werden. Sowohl bei der Verwendung von externer kryptographischer Hardware als auch bei den erwähnten Alternativen muss stets sichergestellt sein, dass private Schlüssel entweder direkt dort erzeugt oder auf sicherem Wege dorthin importiert werden können (technischer Transportschutz und organisatorische Maßnahmen). Zudem darf privates Schlüsselmaterial, einmal im Speicher abgelegt, nicht mehr exportiert werden können.

**Die Verwendung von rein softwarebasierten Zertifikaten mit beliebigem Speicherort auf dem Endgerät wird nicht empfohlen**, da diese grundsätzlich kopiert bzw. unbemerkt entwendet werden können und der PIN-Schutz entfernt werden kann.

Beispiele für in Frage kommende Geräte:

- Smartcard (je nach Anwendung können bestimmte Sicherheitsklassen für Smartcard-Lesegeräte gefordert werden)
- USB Krypto-Stick

## FIDO2

FIDO2 (Fast Identity Online) ist ein standardisiertes Verfahren, das ebenfalls nach dem Public-Key-Prinzip arbeitet. Die Besonderheit ist, dass hier nicht nur ein Schlüsselpaar zur Authentifizierung eingesetzt, sondern für jeden Dienst ein eigenes Schlüsselpaar generiert wird. **Dabei werden die Schlüssel unzertrennlich an die URL des Dienstes gebunden, mit dem die Authentifizierung stattfinden soll.** Die versehentliche Übermittlung von Zugangsdaten an eine gefälschte Internetseite mit einer anderen URL wird somit technisch ausgeschlossen. Die privaten Schlüssel werden ausschließlich auf einem gesicherten Gerät, dem sog. FIDO2-Authenticator, generiert, gespeichert und verarbeitet. Sie können diesen technisch nicht verlassen.

Vor der Verwendung ist eine Registrierung bei dem jeweiligen Dienst erforderlich, wobei der Dienst den öffentlichen Schlüssel des Benutzers bei sich hinterlegt. Bei der Authentifizierung schickt der Dienst eine Anfrage („Challenge“) an den Benutzer, welche dieser mit seinem privaten Schlüssel signiert („Response“). Das Senden der Signatur muss vom Benutzer aktiv bestätigt werden, z.B. über einen Berührungssensor

oder durch die Eingabe einer PIN. So wird verhindert, dass beispielsweise Schadcode auf dem Rechner unbemerkt vom Benutzer Authentifizierungsvorgänge ausführt. Der Dienst verifiziert schließlich die Signatur mit dem bei ihm hinterlegten öffentlichen Schlüssel.

Technisch gesehen besteht FIDO2 aus zwei Hauptkomponenten:

- Die **WebAuthn-API** ist ein offizieller Web-Standard, der von allen modernen Browsern angeboten wird. Die Methoden dieser Browser-API werden durch ein clientseitiges JavaScript der Webanwendung aufgerufen. Dadurch kann die Webanwendung dem Benutzer eine FIDO2-Authentifizierung über den Browser anbieten.
- Das **CTAP-Protokoll** (Client to Authenticator Protocol) kümmert sich um die Kommunikation zwischen dem Browser und dem verwendeten FIDO2-Authenticator.

Beispiele für in Frage kommende Geräte als FIDO2-Authenticator:

- FIDO2 USB-Key (diverse Hersteller)
- FIDO2 NFC-Key (diverse Hersteller)
- FIDO2 Smart Card (diverse Hersteller)

**FIDO2-Erweiterung: Passkeys - Das Endgerät als Schlüsselspeicher**

Bei Passkeys handelt es sich um eine Erweiterung des FIDO2-Standards, der im Jahr 2022 von den Herstellern Apple, Google und Microsoft vorgestellt wurde. Ziel der Erweiterung ist es, die Notwendigkeit des separaten Authenticators für eine FIDO2-basierte Authentifizierung zu eliminieren. Passkeys verwenden stattdessen das jeweilige Endgerät als Schlüsselspeicher.

Zentraler Bestandteil des Passkeys-Verfahrens ist aktuell aber auch eine obligatorische Synchronisation der privaten Schlüssel mit der jeweiligen Hersteller-Cloud. Dies soll es dem Benutzer ermöglichen, die einmal eingerichteten Passkeys auf mehreren Endgeräten zu nutzen bzw. diese bei Verlust des Endgerätes einfach wiederherzustellen. Dabei hängt die Sicherheit von Passkeys von der Integrität des Endgeräts, dem Synchronisierungsverfahren zur Hersteller-Cloud, der Integrität des Herstellers und dessen Cloud ab.

## 2.4 Faktor Biometrie

Die Nutzung biometrischer Merkmale zur Authentifizierung wie Fingerabdruck oder Gesichtserkennung ist mittlerweile eine verbreitete Standardfunktion auf mobilen Endgeräten wie Smartphones und Tablets. Das Verfahren ist vergleichsweise benutzerfreundlich, da der Benutzer sich nichts merken und kein zusätzliches Gerät mit sich führen muss. Jedoch hängt die Zuverlässigkeit dieser Technologie stark von der Qualität der jeweiligen Implementierung auf den Endgeräten ab und kann deshalb an dieser Stelle nicht pauschal beurteilt werden. Zudem können biometrische Merkmale vom Benutzer unbemerkt kopiert und die Kopie unter Umständen zur Überwindung des Faktors verwendet werden (z.B. Entnahme eines Fingerabdrucks von einem berührten Gegenstand oder Entnahme des Retinaabdrucks von einem Bild).

Dennoch eignen sich die zur Verfügung stehenden, nicht-zertifizierten Verfahren in der Regel zumindest technisch als Ergänzung (dritter Faktor) bzw. als zusätzliche Absicherung eines Verfahrens mit dem Faktor „Besitz“. Vor der Verwendung von biometrischen Merkmalen der Benutzer sind ggf. datenschutz- und personalvertretungsrechtliche Belange zu klären.

# 3 Sicherheitstechnische Empfehlungen des LSI

## 3.1 Allgemeine Empfehlungen zum Einsatz einer MFA

Mittels einer sorgfältig konzipierten und umgesetzten MFA werden die Angriffsmöglichkeiten von Angreifern und Cyberkriminellen stark eingeschränkt und das Risiko für eine erfolgreiche Kompromittierung der Zugänge stark reduziert. Ziel ist, eine Phishing-Resistenz durch technische Lösungen herzustellen. Schulungen und Awareness-Kampagnen für die Benutzer sind sinnvoll, können aber lediglich unterstützend wirken. Die Sicherheit eines Authentifizierungsverfahrens darf nicht ausschließlich vom Benutzerverhalten abhängen.

Eine MFA wird grundsätzlich für alle Arten von Zugängen bzw. Benutzerkonten empfohlen. Insbesondere in folgenden Fällen ist der Einsatz aus sicherheitstechnischer Sicht dringend empfohlen:

- Absicherung von Zugängen, die aus dem öffentlichen Internet erreichbar sind
- Absicherung von Zugängen für hoch privilegierte Benutzerkonten

Die aktuell verfügbaren MFA-Verfahren unterscheiden sich sowohl in der technischen Umsetzung als auch nach den verbleibenden Restrisiken. Grundsätzlich gilt:

***Eine** MFA ist immer besser als **keine** MFA.*

Zur Auswahl eines MFA-Verfahrens, das zuverlässig gegen aktuelle Angriffsformen schützen soll, sollten folgende Eigenschaften berücksichtigt werden:

1. Standard-basiert
2. Hardware-basiert
3. (Echtzeit-)Phishing-resistent

**Standard-basiertes Verfahren**

Es existieren internationale Standards für MFA, die eine stetige Weiterentwicklung und gemeinsame Qualitätskontrolle der standardisierten Formate und Prozesse mit sich bringen. Die Verwendung von Standards ermöglicht eine effiziente und unabhängige sicherheitstechnische Bewertung und Einbindung in den Sicherheitsprozess einer Organisation. Bei Lösungen, die proprietäre Prozesse und/oder Formate nutzen, hängt die Sicherheit und deren Bewertung stets von der dauerhaften Kooperation und beständigen Weiterentwicklung der Hersteller/Lizenzgeber ab. Zudem sind standardisierte Verfahren langfristig kostengünstiger als proprietäre Lösungen.

**Hardware-basiertes Verfahren**

Eine MFA-Lösung ist Hardware-basiert, wenn sich der Besitz-Faktor auf einer dedizierten Hardware befindet, die gesonderte Sicherheitsgarantien mitbringt, z.B. durch spezielle kryptografisch gesicherte Komponenten. Alle kryptografischen Vorgänge laufen innerhalb eines gesicherten Bereichs ab. Unbefugtes Auslesen und Kopieren von privatem Schlüsselmaterial wird hardwareseitig verhindert. Ein Hardware-Token kann durch weitere Merkmale vor Missbrauch geschützt werden (z.B. Feststellung der Benutzerpräsenz durch PIN-Eingabe, Tastendruck oder Abfrage des Fingerabdrucks). Zusätzlich ist bei einer Hardware-basierten MFA-Lösung nutzerseitig von einem erhöhtem Sicherheitsbewusstsein auszugehen, da die Nutzer

einen physischen „Schlüssel“ erhalten. Das Abhandenkommen eines solchen Schlüssels ist für den Nutzer direkt spürbar.

**Eine äquivalente Sicherheit durch rein softwarebasierte Lösungen ist nicht realisierbar.** Unter Abwägung aller Umstände und Rahmenbedingungen kann eine softwarebasierte Lösung umgesetzt werden, bevor gänzlich auf eine MFA verzichtet wird.

**(Echtzeit-)Phishing-Resistenz**

Bei modernen Phishing-Angriffen werden Nutzer mittels einer gefälschten Anmeldeseite dazu gebracht, freiwillig ihre Anmeldedaten inklusive des zweiten Faktors in die Hände des Angreifers zu geben. Phishing-resistente MFA-Lösungen verhindern dies durch ihre technische Umsetzung.

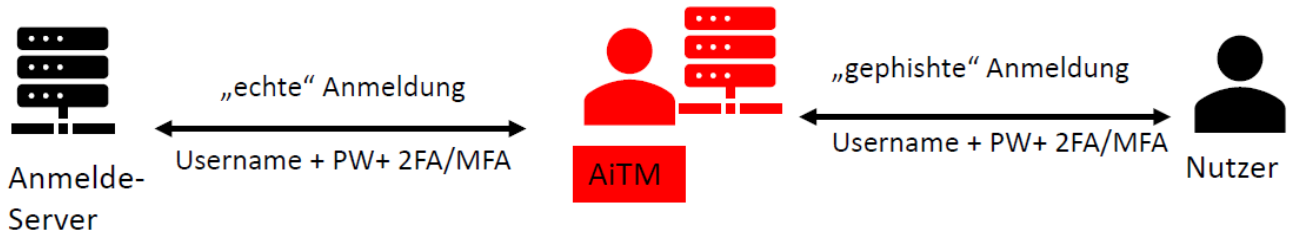
Die vorgestellten Varianten von Einmalpasswörtern (OTP-/TAN-basierte Verfahren) sind in der Regel nicht (Echtzeit-)Phishing-resistent und können deshalb nur bedingt empfohlen werden, z.B. nur wenn zwingende organisatorische oder technische Gründe gegen den Einsatz einer MFA-Lösung sprechen, die im folgenden Kapitel 3.2 empfohlen wird.

## 3.2 Empfehlung zum Einsatz einer Echtzeit-Phishing-resistenten MFA

Um eine Resistenz gegen Echtzeit-Phishing zu erzielen, wird aktuell eine Hardware-basierte Lösung mittels **PKI-Zertifikat oder dem FIDO2-Standard** empfohlen.

Um die Gefährdung zu verdeutlichen, wird die Vorgehensweise des Angreifers beim Echtzeit-Phishing am Beispiel eines „Adversary in The Middle“-Angriffs (AiTM) kurz aufgezeigt:

Beim AiTM läuft sämtlicher Authentifizierungsverkehr (unbemerkt vom Benutzer) über einen vom Angreifer kontrollierten „bösen Proxy“:




1. Der Angreifer sendet einen initialen Phishing-Link, z.B. per E-Mail.
2. Das Opfer ruft die Phishing-Seite auf.
3. Der Angreifer wird darüber von seinem Angriffstool in Kenntnis gesetzt, bzw. das Angriffstool ist in der Lage, den weiteren Angriff in Echtzeit automatisiert durchzuführen.
4. Im Hintergrund loggt sich der Angreifer mit dem abgegriffenen Passwort beim Dienst ein und triggert damit den MFA-Mechanismus.
    a. Im einfachsten Fall eines Einmalpassworts kann der Angreifer dieses einfach direkt abgreifen, in dem er dem Benutzer eine entsprechende Eingabemaske einblendet
    b. Falls die Anwendung erst eine transaktionsabhängige Information für den Benutzer generiert (z.B. einen QR-Code, den der Benutzer vom Bildschirm abscannt), muss der Angreifer etwas mehr Arbeit investieren. Da der Angreifer die tatsächliche Anmeldung initiiert hat, bekommt er den QR-Code angezeigt. Diesen muss er dem Benutzer weiterleiten. Sobald der Benutzer diesen weitergeleiteten QR-Code verarbeitet, ist der Angreifer aber auch in diesem Fall erfolgreich angemeldet.

Dieses Angriffsszenario kann nur mit einer per Design Phishing-resistenten MFA-Lösung verhindert werden. Dazu muss der vom Benutzer verwendete Browser technisch verifizieren können, dass das verwendete MFA-Verfahren zur korrekten URL des Dienstes gehört. Dies gelingt beispielsweise durch folgende Verfahren:

- **Zertifikat**: Die Verwendung eines Zertifikats ermöglicht durch mutual-TLS, dass sich nicht nur der Client beim Server, sondern auch der korrekte Server beim Client authentifiziert.
- **FIDO2**: Die Verwendung von FIDO2 über die WebAuthn-API des Browsers ermöglich eine Verifizierung des Servers, indem der FIDO2-Schlüssel für den authentisierenden Dienst an eine zuvor registrierte URL gebunden ist.

Hinweis zum Einsatz von **Passkeys**:

Das Authentifizierungsverfahren ist grundsätzlich sicherheitstechnisch gleich stark wie das FIDO2-Verfahren, da das gleiche Prinzip zugrunde liegt. Unterschiede gibt es aber im Umgang mit den privaten Schlüsseln.

Bei FIDO2 sind die privaten Schlüssel sowohl an den authentisierenden Dienst als auch an den physischen FIDO2-Authenticator des Benutzers gebunden, da diese ausschließlich auf dem FIDO2-Authenticator gespeichert sind. Bei den Passkeys hingegen fällt die Bindung an den Authenticator weg, da die Passkeys auf dem jeweiligen Endgerät gespeichert werden. Zudem ist es möglich, denselben Passkey mittels Synchronisation über die jeweilige Hersteller-Cloud auf mehreren Endgeräten zu benutzen.

Die Hersteller versprechen in der Regel, dass das private Schlüsselmaterial der Benutzer geschützt ist. Die Aussage ist jedoch schwer durch unabhängige Stellen zu beweisen und basiert deshalb maßgeblich auf dem Vertrauen zum Hersteller. Die Risiken, die durch die Synchronisation der privaten Schlüssel mit einer Public-Cloud entstehen, sind schwer einzuschätzen.

Der Einsatz von Passkeys erfordert deshalb eine sorgfältige Einzelbetrachtung des Anwendungsfalls.

## 3.3 Nötige Überlegungen zur Umsetzung einer MFA

**Überlegungen zum MFA-Anwendungsfall**

- Wie heterogen ist das technische und organisatorische Umfeld (z.B. verschiedenartige Endgeräte und Betriebssysteme, unterschiedliche interne und externe Benutzergruppen, …)? Welche Lösung eignet sich sicherheitstechnisch am besten, um damit umzugehen?
- Muss eine Verbindung zwischen Gerät und MFA-Token aufgebaut werden können? Welche Schnittstellen stehen dafür an den Endgeräten zur Verfügung?

**Überlegungen zum MFA-Prozess**

- Wie kann der Registrierungsprozess sicher und effizient gestaltet werden?
- Wie sieht der Prozess für Backup bzw. Recovery aus, falls ein Token verloren geht? Der Recovery-Prozess darf sicherheitstechnisch nicht schwächer sein als die Erstregistrierung.

**Überlegungen zum MFA-Risikomanagement**

- Echtzeit-Phishing (AiTM) kann aus heutiger Sicht nur durch bestimmte technische Verfahren (Hardware-Zertifikat oder FIDO2) ausgeschlossen werden. Bei allen anderen Verfahren verbleibt ein Risiko, welches bewertet und von den Projektverantwortlichen getragen werden muss.
- Grundsätzlich besteht bei allen bekannten MFA-Lösungen immer noch ein Restrisiko eines Lieferkettenangriffs bei der jeweils eingesetzten Hard- bzw. Software. Das Risiko besteht hierbei in

der Auslieferung manipulierter Geräte und/oder kompromittierter Programme. Die Absicherung gegen derartige Gefährdungen ist jedoch separat zu betrachten und nicht Teil dieses Leitfadens.

## 3.4 Die Grenzen der Sicherheit durch MFA

Selbst eine perfekte MFA-Lösung schützt nur den Prozess der initialen Authentifizierung. Sie schützt jedoch nicht gegen einen Diebstahl einer bereits authentifizierten Benutzersitzung (Session). Der Angriff erfolgt hier nach der Authentifizierung.

Falls die Anwendung beispielsweise Session-Cookies im Browser speichert, könnten diese von einem Schadcode ausgelesen und dem Angreifer übermittelt werden.

Lösungen für derartige Angriffe sind nicht in der MFA zu finden, sondern beispielsweise:

- in einer zuverlässigen Endpoint-Protection (z.B. zum Schutz vor Schadcode, der Session-Informationen auslesen kann)
- in einer robusten Software-Architektur (z.B. clientseitig nur kurzlebige Session-Identifikatoren speichern, um die Auswirkung einer einmaligen Kompromittierung zeitlich einzudämmen oder einer Bindung der Session-Identifikatoren an die IP-Adresse des Benutzers)

Für kritische Operationen kann auch eine erneute Abfrage der MFA helfen, sodass gestohlene Sessions einen geringeren Wert haben.

# 4 Quellen und weitere Informationen


[1] Bundesamt für Sicherheit in der Informationstechnik, „**Die Lage der IT-Sicherheit in Deutschland 2023**“, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html, abgerufen am 06.06.2024.

[2] Bundeskriminalamt, „**Cybercrime – Bundeslagebild 2023**“, URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html, abgerufen am 06.06.2024.

[3] Bayerisches Staatsministerium des Inneren, für Sport und Integration, Bayerisches Staatsministerium der Finanzen und für Heimat, **„Cybersicherheit in Bayern 2023 – Bericht zur Cybersicherheit in Bayern“**, URL: https://www.stmi.bayern.de/assets/stmi/sus/datensicherheit/bericht_cybersicherheit_bayern_2023.pdf, abgerufen am 06.06.2024.

[4] Bayerisches Landeskriminalamt, „**Cybercrime – Lagebild Bayern 2023**“, URL: https://www.polizei.bayern.de/mam/kriminalitaet/240503jahreslagebild_cybercrime_2023.pdf, abgerufen am 06.06.2024.

[5] Bundesamt für Sicherheit in der Informationstechnik, „**Passwörter verwalten mit dem Passwort-Manager**“, URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html, abgerufen am 06.06.2024.

[6] Bayerisches Staatsministerium für Digitales, „**Passwort- und Cybersicherheitstipps**“, URL: https://www.stmd.bayern.de/service/passwort-und-cybersicherheits-tipps/, abgerufen am 06.06.2024.

[7] Bundesamt für Sicherheit in der Informationstechnik, „**Zwei-Faktor-Authentisierung**“, URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html, abgerufen am 06.06.2024.

[8] Bundesamt für Sicherheit in der Informationstechnik, „**Technische Betrachtung: Wie sicher sind die verschiedenen Verfahren der 2-Faktor-Authentisierung (2FA)?**“, URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html, abgerufen am 06.06.2024.

[9] Internet Engineering Task Force (IETF), „**RFC 6238 TOTP: Time-Based One-Time Password Algorithm**“, URL: https://datatracker.ietf.org/doc/html/rfc6238, abgerufen am 06.06.2024.