1. Hintergrund

Der (Zugriffs-) **Schutz** eines **SAP-Systems** hängt unter anderem auch von der Art und Weise der Systemanmeldung („Authentifizierung“) und von dem Umgang mit den zur Authentifizierung notwendigen, vergebenen und gespeicherten Passwörtern ab.

Die **Authentifizierung** eines SAP-Benutzers ist demzufolge ein wichtiges **Element** der **SAP-Informationssicherheit**. Durch geeignete Authentifizierungsverfahren wird sichergestellt, dass die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** der **Informationen** und **Informationsflüsse** ausreichend geschützt sind.

Mit zunehmender Verwendung „verteilter“ (SAP-) Systeme, die teilweise auf offenen Standards und flexiblem Informationsaustausch mit verschiedenen Geschäftspartnern basieren, wird das Einrichten von „Identitäten“ bzw. Benutzer für kommunizierende Partner oder Systeme ebenso zu einem weiteren wichtigen Element der Informationssicherheit.

Grundsätzlich bietet SAP eine Vielzahl von Authentifizierungsmechanismen mit unterschiedlichen Komplexitäts- und Sicherheitsgraden, mit deren Hilfe sich Benutzer an einem SAP-System anmelden können. So existieren beispielsweise für die folgenden vier „Zugriffskanäle“ die aufgeführten Authentifizierungsfunktionen:

- **SAP-GUI**
  - Interaktive Dialogauthentifizierung,
  - Transparente Zugriffsauthentifizierung mit Single Sign-On[1] (SSO-Server, Zertifikate).
  - Verschlüsselte Übertragung („DIAG“[2], „SNC“[3]).
- **Web-basierte Portaloberfläche** („Browser“)
  - Web-Browser („Client“ für Portal) und Application Server für Java
- **Web-Services**
  - HTTP[4]-Transportebene (Standard-HTTP-Authentifizierung),
  - SOAP[5]-Nachrichtenebene (Standard WS-Mechanismen).

---

[1] Single-Sign-On (kurz: SSO) wird auch als „Einmalanmeldung“ bezeichnet. Grundsätzlich bedeutet SSO, dass ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt (autorisiert) ist, am selben Arbeitsplatz zugreifen kann, ohne sich jedes Mal neu anmelden zu müssen. Somit reicht beispielsweise bei dem SSO-Verfahren die Authentifizierung an dem Arbeitsrechner aus, um die Anwendung SAP ohne weitere Authentifizierung nutzen zu können. Wird das SSO-Verfahren im Zusammenhang mit „Alt-Systemen“ (= niedriger Release-Stand) genutzt, bedingen die sicherheitstechnischen Möglichkeiten des „Alt-Systems“ das Schutz eines z.B. SAP-Systems.

[2] **D**ynamic **I**nformation and **A**ction **G**ateway (DIAG) ist ein proprietäres Protokoll der SAP AG, welches für die Kommunikation zwischen SAP GUI und dem Applikationsserver eines SAP-Systems eingesetzt wird. Außerdem verwendet der SAP Internet Transaction Server dieses Protokoll, um mit dem R/3-System zu kommunizieren. Dem proprietären Protokoll DIAG liegt intern das Remote Function Call (kurz: RFC) zu Grunde. Mit DIAG werden binäre Daten übertragen. Es handelt sich aber nicht um eine Verschlüsselung, sondern DIAG verwendet Verfahren zur Datenkompression. Die Nutzung bzw. Aktivierung erfolgt über den SAP-Parameter: TDW_Compress = 1.

[3] SNC = Secure Network Communications integriert SAP NetWeaver SSO oder ein externes Sicherheitsprodukt in SAP-Systeme. Mit der Verwendung von SNC erhöht sich die (System-) Sicherheit, indem Sie zusätzliche Funktionen eines Sicherheitsprodukts nutzen, die in SAP-Systemen nicht direkt verfügbar sind.

SNC schützt die Datenkommunikationspfade zwischen verschiedenen Clients- und Serverkomponenten des SAP-Systems, die das SAP-Protokoll RFC oder DIAG verwenden. Mit SNC können bekannte kryptografische Algorithmen angewendet werden.

[4] Hypertext Transfer Protocol: Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz.

[5] Simple Object Access Protocol.

- **Kommunikation zwischen Systemen**
  - SAP-spezifische Protokolle wie RFC[6],
  - HTTP-Kommunikationsprotokolle,
  - SOAP-Protokolle.

Je nach benutztem „Zugriffskanal“ und in Abhängigkeit des geforderten Zugriffsschutzes sowie des SAP-Release-Standes sind der in der Passwort-Richtlinie entsprechende Regelungen und Vorgaben seitens des (IT-) Managements vorzunehmen.

Die nachfolgenden Mindestanforderungen an eine Passwort-Richtlinie beziehen sich überwiegend auf die „interaktive Dialogauthentifizierung“ (SAP-GUI). Sofern andere Authentifizierungsverfahren, wie z.B. SSO, zum Einsatz kommen, sind die Inhalte der SAP-Passwort-Richtlinie entsprechend anzupassen.

Hinweis

Im Zusammenhang mit der Erstellung einer (UEi- bzw. TK-) individuellen SAP-Passwort-Richtlinie ist es wichtig den gesamten “**Lebenszyklus**”[7] eines **SAP-Passwortes** zu betrachten.

Die daraus abzuleitenden (Soll-) Vorgaben umfassen neben der Erstellung (“**Komplexität**”), der Vergabe (“**Initialpasswor**t”) und des **Passwortwechsels** vor allen Dingen **Anweisungen** bzw. **Handlungsempfehlungen** zur **Vermeidung** von **Passwort-Diebstahl** („Outsider“ / „Insider“).[8]

2. Geltungsbereich (Rev.)

Die im Zusammenhang mit der SAP-Passwort-Richtlinie nachfolgend dargestellten Soll-Vorgaben sind grundsätzlich für alle Prüfungen der SAP-Passwort-Verfahren in der Diehl-Gruppe – ergänzend zu den bereits vorhandenen Passwort-Vorgaben - heranzuziehen.

3. Definitionen

Hash-Funktion	Für das sichere Speichern von (SAP-) Passwörtern werden Hash-Funktionen bzw. –algorithmen eingesetzt, bei denen das durch den Benutzer vergebene Passwort auf einen Hashwert „abgebildet“ wird. Die unterschiedlichen Längen der verschiedenen Benutzer-Passwörter werden dabei auf einen immer gleich langen Hash-Wert übertragen. Der derzeit in SAP anwendbare sicherste Hash-Algorithmus ist die zweite Version des „Secure Hash Algorithm“ (kurz: SHA-2).[9]

[6] Remote Function Call – Aufruf von Funktionsbausteinen aus einem entfernten (SAP-) System.

[7] Lebenszyklus Passwort mit z.B. Beantragung, Prüfung, Gewährung, Übermittlung, Verfall, Sperre, etc.

[8] Nach einigen Expertenmeinungen ist es wahrscheinlicher, dass (Daten-) Sicherheitslücken eher durch einen „Phishing-Angriff“ oder durch einen Angriff eines Innentäters entstehen, als durch (externe) „Brute-Force-Angriffe“.

[9] Standardisiert und veröffentlicht vom US-amerikanischen National Institute of Standards and Technology (NIST, vergleichbar mit dem deutschen „Bundesamt für Sicherheit in der Informationstechnik“, kurz: BSI).

Phishing	Der Begriff umschreibt eine Vorgehensweise, bei der die eigentlich streng vertraulichen Zugangsinformationen eines Benutzers mittels eines „Köders“[10] „abgefischt“ bzw. einer anderen, nicht berechtigten Person zu Kenntnis gelangen.
Brute-Force-Angriff	Hinsichtlich des Herausfindens eines verwendeten Passworts ist der – im Vergleich zur algorithmischen Wiederherstellen des Passworts - einfachste Ansatz, alle potenziellen Lösungen bzw. Passwörter durchzuprobieren, bis das richtige Passwort gefunden ist. Somit stellt ein Brute-Force-Angriff dem Grunde nach ein einfaches Ausprobieren von möglichen Passwörtern dar. Ein Brute-Force-Angriff auf die mit Hashfunktionen verschlüsselten (SAP-) Passwörter erfordert die Berechnung von Hashwerten für sehr viele mögliche Passwörter. Der Vergleich mit des jeweils berechneten Hashwertes mit dem in SAP gespeicherten ermöglicht die Verschlüsselung auszuhebeln. Die vordefinierten Hashlisten häufig verwendeter Passwörter werden allgemein als „Rainbow Tables“ bezeichnet.
„Privilegierte“ Benutzer	Benutzer mit erweiterten Berechtigungen wie z.B. System-Administratoren oder „Key User“.

4. Zielsetzung

Mit dem Erstellen bzw. Pflegen einer **Passwortrichtlinie** sind grundsätzlich folgende **Zielsetzungen** verbunden:

- Aufstellen von Regelungen und Vorgaben zur Benutzer-Authentifizierung,
- Absicherung des SAP-Anmeldevorgangs,
- Schutz vor Passwort-Hacking,
- Sensibilisierung der Mitarbeiter hinsichtlich der Verwendung und Änderung von Passwörtern.

5. Normative Anforderungsgrundlagen

1. Ab 2014: GoBD,
2. HGB, KonTraG,
3. IDW PS330,
4. Ab 25. Mai 2018: Anforderungen aus der **Datenschutzgrundverordnung** (kurz: DSGVO) **[11]**,
5. SAP Hinweise,
6. BSI IT-Grundschutz,
7. Diehl-interne Vorgaben (z.B. vom Corporate Information Security Officer).

[10] Zum Beispiel mittels einer vermeintlichen E-Mail der lokalen SAP-Administration mit der Aufforderung, seine Zugangsdaten zwecks Abgleich mit den in einer Datenbank gespeicherten Inhalten mitzuteilen.

[11] Teilweise wird in den vorliegenden Soll-Vorgaben noch auf die Vorgaben und Anforderungen aus dem **Bundesdatenschutzgesetz** verwiesen. Eine Aktualisierung auf die Anforderungen aus der DSGVO und Abstimmung mit dem Corporate Privacy Officer, Herrn Dr. Buss, ist geplant.

6. Verantwortlichkeiten

Die Verantwortung für die **Initiierung** einer SAP-Passwort-Richtlinie liegt zunächst bei den **gesetzlichen Vertretern** der Unternehmenseinheit. Die konkrete **Erstellung** und **Ausprägung** einer SAP-Passwort-Richtlinie erfolgt regelmäßig durch die **IT-Sicherheitsbeauftragten** bzw. durch den **IT-Leiter**.

Die Verantwortung für die **Umsetzung** der Richtlinie liegt regelmäßig bei dem zuständigen (System-) **Administrator** bzw. dem **IT-Leiter**.

Die konkreten Verantwortlichkeiten sind mit den eineindeutigen Funktionsnamen in der Richtlinie aufzuführen.

7. Mindestanforderungen

7.1. Vorgabe ist vorhanden

Eine aktuelle, schriftliche und entsprechend freigegebene, datenschutzkonforme Passwort-Richtlinie liegt für alle SAP-Systeme und alle darin enthaltenen Mandanten vor.

7.2. Formale Kriterien werden erfüllt

Die Passwortrichtlinie erfüllt folgende **formalen Anforderungen** bzw. **Dokumentationsstandards**:

- **Schriftform**: Die Passwort-Richtlinie liegt in Schriftform vor.
- **Freigabe**: Die Passwort-Richtlinie ist entsprechend freigegeben.
- **Aktualität**: Die Passwort-Richtlinie ist aktuell.
- **Kommunikation**: Die Passwort-Richtlinie wird an die relevanten Stellen kommuniziert.

Die schriftliche **SAP-Passwort-Richtlinie** muss derart verfasst sein, dass sie

- verständlich, zuverlässig, nachvollziehbar, administrierbar, umsetzbar sowie überprüfbar und
- „ordnungsgemäß“ gemäß den zugrundeliegenden rechtlichen Normen ist. Die Ordnungsmäßigkeit ist gegeben, wenn die
  - Einhaltung gesetzlicher Anforderungen,
  - Gewährleistung der – teilweise gesetzlich geforderten – Nachvollziehbarkeit,
  - Gewährleistung der Datenintegrität,
  - Gewährleistung der Überprüfbarkeit der Wirksamkeit von Datenschutzkontrollmaßnahmen, frühzeitige Erkennung und Beseitigung von potenziellen Schwachstellen, sowie das
  - Möglichkeit vorhanden ist, Verstöße gegen Sicherheitsvorgaben zu (frühzeitig) erkennen,

  gegeben ist.

7.3. Inhaltliche Vorgaben werden erfüllt

1. Definition des Prozesses der Passwortvergabe

- Beschreibung des Prozesses zur SAP-Passwortvergabe unter Berücksichtigung von
  - Prozessverantwortlichkeiten,
  - Prozessbeginn und –ende,
  - Prozessziel, etc.
- Bei Verwendung einer Software (z.B. SAP-Password Reset, Akquinet) ist auf die vorhandene Verfahrensdokumentation[12] zu verweisen.

2. Umgang mit Passwörtern und Verwendung von Passwort-Speicher-Software

Die SAP-Passwort-Richtlinie muss im Zusammenhang mit der **Sensibilisierung** der Benutzer mindestens folgende Hinweise enthalten:

- Passwörter dürfen niemals in E-Mails, Chats oder anderen elektronischen Kommunikationsmedien preisgegeben werden. **Ausnahme:** Mitteilung von Initialpasswörtern.
- Passwörter dürfen niemals aufgeschrieben (z.B. Zettel unter Schreibtischunterlage) oder unverschlüsselt gespeichert werden.
- Weder persönliche Passwörter noch die „eigenen“ Regeln zum Generieren von persönlichen Passwörtern dürfen anderen Personen mitgeteilt werden.
- Passwörter dürfen nicht auf Fragebögen oder Formularen angegeben werden.
- Die Nutzung von „Passwort-Erinnerungsfunktionen" Speicherfunktionen (z.B. in Web-Browsern) ist aus sicherheitstechnischer Sicht nicht gestattet.
- Sollte der Verdacht bestehen, dass ein Passwort (gegebenenfalls versehentlich) kompromittiert wurde, so ist dieses unverzüglich zu ändern.
- Es sind Passwörter zu wählen, die nicht gleichzeitig auch auf unternehmensfremden Systemen (z.B. Kunden- oder Privatbereich) verwendet werden.
- Bei Verwendung von **Passwort-Speicher-Software**, wie z.B. Keepass, ist ein entsprechend „starkes“ Master-Passwort zu verwenden. Für dieses Master-Passwort gelten die gleichen vorgenannten „Regeln“.

3. Beschreibung der verwendeten Authentifizierungsverfahren

- Im Zusammenhang mit der Authentifizierung an ein SAP-System sind die mit jeweils eingesetzten Authentifizierungsverfahren verbundenen („technischen“) Besonderheiten und vorgenommenen Einstellungen kurz zu beschreiben.
- Bei Standard-Verfahren bzw. –Einstellungen kann auch auf die vorhandene Verfahrensdokumentation verwiesen werden.

[12] Nach dem Schreiben vom Bundesministerium der Finanzen (BMF) vom 14. November 2014 besteht eine Verfahrensdokumentation aus folgenden vier Bestandteilen (s.a. Schreiben, Rz. 153):

- Allgemeine Beschreibung,
- Anwenderdokumentation,
- Technische Systemdokumentation und
- Betriebsdokumentation.

4. Festlegung der „globalen“ Einstellungen für Passwort-Regeln

- Dabei sind folgende, **beispielhaft** aufgeführte Sachverhalte, zu berücksichtigen:[13]
  - (Mindest-) Passwortlänge,
  - Das erste Zeichen eines Passworts darf kein Ausrufezeichen, Fragezeichen oder Leerzeichen sein,
  - Die ersten drei Zeichen des Passworts und der Benutzerkennung dürfen nicht identisch sein,
  - Keines der ersten drei Zeichen darf ein Leerzeichen sein,
  - Dass Passwort darf nicht PASS oder SAP* lauten,
  - Sofern der Benutzer sein Passwort selbst ändern kann, muss dieses Passwort von den letzten fünf verwendeten Passwörtern unterschiedlich sein.
  - Das Passwort kann von einem Benutzer nach dessen korrekter Eingabe geändert werden,
  - Ein Benutzer kann sein Passwort maximal einmal täglich ändern; ein Administrator kann das Passwort eines Benutzers beliebig oft ändern,
  - Beim Passwort wird in Groß- und Kleinschreibung unterschieden,
  - Änderungen der Passwortregeln (z. B. über eine Änderung der Einträge der Tabelle USR40) betreffen nicht bereits vorhandene Kennwörter. Die Passwortregeln werden nur bei der Änderung eines Passworts berücksichtigt,
  - Setzen Parameter für Verschlüsselung (aktiv für z.B. SNC, RCF, etc.). Die vorhandenen Verschlüsselungstechniken sind zu nutzen.
- Die „global“ vorgenommenen Einstellungen können bei neueren Release-Ständen durch definierte SAP Sicherheitsrichtlinienattribute zu z.B. Passwortänderungen „wirkungslos“ werden (s.a. hierzu Abschnitt 6 i.V.m Anlage I).

[13] Die finalen Vorgaben erfolgen durch die jeweilige UEi (Dateneigner) oder durch den CISO.

5. Festlegung der Anmeldeparameter, weitere Parameter und Sicherheitsrichtlinien

- Die Anmeldeparameter legen die Vorgaben des SAP-internen Zugriffschutzes fest. Die gesetzten Parameter tragen somit erheblich zur SAP-Systemsicherheit bei.[14]
- Die jeweilige Ausprägung einzelner **Anmelde-Parameter** ist abhängig von dem **jeweiligen SAP-Releasestand** und den **Diehl-internen Vorgaben[15]**. Diese „globalen" Parameter-Einstellungen gelten nur für Benutzer, deren Benutzerstammsatz keiner Sicherheitsrichtlinie zugeordnet ist.
- Bei neueren SAP-Release-Ständen (ab SAP NetWeaver 7.31) können sogenannte **Sicherheitsrichtlinien** mit einzeln auszuprägenden Attributen eingesetzt werden. Die Attribute umfassen nachfolgende „Attributsgruppen"
  - o Passwortregeln,
  - o Passwortänderung
  - o **Anmelderegeln**.

  Bei der Festlegung der Anmeldeparameter sind die in **Anlage I**, Seite 12, **beispielhaft** aufgeführten Anmeldeparameter (→ Attributsgruppe 3) zu berücksichtigen. Die aufgeführten Attribute werden in der SAP-Tabelle „Sec_Policy_Attr" gespeichert.

6. Passwörter für „nicht-personalisierte" SAP-Benutzer mit besonderen Privilegien[16]

- Beschreibung des Prozesses zur SAP-Passwortvergabe für „privilegierte" oder nicht-personalisierte SAP-Benutzer
  - o In Ergänzung zu dem „Standard"-Vergabeprozess sind die „Besonderheiten" darzustellen. Darunter zählen **beispielsweise**,[17]
    - Passwort-Länge: mindestens 16 Zeichen
    - Passwort-Wechselfrist: s.a. nachfolgenden Abschnitt 7. Passwort-Wechselfristen,
    - Unterschiedliche Passwörter für die Authentifizierung der privilegierten bzw. nicht-personalisierten SAP-Benutzer auf System-, Datenbank- oder Anwendungsebene.[18]
    - Unterschiedliche Passwörter für die Authentifizierung der privilegierten bzw. nicht-personalisierten SAP-Benutzer im Entwicklungs-, Qualitätssicherungs- und Produktivsystem.

[14] Die Parameter können sowohl im SAP-Default-Profil als auch in einzelnen Instanzprofilen (→ relevant bei Login-Parameter) gesetzt werden. Instanzprofile liefern einem Applikationsserver zusätzliche Konfigurationsparameter, die die Einstellungen im Default-Profil vervollständigen. Normalerweise handelt es sich um Parameterwerte, die je nach Anforderungen (Ressourcen und Applikationen) der Instanz angepasst werden. Außerdem definieren sie die verfügbaren Instanzressourcen (Hauptspeicher, Shared Memory, Rollspeicher usw.) und wie man den SAP-Applikationspuffern Speicher zuweist.

[15] Zum Beispiel: „**Konzept zur Erhöhung der SAP-Security**", Dateiname „DIG_SAP_Security_v1.22.docx, Version 1.22, Stand 8.April 2016, Ersteller: Diehl Informatik GmbH (nicht verbindlich für Diehl-Konzern bzw. nicht freigegeben).

[16] In einem SAP-System sind dies üblicherweise die Notfall-Benutzer. Im Gegensatz hierzu sind privilegierte Benutzer, wie z.B. Key User, Modul-Betreuer oder Administratoren, in SAP grundsätzlich personalisiert.

[17] Die beispielhaft aufgeführten Ausprägungen beruhen auf Best-Practice-Ansätzen und wurden noch nicht im Detail mit dem Corporate Information Security Officer (CISO) abgestimmt.

[18] Aufnahme von Hinweis, dass Ausnahmen aus Produktivitäts- oder anderweitigen Gründen durch den CISO zu genehmigen sind.

7. Passwort-Wechselfristen

- Definition der Wechselfristen unter Berücksichtigung von
  - SAP Sicherheitsrichtlinienattribute zu Kennwortänderungen,
  - Prozessbeginn und –ende,
  - **Beispiele Mindest-Vorgaben**:
    - Mindestens vierteljährlicher Passwortwechsel,
- Bei Verwendung einer Software (z.B. Microsoft Laps, Microsoft) ist auf die vorhandene Verfahrensdokumentation zu verweisen.

8. Vorgaben zur Passwort-Komplexität

- Festlegen der Passwort-Komplexität mittels Beschreibung einzelner Einflussgrößen wie z.B.
  - Passwortlänge (mindestens **acht** Zeichen)
  - Ausprägung folgender Merkmalsklassen:
    - Klein- und Großbuchstaben (mindestens ein Klein- und ein Großbuchstabe)
    - Zahlen (mindestens eine Zahl)
    - Satz- und Sonderzeichen (mindestens ein Zeichen).
  - Kein „triviales“ Passwort, keine Muster aus Wörtern oder Zahlen (s.a. nächsten Abschnitt 9.)

9. Definition von "verbotenen" bzw. trivialen Passwörtern

- Neben den Passwort-relevanten Einstellungen (über Systemprofilparameter), sind die in der Tabelle USR40 die **unzulässigen Passwörter** (z. B. triviale Kennwörter oder einfache Zeichenkombinationen) aufzuführen. Diese Liste ist in jedem System – sprich auch in einem Entwicklungs- und Qualitätsicherungssystem – zu erstellen und fortlaufend zu pflegen. Sie muss mindestens nachfolgende Einträge bzw. enthalten:[19]
  - Wochentage,
  - Monate,
  - Länder,
  - Feiertage,
  - Jahreszeiten,
  - Häufig verwendete Vornamen,
  - Automarken,
  - Namen der Diehl-Standorte,
  - Namen der Diehl-UEi‘s.

[19] Die IT-Revision hält eine Liste von 81 Diehl-spezifischen „trivialen“ Passwörtern vor, die bei Bedarf weitergeleitet werden kann.

10. Vergabe von Initial-Passwörter

- Initial-Passwörter werden bei der Anlage einer Benutzerkennung oder nach der Rücksetzung eines Benutzer-Passwortes erzeugt. Bei der ersten oder einer erneuten Anmeldung des Benutzers muss dieser das Initial-Passwort durch ein benutzerdefiniertes Passwort ersetzen.
- Für die Erzeugung von Initial-Passwörter sollte nur der in SAP vorhandene Passwort-Assistent verwendet werden.
- Über die Richtlinie sind folgende Sachverhalte festzulegen:
  - Benutzer-Administratoren vergeben nicht immer wieder dasselbe Ininital-Passwort,
  - Nur autorisierte Benutzer dürfen die Berechtigung besitzen, Initial-Passwörter zu vergeben,
  - Kein Zugriff auf die Tabelle „USR02“, da hier auch gespeichert wird, welcher Benutzer noch kein Initial-Passwort zugewiesen bekommen hat.
  - Wird das vergebene Initial-Passwort nach einer vordefinierten Frist (z.B. 5 Tage) vom Benutzer nicht geändert, wird das Passwort ungültig bzw. der Zugang gesperrt.

11. Passwörter und Anwendungsentwicklung

Die Entwickler von SAP-Anwendungen haben sicherzustellen, dass das Programm die folgenden Sicherheitsvorkehrungen enthält:

- Unterstützung von Authentifizierungen von Individual-Benutzern und keine Gruppen,
- Keine Speicherung von verschlüsselten Passwörtern mit Hilfe von „unsicheren“ Verfahren (z.B. SHA-1),
- Keine Speicherung von verarbeiteten Passwörtern im Klartext oder in einfach verschlüsselter Form,
- Zugriffsmöglichkeiten auf SAP-Systeme ohne Authentifizierung dürfen nicht implementiert werden.

Des Weiteren ist sicherzustellen, dass

- für den Zugriff auf andere SAP-Systeme mindestens eine Authentifizierung durch Benutzername und Passwort implementiert ist,

  Hinweis: bei Systemen mit bestimmten Sicherheitsanforderungen können weitere Authentifizierungsmechanismen erforderlich werden.
- SAP-Applikationen die in den vorgenannten Abschnitten beschriebenen Kriterien durch technische Vorgaben erfüllen,
- SAP-Applikationen lediglich die Anmeldung individueller Benutzer (statt z.B. Benutzergruppen) ermöglichen,
- Die Übertragung von Passwörtern bei einer SAP-System-Anmeldung nur verschlüsselt erfolgt,
- die SAP-Anwendung es ermöglicht, einzelnen SAP-Benutzern Berechtigungen oder Funktionen zuzuweisen. Hierdurch wird ausgeschlossen, dass einzelne Benutzer (z.B. im Fall der Stellvertretung) niemals die Benutzerkonten von Kollegen benutzen müssen,
- maximal fünf erfolglose Anmeldeversuche zur Sperrung des betroffenen Benutzerkontos führen,
- bei der Eingabe der Passwörter diese nicht am Bildschirm angezeigt werden,
- das System Passwortwechsel im vorgegebenen Turnus initiiert,
- Gesperrte Benutzer sollten nicht automatisch (z.B. über Nacht) systemseitig wieder freigeschaltet werden.

12. Absicherung der SAP-Tabellen mit Kennwort-Hash-Werten

Neben der Komplexität von SAP-Passwörtern (s.a. Abschnitt 9) stellt auch die Speicherung der Passwörter im SAP-System einen wesentlichen Einflussfaktor auf die SAP-Sicherheit dar. Selbst bei hinreichend komplexen SAP-Passwörter kann eine fehlende bzw. unzureichend robuste Verschlüsselung der Passwörter in den SAP-Tabellen ein Sicherheitsrisiko darstellen (→ z.B. Aufruf der Tabellen durch nicht berechtigte Personen).

Hierzu sind bei den Vorgaben folgende Sachverhalte zu berücksichtigen:

- Upgrade des SAP Kernels auf den Release-Stand 7.02 oder höher, um die "PWDSALTED-HASH" Hashwerte zu unterstützen,
- Verwendung des neuesten Hash Algorithmus (mindestens "Iterated salted SHA1", statt MD5 and SHA1, Aktivierung der verfügbaren Verschlüsselungstechniken),
- Setzen des Parameters "login/password_downwards_compatibility" auf "0", um sicherzustellen, dass die stärksten Hashwert-Verfahren zur Anwendung kommen,
- Entfernen der alten, redundanten in der Tabelle USR02 gespeicherten Passwort-Hashwerte. Dies kann mit dem Report „CLEANUP_PASSWORD_HASH_VALUES" erfolgen,
- Starke Einschränkung der Möglichkeit, über das Auslesen und Extrahieren von nachfolgend aufgeführten Tabellen und Ansichten („views") auf Passwort-Informationen zuzugreifen: [20]
  - USH02,
  - USH02_ARC_TMP,
  - USR02,
  - USRPWDHISTORY,
  - VUSER001,
  - VUSR02_PWD.

  } Zuordnung einer Berechtigungsgruppe, die **keinem** Benutzer zugeordnet ist (z.B. SPWD).
- Setzen des Parameters "login/min_password*" zur Stärkung der Passwort-Komplexität,
- Einstellen einer gesicherten Netzwerkkommunikation über das Setzen folgender Parameter:
  - Parameter "snc/enable = 1"
  - Parameter "snc/accept_insecure_gui = 0" oder „= U".
- Weitere, zu regelnde Zugriffsmöglichkeiten auf die Passwort-SAP-Tabellen:
  - SQL-Datenbank Befehle,
  - Single-Sign-On,
  - Business Warehouse,
  - Andere SAP-Systeme wie Entwicklungs- und Qualitätssicherungssystem (neben Produktivsystem).

[20] In Abhängigkeit des jeweiligen SAP-Release-Standes. Die einschlägigen, von SAP herausgegebenen „SAP-Hinweise" sind regelmäßig zu berücksichtigen.

8. Reports, Transaktionen und Tabellen zu SAP-Passwörtern

Bei den nachfolgend - nicht abschließend - aufgeführten (SAP-) Reports, Transaktionen und Tabellen ist zwischen folgenden inhaltlichen Zielstellungen zu unterscheiden:

- Unterstützung bei der Erstellung einer Passwort-richtlinie,
- Kontrolle bzw. Überwachung von Passwort-relevanten Sachverhalten.

Report, Transaktion, Tabelle	Beschreibung
RSUSR003	Analyse der Standard-Benutzer, Informationen zum Kennwortstatus (trivial / nicht trivial) sowie zum Grund einer möglichen Benutzersperre.
USR02	Tabelle Anmeldedaten
SU01 (TC)	Benutzerpflege, Zuordnung der Sicherheitsrichtlinien zu Benutzern
SECPOL (TC)	Pflege der Sicherheitsrichtlinien
Sec_Policy_Attr	Tabelle, inder die Attribute der Sicherheitsrichtlinien gespeichert werden.
Sec_Policy_RT	Tabelle, die zur Überprüfung der Konfiguration herangezogen werden kann.
SECPOL_DISPLAY_CHANGE-DOCUMENTS	Report, die Änderungen an den Sicherheitsrichtlinien auswertet.
SECPOL_CHANGES	Transaktion, mit der Änderungen an den Sicherheitsrichtlinien ausgewertet können.
RSUSR100N	Report, mit dem die vorgenommene Zuordnung von Sicherheitsrichtlinien zu Benutzern ausgewertet wird.
RSPFPAR	Anzeige von Parametern.

Anlage I – SAP-Sicherheitsrichtlinien-Attribute

Attribut	Atributs-gruppen 1 = Passwortregel 2 = Passwortänderung 3 = Anmeldung	Standard	Wertebe-reich	Beschreibung, kurz	Beschreibung, detailliert	Abwärts-kompatibilität
CHECK_PASSWORD_BLACKLIST	1	1	String	Prüfung der Kennwort-Blacklist (Tabelle USR40)	Legt fest, ob das System das Kennwort bei der Anmeldung mit einer Negativliste verbotener Kennwörter abgleicht. Wenn der Administrator ein verbotenes Kennwort vergibt, gibt das System nur eine Warnung aus, über die sich der Administrator hinwegsetzen kann.	---
MIN_PASSWORD_DIGITS	1	0	Zulässige Werte: 0- 40	Minimale Anzahl von Ziffern	Bestimmt die Mindestanzahl an Ziffern (0-9), die in einem Kennwort enthalten sein müssen. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 0 - 8.
MIN_PASSWORD_LENGTH	1	6	Zulässige Werte: 3- 40	Minimale Kennwortlänge	Bestimmt die Mindestlänge eines Kennworts. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 3 - 8.
MIN_PASSWORD_LETTERS	1	0	Zulässige Werte: 0- 40	Minimale Anzahl von Buchstaben	Bestimmt die Mindestanzahl an ASCII-Buchstaben (A-Z und a-z), die in einem Kennwort enthalten sein müssen. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 0 - 8.

Attribut	Atributs-gruppen 1 = Passwortregel 2 = Passwortänderung 3 = Anmeldung	Standard	Wertebe-reich	Beschreibung, kurz	Beschreibung, detailliert	Abwärts-kompatibilität
MIN_PASSWORD_LOWERCASE	1	0	Zulässige Werte: 0- 40	Minimale Anzahl von Kleinbuchstaben	Bestimmt die Mindestanzahl an ASCII-Kleinbuchstaben (a - z), die in einem Kennwort enthalten sein müssen. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 0 - 8.
MIN_PASSWORD_SPECIALS	1	0	Zulässige Werte: 0- 40	Minimale Anzahl von Sonderzeichen	Bestimmt die Mindestanzahl an Sonderzeichen, die in einem Kennwort enthalten sein müssen. Als Sonderzeichen werden alle Zeichen betrachtet, die weder Ziffern (0-9) noch ASCII-Buchstaben (A-Z oder a-z) sind. Hierzu gehören nationale Sonderzeichen und Unicode-Zeichen, sofern es sich um ein Unicode-System handelt, ebenso wie die ASCII-Zeichen !"@ $%&/()=?'`*+~#-_.,;:{[]}\<>|. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 0 - 8.
MIN_PASSWORD_UPPERCASE	1	0	Zulässige Werte: 0- 40	Minimale Anzahl von Großbuchstaben	Bestimmt die Mindestanzahl an ASCII-Großbuchstaben (A-Z), die in einem Kennwort enthalten sein müssen. Das Attribut wirkt sowohl bei der Vergabe neuer Kennwörter als auch bei der Kennwortänderung oder beim Zurücksetzen bestehender Kennwörter.	Falls Profilparameter login/password_downwards_compatibility den Wert 5 hat, ist der zulässige Wertebereich 0 - 8.
MIN_PASSWORD_CHANGE_ WAITTIME	2	1	---	Minimale Wartezeit bei Kennwortänderung	---	---

Attribut	Atributs-gruppen 1 = Passwortregel 2 = Passwortänderung 3 = Anmeldung	Standard	Wertebe-reich	Beschreibung, kurz	Beschreibung, detailliert	Abwärts-kompatibilität
MIN_PASSWORD_DIFFERENCE	2	1	---	Anzahl unterschiedlicher Zeichen bei Änderung	---	---
PASSWORD_CHANGE_FOR_SSO	2	1	---	Kennwortänderungspflicht bei SSO-Anmeldung	---	---
PASSWORD_CHANGE_INTERVAL	2	0	---	Intervall regelmäßiger Kennwortänderungen	---	---
PASSWORD_COMPLIANCE_TO_CURRENT_POLICY	2	0	---	Kennwortänderung nach Regelverschärfung	---	---
PASSWORD_HISTORY_SIZE	2	5	---	Größe der Kennworthistorie	---	---
DISABLE_PASSWORD_LOGON	3	0	---	Kennwortanmeldung unterbinden	---	---
DISABLE_TICKET_LOGON	3	0	---	Ticketanmeldung unterbinden	---	---
MAX_FAILED_PASSWORD_LOGON_ ATTEMPTS	3	5	---	Maximale Anzahl von Fehlversuchen	---	---

Attribut	Atributs-gruppen 1 = Passwortregel 2 = Passwortänderung 3 = Anmeldung	Standard	Wertebe-reich	Beschreibung, kurz	Beschreibung, detailliert	Abwärts-kompatibilität
MAX_PASSWORDJDLE_INITIAL	3	0	---	Gültigkeit ungenutzter Initialkennwörter	---	---
MAX_PASSWORDJDLE_PRO-DUCTIVE	3	0	---	Gültigkeit ungenutzter Produktivkennwörter	---	---
PASSWORD_LOCK_EXPIRATION	3	0	---	Automat. Aufhebung der Kennwortsperre	---	---
SERVER_LOGON„PRIVILEGE	3	0	---	Anmeldeverhalten bei Parameter login/ser-ver_logon_restriction = 1	---	---

♦ ♦ ♦