Handlungsempfehlung sichere Authentifizierung

Stand 05.02.2020

1 Zielgruppen

Diese Handlungsempfehlung richtet sich an Nutzer, Verantwortliche und Dienstleister welche eine sichere Authentifizierung nutzen wollen.

Eine sichere Authentifizierung ist erforderlich um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern. Benutzer erhalten je nach eingesetztem Authentifizierungsverfahren eine oder mehrere Faktoren (Benutzerkennung, persönliches Passwort, Token, Pin-Nummer, EC-Karte…), um sich so gegenüber dem System als berechtigt ausweisen zu können. Dem authentifizierten Benutzer wird der Zugang zum System, zur Anwendung oder zu Teilen der Anwendung entsprechend den vergebenen Rechten eröffnet.

Dabei ist der Zugriff über Zugangskennung mit Passwort gegenüber höherwertigen Authentifizierungsmechanismen abzugrenzen, welche den Vorzug erhalten sollten. Mit den folgenden Hinweisen sollen Empfehlungen zur Gestaltung und Tipps zur Kontrolle einer datenschutzgerechten Authentifizierung gegeben werden.

Dabei haben die Nutzer informationstechnischer Systeme zunächst selbst ein großes Interesse daran, die eigenen Daten vor den neugierigen Augen unberechtigter Dritter zu bewahren. Darüber hinaus ist die mit den Faktoren verliehene eigene Identität ein hohes Gut; gerät sie in falsche Hände werden einem missbräuchlichen Zugriffe selbst zugerechnet.

Weiterhin gilt es insbesondere im beruflichen Umfeld, die zur Verarbeitung zugewiesenen Daten von Auftraggebern, Kunden und Bürgern zu schützen.

Für Verantwortliche gelten durch die DS-GVO unter anderem folgende Vorgaben:

- **Art. 5 DS-GVO**
  - Verpflichtung, angemessene Sicherheit der Verarbeitung zu gewährleisten;
  - Dokumentation für Nachweisbarkeit.

- **Art. 24 (1) DS-GVO**
  - Berücksichtigung von Rahmenbedingungen der Verarbeitung;
  - Verpflichtung zur risikobasierten Vorgehensweise;
  - Dokumentation für Nachweisbarkeit und Prüfbarkeit.

- **Art. 25 (1) DS-GVO**
  - angemessene Sicherungsmaßnahmen;
  - Berücksichtigung von Rahmenbedingungen der Verarbeitung;
  - Verpflichtung zur risikobasierten Vorgehensweise;
  - im Rahmen von Planung/Entwicklung und Betrieb.
- **Art. 32 (1) DS-GVO**
  - angemessene Sicherungsmaßnahmen;
  - Berücksichtigung von Rahmenbedingungen der Verarbeitung;
  - Verpflichtung zur risikobasierten Vorgehensweise;
  - Implementierung einer zyklischen und standardisierten Vorgehensweise.

Für Dienstleister, welche als Auftragsverarbeiter tätig werden, gelten unter anderem folgende Vorgaben der DS-GVO:

- **Art. 28 DS-GVO**
  - Verarbeitung von personenbezogenen Daten nur auf Weisung des Verantwortlichen;
  - ergreift gemäß Artikel 32 erforderliche Maßnahmen;
  - unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen von Betroffenen nachzukommen;
  - unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten;
  - Information des Auftragsverarbeiters an den Verantwortlichen, falls er der Auffassung ist, dass eine Weisung gegen Datenschutzbestimmungen verstößt.
  -

2 Unterschiedliche Authentifizierungsverfahren

2.1 Zugangskennung

Das klassische Authentifizierungsverfahren ist die Verwendung von Zugangsdaten. Diese sind geheim gehaltene Informationen, die aus einer Benutzerkennung und einem Kennwort/PIN bestehen. Dieses Paar nennt man Zugangskennung. Dieses Verfahren stützt sich rein auf die Verwendung von Wissensfaktoren.

2.1.1 Passwortgenerierung für Zugangskennungen

Die Kriterien für die Passwortstärke hängen von Passwortlänge und Zeichenvorrat ab. Hierbei gilt, dass die Passwortlänge, die Passwortstärke wesentlich mehr beeinflusst, als der verwendete Zeichenvorrat[1]. Auf kompliziert einzugebende Sonderzeichen und Umlaute kann daher verzichtet werden, zumal sich diese auch nicht unbedingt über jede

[1]Kallinna, Udo H.: „Passwortsicherheit I: Fakten, keine Mythen!“ https://www.dsin-blog.de/2012/03/28/passwortsicherheit-i-fakten-keine-mythen/

Tastatur eingeben lassen. Der Zeichenvorrat des Passwortes sollte sich daher aus Klein- und Großbuchstaben sowie Ziffern und Satzzeichen zusammensetzen.

Moderne Verschlüsselungsverfahren sind technisch so weit fortgeschritten, dass sie in der Praxis außer durch das Austesten aller möglichen Schlüssel – der sogenannten Brute-Force-Methode – meist nur durch einen Wörterbuchangriff geknackt werden können. Die Schwachstelle ist bei beiden Angriffen das vom Benutzer gewählte Passwort. Damit ein Passwort nicht unsicherer ist als die eigentliche Verschlüsselung (viele gängige Verfahren nutzen 128-Bit-Schlüssel), ist für dieses theoretisch eine Folge von etwa 20 zufälligen alphanumerischen Zeichen erforderlich. Falls das Passwort nicht aus gleichverteilt zufälligen Zeichen besteht, sind sogar deutlich längere Zeichenfolgen nötig, um die gleiche Sicherheit zu erreichen.

I 2017 veröffentlichte das National Institute of Standards and Technology (NIST) der USA neue Regeln für sichere Passwörter[2]. Den Autoren nach erzeugten viele der altbewährten Regeln - wie etwa Groß- und Kleinschreibung, Sonderzeichen, häufiges Wechseln der Passwörter -, die in den letzten Jahren als wichtige Empfehlung galten, nur wenig bis gar keine zusätzliche Sicherheit. Passwörter sollen künftig mindestens acht Zeichen lang sein, die Obergrenze sollte nicht unterhalb von 64 Zeichen liegen.

Im Grundschutz-Kompendium, Edition 2020 (01.02.2020), rät auch das Bundesamt für Sicherheit in der Informationstechnik (BSI)- nicht mehr zum regelmäßigen Passwort-Wechsel, sondern empfiehlt diesen nur noch, falls ein Passwort in fremde Hände geraten sein könnte[3]. Auch auf Vorgaben zu festen Regeln für Länge und Komplexität von Passwörtern wird hier nun verzichtet und stattdessen „ausreichend starke Passwörter“ gefordert.

2.2 Zwei-Faktor-Authentifizierung (2FA) und Multi-Faktor-Authentifizierung

Die 2FA ist eine Multi-Faktor-Authentifizierung (MFA) mit der minimal möglichen Anzahl unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Bei der MFA werden üblicherweise drei Kategorien von Faktoren unterschieden:

- Etwas, das nur der Nutzer kennt, wie z. B. Passwort, PIN oder TAN (Wissensfaktoren),
- etwas, das nur im Besitz des Nutzers ist, wie z. B. Smartphone, Smartcard, Token oder andere Hardware-Schlüssel (Besitzfaktoren), und

[2] *Das National Institute of Standards and Technology (NIST, deutsch: Nationales Institut für Standards und Technologie) hat als Bundesbehörde der Vereinigten Staaten von Amerika unter dem Titel „NIST Special Publication 800-63B - Digital Identity Guidelines Authentication and Lifecycle Management” vom Juni 2017 folgende Anforderung im Kapitel „5.1.1.2 Memorized Secret Verifiers“ veröffentlicht:„Verifiers shall require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers should permit subscriber-chosen memorized secrets at least 64 characters in length.“. Quelle:* https://pages.nist.gov/800-63-3/sp800-63b.html

[3] BSI Kompendium Edition 2020 vom 01.02.2020, Baustein ORP.4 Identitäts- und Berechtigungsmanagement, ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B), Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

- ein biometrisches Merkmal, das einzig und allein dem Nutzer zugeordnet werden kann und das untrennbar zu ihm gehört, wie z. B. der Scan des Fingerabdrucks oder der Retina (Biometriefaktoren).

Im Alltag kommt die 2FA zum Beispiel bei der Nutzung eines Geldautomaten zur Anwendung: Erst die Kombination aus Bankkarte und PIN ermöglicht die Transaktion.

Bei der Auswahl von Faktoren für eine 2FA sollte man im Sinne der Sicherheit jeweils Faktoren aus zwei unterschiedlichen Kategorien kombinieren. Nur so lässt sich ein Missbrauch befriedigend einschränken. So ist es bei der Wahl zweier Wissensfaktoren, wie z. B. PIN und TAN beim Onlinebanking, in der Vergangenheit mittels Social Engineering schon häufig zum Missbrauch gekommen.

Allerding bietet auch die 2FA bei der Nutzung von Faktoren aus unterschiedlichen Kategorien keinen absoluten Schutz, wenn z. B. eine technologische Schwachstelle beim Besitzfaktor zum Tragen kommt (Beispiel: Magnetstreifen bei der EC-Karte). Kriminelle sind in der Lage SIM-Karten zu klonen, um diese Authentifizierungsmethode zu überlisten. Ein Nachweiscode kann selbst während eines Telefonats abgefangen werden, wenn z. B. ein Mobilfunknetz kompromittiert ist[4] bzw. Kriminelle auf die Portierung von Telefonnummern oder auf andere Vorgehensweisen zurückgreifen, um Anrufe zu empfangen. Trotzdem bleibt hier der Aufwand zum Missbrauch immer noch höher als bei der Verwendung nur eines Faktors (nur Passwort).

Um die größtmögliche Sicherheit bei der Authentifizierung sicher zu stellen, benötigt man einen Wissensfaktor und einen Faktor, der wirklich den physischen Besitz eines Gegenstandes und eines äußerlichen Merkmals nachweist. Dieses Merkmal muss einzigartig sein und nur dem Nutzer zugeordnet werden können, wie z. B. der Scan eines Fingerabdrucks, um so eine starke Multi-Faktor-Authentifizierungsmethode zu bilden.

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt die Zwei-Faktor-Authentifikation sowohl in seinen Publikationen für Bürger[5], als auch in seinem IT-Grundschutz-Kompendium[6] und sie kann inzwischen als „Stand der Technik“ gelten. Die meisten großen Internet-Dienste wie Amazon, Facebook, Google, Apple, Microsoft, Dropbox oder Twitter bieten sie an. Die Website „twofactorauth.org“ zeigt, nach Kategorien geordnet, welche Dienste die Zwei-Wege-Bestätigung unterstützen.

[4]Schwachstelle im SS7-Netzwerk bei O2-Telefonica (03.05.2017): http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[5]https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/2FA-zwei-faktor-authentisierung.html

[6]https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html, ORP.4.A21 Mehr-Faktor-Authentisierung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

2.3 Weitere Maßnahmen zur Erhöhung der Passwortsicherheit

Unabhängig von der Passwortstärke muss, um eine höhere Sicherheit zu erreichen, zu einem Passwort ein gesalteter Hash gebildet werden und nur dieser darf auf der prüfenden Seite gespeichert werden. Das Klartextpasswort merkt sich der Nutzer idealerweise und speichert/notiert es nicht. Wird nun das Passwort verwendet, um Zugang zu einem System zu bekommen, wird zu dem eingegebenen Passwort der Salt hinzugefügt und wieder der Hash berechnet. Der Zugriff kann gewährt werden, wenn dieser Hash mit dem abgespeicherten Hash übereinstimmt. Der Hash wird nach einem definierten Verfahren so gebildet, dass aus der Kenntnis des Hashes das Passwort nicht in realistischer Zeit zurückberechnet werden kann und die Wahrscheinlichkeit, daß zwei unterschiedliche Kennworte den gleichen Hash erzeugen, sehr gering ist. Um zu verhindern, dass eine kompromittierte prüfende Seite alle anderen Kennworte ebenfalls kompromittiert, sollte jede Seite den Hash nicht nur aus dem Passwort selbst, sondern auch einem eigenen Schlüssel (Salt) bilden sowie um systematisches Probieren (Brute-Force-Methode) weiter zu unterbinden, rechenintensive Passwortableitfunktionen (Schlüsselstreckung)[7] verwenden.

Diese Maßnahmen müssen zwingend sowohl bei der reinen Passwortabfrage als auch bei der Zwei-Faktor-Authentifizierung zum Tragen kommen.

3 Vorbetrachtungen und Bedrohungsszenarien

Entscheidend für die Auswahl einer geeigneten Authentifizierung ist das Anwendungs-Szenario und die Betrachtung des darin enthaltenen Risikos:

- zur Anmeldung an einem lokalen System (z. B. im LAN),
- zur Nutzung externer Accounts (z. B. Mail oder Webseiten),
- zur Authentisierung (z. B. Betreten von Räumen, Nutzung von Geldausgabeautomaten),
- zum Zugriff auf einzelne Dokumente, ZIP-Archive o. ä.

Je nach Umgebung und Aufgabenstellung sind die Rahmenbedingungen für den Einsatz von Authentifizierungsverfahren recht unterschiedlich. Insofern erscheint es nur sinnvoll, die Anforderungen an das Authentifizierungsverfahren den jeweiligen Gegebenheiten anzupassen.

Bei der Verwendung von Zugangskennungen ist hierbei von ausschlaggebender Bedeutung, welche Schutzmaßnahmen gegen die missbräuchliche Verwendung eines Passwortes getroffen werden, insbesondere ob die Zahl der möglichen Fehleingaben wirkungsvoll beschränkt wird. Gerade dieser Faktor hat einen entscheidenden Einfluss auf die Angreifbarkeit des Systems. Wird eine Kennung nach 3-5 Fehleingaben für einen längeren Zeitraum oder ganz gesperrt oder gar ein zusätzliches Medium eingezogen, genügt ein kürzeres und weniger komplexes Passwort; kann ein Angreifer jedoch eine Vielzahl von Möglichkeiten ungestört durchprobieren (Brute-Force-Angriff),

[7] Schlüsselstreckung ist eine kryptographische Schlüsselableitungsoperation, die einen schwachen Schlüssel, üblicherweise ein Passwort, sicherer machen soll, indem sie dafür sorgt, dass zum Durchprobieren aller Möglichkeiten mehr Mittel (Zeit, Speicher) benötigt werden.

bietet nur eine erhöhte Passwortlänge bei größtmöglicher Zeichenvielfalt, oder besser noch die Verwendung einer Zwei-Faktor-Authentifizierung einen wirksamen Schutz.

3.1 Passwortwechsel

Wenn die Passwort-Strategie in einer Organisation an der Bedrohungslage und den möglichen Angriffsszenarien ausrichtet wird, gibt es wenige Anlässe, bei denen ein Passwort zu wechseln ist:

- Bei der Erstkonfiguration (Ändern des voreingestellten Passworts),
- wenn das Passwort ausgespäht oder weitergegeben wurde

3.2 Gesicherte Bereiche

In gesicherten Bereichen kann somit selbst ein Passwort, das lediglich acht Zeichen umfasst und aus Groß- und Kleinbuchstaben sowie Ziffern zusammengesetzt ist, einen hinreichenden Schutz sicherstellen. Allerdings muss gewährleistet sein, dass sich das Passwort nicht leicht erraten lässt. Keine Verwendung finden sollten daher exemplarisch Vornamen des Nutzers, seiner Familienangehörigen, Name des Hundes, Monatsbezeichnungen oder ähnlich offensichtliche Angaben.

3.3 Ungesicherte Bereiche

Ganz anders stellt sich die Situation in ungesicherten Bereichen dar, die einen Brute-Force-Angriff nicht wirksam ausschließen; hier kommt es darauf an, Passworte so komplex und lang zu gestalten, dass ein erfolgreiches Durchprobieren aller möglichen Kombinationen jeden sinnvollen Zeitrahmen sprengt.

Hier verwendete Passworte sollten daher mindestens 12 Stellen lang sein, den vollen Zeichenvorrat aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen nutzen und in Wörterbüchern der gängigsten Sprachen nicht vorkommen. Bei Erfüllung dieser Anforderungen entsteht allerdings häufig eine kryptische, sinnlose Zeichenfolge, die schwer zu merken ist (eine Hilfestellung zur Gestaltung längerer, komplexerer und auch merkfähiger Passworte finden Sie in Kapitel 5 Anhang: Hilfen für Nutzer). Die bessere Alternative stellt hier die Verwendung einer Zwei-Faktor- oder Mehr-Faktor-Authentifizierung da.

Unter Umständen kann ein Notieren durchaus sinnvoll sein; dabei darf die Notiz nur das Passwort ohne Kennung, Benutzer oder Verwendungszweck umfassen und muss an einem sicheren Ort unabhängig von den benutzten Geräten verwahrt werden.

3.4 Administrative Zwecke

Bei der Wahl von Passworten für Benutzerkonten mit erweiterten Rechten ist besonderer Wert auf eine hohe Qualität zu legen, da das Schadenspotential eines möglichen Missbrauchs deutlich höher ist. Darüber hinaus sind nicht personengebundene Administrationspasswörter stets zu notieren und in einem verschlossenen und ggf. zusätzlich versiegelten Umschlag in Tresoren oder Bankschließfächern sicher zu verwahren.

Bei sehr hohen Anforderungen an die Sicherheit sollte die Aufteilung des Passworts in zwei Teile erwogen werden, um einen berechtigten Zugang mit administrativen Rechten nur zwei Personen gemeinsam zu ermöglichen („Vier-Augen-Prinzip”); dann

jedoch ebenfalls in Verbindung mit 2FA; maßgeblich ist jedoch die Beurteilung der Bedrohungslage!]

3.5 Single Sign-on Lösungen (SSO)

Daneben sind in der Praxis zunehmend sog. Single Sign-on Lösungen anzutreffen, bei denen sich der Benutzer zu Beginn seiner Tätigkeit einmalig am System oder einem SSO-Dienstleister authentisiert und das System oder der SSO-Dienstleister die weiteren Anmeldungen des Benutzers an einer Vielzahl von Anwendungen intern selbstständig handhabt. Für derartige Verfahren ist aufgrund des unübersehbaren Gefahrenpotentials eine ausschließlich auf der Angabe einer Nutzerkennung und eines Passwortes aufbauende Authentisierung unzureichend. Hier müssen Zwei-Faktor- oder Mehr-Faktor-Authentifizierung die Identität eines berechtigten Nutzers sicherstellen.

4 Folgende Regeln beim Einsatz von Zugangskennungen sind stets zu beachten:

- **Erkannte Gefahren sofort bannen**

  Besteht der Verdacht, dass von einem Passwort unbefugt Kenntnis genommen wurde, ist es umgehend zu ändern.

- **Vorsicht bei der Eingabe**

  Die Passworteingabe sollte stets unbeobachtet erfolgen können. Insbesondere in Arbeitsbereichen mit Publikumsverkehr ist bereits bei der Aufstellung entsprechender Geräte hierauf Rücksicht zu nehmen.

- **Default-Einstellungen sofort ändern**

  Bei vielen Gelegenheiten wird von zentraler Stelle bzw. in einer lokalen Anwendung mit voreingestellten Passwörtern gearbeitet, die häufig auch noch bei den verschiedenen Anwendern identisch sind. So manches „Standardpasswort" lässt sich im Internet recherchieren.

  Sofern eine Neuvergabe bei der Erstanmeldung nicht erzwungen wird, sollte jeder Anwender schnellstmöglich selbst eine Änderung durchführen.

- **Für jeden spezifischen Zweck ein eigenes Passwort**

  Es sollte nicht überall ein und dasselbe Passwort genutzt werden. So eignet sich das Kennwort für die Anmeldung am Arbeitsplatz nicht für die Nutzung beim privaten Mail-Account oder für den Zugang zum Onlinespiel. Selbst innerhalb der unterschiedlichen Bereiche sollten für jede Anwendung verschiedene Passworte verwendet werden; dies begrenzt den Schaden für den Fall, dass ein Passwort ausgespäht oder geknackt werden konnte; der unberechtigte Zugang bleibt dabei auf eine spezielle Anwendung begrenzt.

- **Auch die Kennung kann ein Geheimnis darstellen**

  Solange die Kennung nicht aus auch in anderem Zusammenhang bekannten Begriffen besteht (z. B. E-Mail-Adresse; Vor- und Zuname; Organisationseinheit)

oder aus solchen abgeleitet werden kann, sollte sie genauso wie das Passwort geheim gehalten werden.

- **Sichere Freigabe einer gesperrten Zugangskennung**

  Nach mehrfacher Falscheingabe eines Passwortes wird die entsprechende Zugangskennung in der Regel gesperrt; ebenso wichtig ist es allerdings, dass Freigaben gesperrter Zugangskennungen nur im nur im Rahmen definierter Prozesse durch vertrauenswürdige Stellen veranlasst werden können. Auch kann der Prozess gestaffelt gestaltet werde: z. B. Sperrung für eine Minute nach drei Fehlversuchen, endgültige Sperrung nach drei weiteren Versuchen.

- **Passwortsammlungen nur in gesicherter Umgebung**

  Ist aufgrund der Menge der Kennungen und deren Komplexität ein Notieren von Passworten nötig, so ist besondere Sorgfalt bei der Aufbewahrung derartiger Sammlungen erforderlich. Eine denkbare Möglichkeit sind sog. Passwortsafes (auch Passwortmanagern): Softwaresicherheitstools, die die gesammelten Passwörter verschlüsselt abspeichern. Das zugehörige Master-Passwort sollte allerdings nicht in räumlicher Verbindung mit der Schlüsseldatei hinterlegt sein. Auch darf der Passwortsafe nur in gesicherten Umgebungen mit logischer, besser noch physischer Trennung von den Anwendungen, aufbewahrt werden, die Brute-Force Angriffe auf das Masterpasswort ausschließen.

- **Für Schicksalsschläge vorsorgen**

  Eine für den Notfall angelegte und sicher verwahrte Passwortliste und/oder die Aufnahme in das eigene Testament regelt auch beim Eintreten eines plötzlichen Todes- oder Pflegefalls das digitale Erbe.

5 Anhang: Hilfen für Nutzer

Um ein komplexeres Passwort zu generieren, das sich dennoch leicht merken lässt, kann man aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und Sonderzeichen einstreuen.

So entsteht z. B. aus:

„Eile mit Weile" = EimiWe!

oder aus

„Alle meine Entchen schwimmen auf dem See" = <AmEs@dS

Eine andere Methode ist, die Vokale in Worten systematisch durch andere Zeichen (Ziffern oder Sonderzeichen) zu ersetzen und nach Bedarf Sonderzeichen zu ergänzen.

So entsteht z.B. nach Auflösen der Umlaute (a=1, e=3, i=5, o=7, u=9) aus:

„Datenschutz" = D1t3n@sch9tz

„Polizeiauto" = P7l5z35#19t7

In diesem Beispiel ist es wichtig, Ausgangsworte zu wählen, die möglichst viele unterschiedliche Vokale aufweisen.

Absolut ungeeignet hingegen sind Trivialpasswörter wie Passwort, geheim, August11, 23Montag, Hans, Bello, Ulrike, etc. da sie zu einfach erraten werden können bzw. in entsprechenden Wörterbüchern zu finden sind und durch Tools für Brute-force-Attacken sekundenschnell enttarnt werden können.

Die Landesbeauftragte für den Datenschutz
Niedersachsen

Prinzenstraße 5 30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de

Stand: 05.02.2020