epas

Enterprise Password Analytics Solution

Einhaltung des BSI IT-Grundschutz ORP 4: Identitäts- und Berechtigungsmanagement mit Hilfe von EPAS

Das Bundesamt für Sicherheit in der Informationstechnik („BSI“) hat bis 2020 in seinem IT-Grundschutz-Kompendium regelmäßiges Ändern von Passwörtern bevorzugt. In der, im Februar 2020 publizierte Ausgabe wird diesen Wechseln nicht mehr empfohlen. Hingegen muss ein Passwort spätestens bei einem Verdacht auf Missbrauch gemäß BSI-Richtlinien geändert werden. Abwechselnde und sichere Passwörter bei verschiedenen Anmeldungen sollten verwendet werden und diese müssen geändert werden, wenn der Verdacht auf eine Kompromittierung des entsprechenden Accounts bzw. Passworts besteht.

Die Detack GmbH bietet seit 2013 eine, auf eigener Hardware basierte Softwarelösung an, die in dem Rechenzentrum der Kunden installiert wird und nur von der IT-Abteilung der Kunden in einer gesicherten Umgebung und ohne Internetverbindung betrieben wird.

EPAS besteht aus 2 Komponenten: EPAS Audit und EPAS Enforcer.

EPAS Audit analysiert und bewertet die Passwort-Qualität, wie in dem „BSI IT-Grundschutz ORP 4: Identitäts- und Berechtigungsmanagement“ empfohlen ist, indem es einen echten Angriff simuliert, ohne die Kennwörter jemals offenzulegen oder zu speichern und ohne die Verfügbarkeit des Zielsystems zu gefährden. EPAS bietet eine effektive Qualitätssicherung für die passwortbasierte Authentifizierung mithilfe europaweiter und in Nordamerika patentierter Technologie.

EPAS Audit extrahiert alle Passwort-relevanten Daten vom Zielsystem, um diese dann für eine Bewertung der Widerstandsfähigkeit der Passwörter gegen Angriffe heranzuziehen. Zum Schutz der Prüfobjekte verwendet EPAS ausschließlich die vom Hersteller vorgesehenen Schnittstellen zur Extraktion verschlüsselter Daten. Somit entsteht kein Risiko für die Systemstabilität der ausgewählten Zielsysteme.

EPAS Enforcer ist ein Modul zur Verbesserung der Passwortqualität, welche die Verwendung von schwachen, wiederverwendeten oder gemeinsam benutzten Passwörtern bei jedem Passwort-Wechseln systematisch verhindert. Der EPAS Enforcer prüft bei neu gesetzten Passwörtern und Passwortwechsel, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht. Für den Endbenutzer heißt das, dass früher erlaubte Passwörter wie „Passwort123“ oder „Geheim!“ nicht mehr akzeptiert werden.

In diesem Dokument wird gegenübergestellt wie EPAS sowohl Audit als auch Enforcer eine Organisation in der Einhaltung von „BSI IT-Grundschutz ORP 4: Identitäts- und Berechtigungsmanagement“ hinsichtlich der Passwortsicherheit unterstützt. Die entsprechenden Funktionen von EPAS werden detailliert erklärt.

„ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)“[1]

„Die Institution MUSS den Passwortgebrauch verbindlich regeln (siehe auch ORP.4.A22 Regelung zur Passwortqualität und ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme).“[1]

✓ Passwörter sind die am häufigsten verwendete Authentifizierungsmethode. Mit dem EPAS Audit wird nachgewiesen, dass das Qualitätsniveau der derzeit verwendeten Kennwörter den hohen Authentifizierungsanforderungen der relevanten Sicherheitsrichtlinien und -standards entspricht.

„Dabei MUSS geprüft werden, ob Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollen, oder ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können.[1]

Passwörter DÜRFEN NICHT mehrfach verwendet werden.“[1]

„Für jedes IT-System bzw. jede Anwendung MUSS ein eigenständiges Passwort verwendet werden.“[1]

✓ Die EPAS Audit-Technologie wird verwendet, um sowohl schwache Passwörter (zu kurz, zu einfach usw.) zu identifizieren, die persönlichen und geheimen Informationen preisgeben würden, als auch die mehrfach von einem Person und von mehreren Personen verwendeten Passwörter zu erkennen, die die Rechenschaftspflicht verhindern. EPAS Enforcer kann sowohl schwache Zugriffsdaten als auch mehrfach von einer Person und von mehreren Personen verwendete Kennwörter verhindern.

„Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden.“[1]

✓ EPAS Audit identifiziert bereits gefährdete oder auf der schwarzen Liste (einschließlich aller bekannten geleakten Passwörter) stehende Passwörter sowie alle verwendeten, leicht zu erratene Passwörter. EPAS Enforcer ermöglicht das Blacklisting aller angesprochener Passwörter und das Festlegen der Mindestanforderungen für die Passwortlänge.

„Passwörter MÜSSEN geheim gehalten werden. Sie DÜRFEN NUR dem Benutzer persönlich bekannt sein. Passwörter DÜRFEN NUR unbeobachtet eingegeben werden. Passwörter DÜRFEN NICHT auf programmierbaren Funktionstasten von Tastaturen oder Mäusen gespeichert werden. Ein Passwort DARF NUR für eine Hinterlegung für einen Notfall schriftlich fixiert werden. Es MUSS dann sicher aufbewahrt werden. Die Nutzung eines Passwort-Managers SOLLTE geprüft werden.
Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.“[1]

---

[1] BSI – IT-Grundschutz Kompendium 2020 ORP.4 Identitäts- und Berechtigungsmanagement: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

✓ EPAS analysiert und bewertet die Kennwortqualität, indem es einen echten Angriff simuliert, ohne die Kennwörter jemals offenzulegen oder zu speichern und ohne die Verfügbarkeit des Zielsystems zu gefährden. EPAS bietet eine effektive Qualitätssicherung für die passwortbasierte Authentifizierung. Dementsprechend werden die Regelungen von ORP.4.A22 fast vollständig von den Funktionen von EPAS abgedeckt, ohne dass zusätzliche Maßnahmen oder Technologien erforderlich sind.

„ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] (B)“[1]

„In Abhängigkeit von Einsatzzweck und Schutzbedarf MÜSSEN sichere Passwörter geeigneter Qualität gewählt werden.
Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist.
Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.“[1]

✓ EPAS analysiert und bewertet die Kennwortqualität, indem es einen echten Angriff simuliert, ohne die Kennwörter jemals offenzulegen oder zu speichern und ohne die Verfügbarkeit des Zielsystems zu gefährden. EPAS bietet eine effektive Qualitätssicherung für die passwortbasierte Authentifizierung. Dementsprechend werden die Regelungen von ORP.4.A22 fast vollständig von den Funktionen von EPAS abgedeckt, ohne dass zusätzliche Maßnahmen oder Technologien erforderlich sind.

„ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)“[1]

„IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden.“[1]

✓ Das EPAS Audit umfasst regelmäßige Aktualisierungen der validen Gründe. Wenn festgestellt wird, dass ein Kennwort bereits gefährdet ist, kann eine Kennwortänderung erzwungen werden. EPAS Enforcer macht den regelmäßigen Wechseln des Kennworts durch einen Benutzer überflüssig. Immer wenn eine Passwortänderung stattfindet, können die bereits kompromittierten Passwörter auf die schwarze Liste gesetzt werden.

„Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.“[1]

EPAS Audit identifiziert bereits gefährdete oder auf der schwarzen Liste (einschließlich aller bekannten geleakten Passwörter) stehende Passwörter sowie alle verwendeten kurzen Passwörter. EPAS Enforcer ermöglicht das Blacklisting aller gehakten Passwörter und das Festlegen der Mindestanforderungen für die Passwortkomplexität.

EPAS Audit und EPAS Enforcer sind mit Wörterbüchern in mehreren Sprachen ausgestattet, die die häufigsten verwendeten Passwörter sowie alle verfügbaren früheren Regelverstöße enthalten. EPAS Audit nutzt diese Wörterbücher, um festzustellen, ob ein Kennwort einem Wörterbucheintrag entspricht oder einem Wörterbucheintrag ähnlich ist. EPAS Enforcer verwendet diese Wörterbücher, um Richtlinien zu implementieren, die Benutzer daran zu hindern, in Wörterbüchern enthaltene einzelne Kennwörter auszuwählen.

EPAS enthält auch eine Funktion, die die Erkennung von Passwörtern ermöglicht, die auf kontextspezifischen Wörtern basiert (d.h. Ableitungen davon). EPAS ist in der Lage, mithilfe von „Maschine Learning“ das Verhalten des Benutzers zu verstehen und ihn daran zu hindern, Kennwörter zu verwenden, die mit öffentlichen Informationen des Benutzers verknüpft sind oder mit seinen historischen Kennwörtern in Verbindung stehen.

EPAS Audit bietet eine Funktion, mit der Benutzer ihre neuen Kennwörter anhand der, an der Sicherheitsrichtlinien der Organisation angepassten, EPAS-Richtlinien überprüfen können. Jedes Passwort erhält einen empfohlenen numerischen Wert, und in schwarzen Listen enthaltene Passwörter werden markiert. EPAS Enforcer gibt ein numerischer Wert des ausgewählten Passwortes an und berechnet die Passwortqualität aus mathematischer und sprachlicher Sicht. Mit einer expliziten Nachricht hilft Enforcer dem Benutzer bei der Auswahl eines sicheren Kennworts.

„Ist dies nicht möglich, so SOLLTE geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden. Standardpasswörter MÜSSEN durch ausreichend starke Passwörter ersetzt und vordefinierte Kennungen MÜSSEN geändert werden.“[1]

EPAS Audit ermittelt, ob anfängliche Kennwörter noch verwendet werden, ob sie von mehreren Benutzern gemeinsam genutzt werden und wann solche Kennwörter geändert wurden.

„ORP.4.M8 Regelung des Passwortgebrauchs“[2]

„Grundsätzlich ist zu überlegen, ob überhaupt Passwörter als alleiniges Authentisierungsverfahren eingesetzt werden sollten oder ob anstelle von Passwörtern andere Authentisierungsverfahren bzw. zusätzliche Authentisierungsmerkmale verwendet werden können, wie Zertifikate oder eine Mehr-Faktor-Authentisierung.
Um Passwörter zu erstellen und handzuhaben, muss es feste Regelungen geben. Die Benutzer von IT-Systemen sind diesbezüglich zu unterweisen. So muss vorgebeugt werden, schwache Passwörter zu verwenden und falsch mit ihnen umzugehen.“[2]

✓ EPAS Audit unterstützt Organisationen dabei, Risiken auf der menschlichen Seite direkt anzugehen, indem das Bewusstsein und die Schulung der Benutzer anhand von Kennwortprüfungsberichten (Reports) gemessen werden. Die Historie der Ergebnisse der Passwortprüfung ermöglicht die Messung der Trainingseffektivität sowie die Eskalation von Informationen und Schulungen für riskantere Benutzer. Unabhängig von der Auditierung-Funktion bietet EPAS eine separate Schnittstelle für die freiwillige Bewertung der Kennwortqualität, die normalerweise von Benutzern verwendet wird, um Kennwörter zu überprüfen, bevor sie verwendet werden. Diese Schnittstelle wird auch im Sensibilisierungstraining verwendet.

EPAS Enforcer bietet direktes Feedback zur Kennwortqualität bei der Kennwortänderung und erhöht so das Verstehen wie ein sicheres Passwort gestalten werden soll. In EPAS Audit und Enforcer können verschiedene Sicherheitsklassen mit dargelegten Richtlinien definiert werden. Es können strengere Regeln z.B. für Mobil- / Telearbeitsregelungen definiert werden, um das Sicherheitsniveau zu erhöhen.

„Ein Passwort muss gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.“[2]

✓ Das EPAS Audit bietet sofortige Einblicke in die sicherheitsrelevanten Aktivitäten von Konten, z. B. letzte Kennwortänderung, letzte Anmeldung, Sperrstatus und Informationen zu Berechtigungen. Diese Daten tragen dazu bei, nicht verwendete Konten zu erkennen und zu entfernen, die noch aktiviert sind und häufig über hohe Berechtigungen verfügen.

EPAS Audit identifiziert bereits gefährdete oder auf der schwarzen Liste (einschließlich aller bekannten geleakten Passwörter) stehende Passwörter sowie alle verwendeten kurzen Passwörter.

---

[2] BSI IT-Grundschutz „Umsetzungshinweise zum Baustein ORP.4: Identitäts- und Berechtigungsmanagement“:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2020/Umsetzungshinweise_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=3#download=1

„Die Wiederverwendung bereits eingesetzter Passwörter sollte unterbunden werden. Gegebenenfalls können Regelungen erlassen werden, dass Passworte nach einer angemessenen Zeitspanne wiederverwendet werden dürfen. Voreingestellte Passwörter und Kennungen, z. B. des Herstellers bei Auslieferung von IT-Systemen, müssen durch individuelle Passwörter und, wenn möglich, Kennungen ersetzt werden.
Stärke der eingesetzten Faktoren (beim Faktor Wissen siehe auch ORP.4.M22 Regelung zur Passwortqualität).“[2]

✓ EPAS ermittelt die Kennwortqualität, indem es einen echten Angriff simuliert, ohne die Kennwörter jemals offenzulegen oder zu speichern und ohne die Verfügbarkeit des Zielsystems zu gefährden. EPAS bietet eine effektive Qualitätssicherung für die passwortbasierte Authentifizierung. EPAS Enforcer verhindert die Wiederverwendung von voreingestellten Passwörter.

„ORP.4.M22 Regelung zur Passwortqualität“[2]

„Werden in einem IT-System oder einer Anwendung Passwörter zur Authentisierung verwendet, so ist dafür zu sorgen, dass sichere Passwörter genutzt werden. Die Vorgaben für Passwörter müssen so gestaltet sein, dass sie einen praktikablen Kompromiss zwischen Komplexität und mit vertretbarem Aufwand nutzbar darstellt. Die Anzahl der möglichen Passwörter eines Authentisierungsverfahrens muss dabei so groß sein, dass ein Passwort nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann. Folgende Regeln zu Passwortgestaltung und -gebrauch müssen deshalb beachtet werden“[2]

✓ Die Benutzerregistrierung in einer Institution umfasst die Erstellung eines Kontos und die Zuweisung eines anfänglichen Passworts, das so schnell wie möglich geändert werden muss. EPAS Audit ermittelt, ob anfängliche Kennwörter noch verwendet werden, ob sie von Benutzern mit mehreren Dateien gemeinsam genutzt werden und wann solche Kennwörter geändert wurden. EPAS Audit-Daten können verwendet werden, um die Registrierung / Abmeldung von Konten mit den tatsächlichen Identitäten im Benutzer-Repository zu korrelieren.

„Ein Passwort darf nicht leicht zu erraten sein, daher darf es keine Informationen aus dem persönlichen oder beruflichen Umfeld des Benutzers enthalten wie z. B. Namen, Kfz-Kennzeichen oder das Geburtsdatum.“[2]

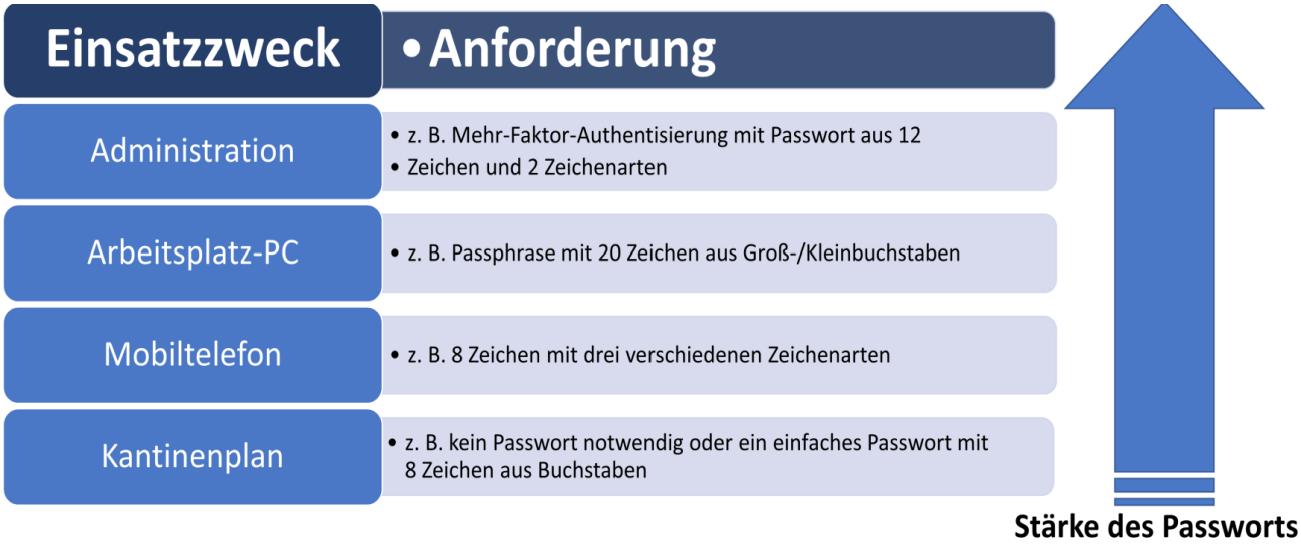
✓ EPAS Audit und EPAS Enforcer sind mit Wörterbüchern in mehreren Sprachen ausgestattet, die die häufigsten verwendeten Passwörter sowie alle verfügbaren früheren Regelverstöße enthalten. EPAS Audit nutzt diese Wörterbücher, um festzustellen, ob ein Kennwort einem Wörterbucheintrag entspricht oder einem Wörterbucheintrag ähnlich ist. EPAS Enforcer verwendet diese Wörterbücher, um Richtlinien zu implementieren, die Benutzer daran hindern, in Wörterbüchern enthaltene einzelne Kennwörter auszuwählen.
EPAS enthält auch eine Funktion, die die Erkennung von Passwörtern ermöglicht, die auf kontextspezifischen Wörtern basieren (d.h. Ableitungen davon). EPAS ist in der Lage, mithilfe von „Maschine Learning“ das Verhalten des Benutzers zu verstehen und ihn daran zu hindern, Kennwörter zu verwenden, die mit öffentlichen Informationen des Benutzers verknüpft sind oder mit seinen historischen Kennwörtern in Verbindung stehen.

„Passwörter dürfen nicht mehrfach verwendet werden, sondern für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden.“[2]

Die EPAS Audit-Technologie wird verwendet, um sowohl schwache Passwörter (zu kurz, zu einfach usw.) zu identifizieren, die persönlichen und geheimen Informationen preisgeben würden, als auch die mehrfach von einem Person und von mehreren Personen verwendeten Passwörter zu erkennen, die die Rechenschaftspflicht verhindern. EPAS Audit kann die mehrfache Verwendung eines Passwortes mithilfe der Auditfunktion entdecken und anfordern, dass diese korrigiert wird.

EPAS Enforcer kann die mehrfache Verwendung automatisch blockieren.

„Bei einem guten Passwort sind die Länge und die Anzahl der verwendeten Zeichenarten wie Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen in sinnvoller Kombination und in Abhängigkeit des verwendeten Verfahrens zu wählen:
• z. B. 20 – 25 Zeichen Länge und zwei genutzte Zeichenarten (weniger komplex, längeres Passwort beziehungsweise Passphrase)
• z. B. 8 – 12 Zeichen Länge und vier genutzte Zeichenarten (komplexer, geringere Länge des Passworts)
• z. B. bei Mehr-Faktor-Authentisierung 8 Zeichen Länge und drei genutzte Zeichenarten
Der Einsatzzweck von Passwörtern beeinflusst die Anforderungen an die Sicherheit von Passwörtern, siehe folgende Abbildung:



Passwörter, die im Rahmen von Mehr-Faktor-Authentisierung eingesetzt werden, können eine geringere Komplexität haben, als wenn sie alleiniger Sicherheitsfaktor sind.“[2]

EPAS Enforcer ist ein EPAS-Modul zur Verbesserung der Passwortqualität, welches die Verwendung von schwachen, wiederverwendeten oder gemeinsam benutzten Passwörtern bei jedem Passwort-Change systematisch verhindert. Der EPAS Enforcer prüft bei neu gesetzten Passwörtern und Passwortwechsel, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht.
Ist der Passwortwechsel nicht erfolgreich, so ermöglicht ein optionales Feature im EPAS Enforcer, dass Benutzer über die Gründe für fehlgeschlagene Passwortänderungen informiert werden (z.B.: „Das Passwort ist nicht stark/lang genug für den Arbeitsplatz-PC – Richtlinien“/ oder „Das Passwort darf nicht in einem Wörterbuch enthalten sei.“). Die Sicherheitsanforderungen für ein Passwort ergeben sich aus kundenspezifischen und gruppenspezifischen Sicherheitseinstufungen sowie der Risikokategorie der zu schützenden Daten.

„ORP.4.M23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme“[2]

Passwort-verarbeitende Anwendungen und IT-Systeme müssen, falls technisch möglich, folgende Randbedingungen einhalten:
Die Wahl von Trivialpasswörtern und gängigen Zeichenketten, z. B. „123456“, „password“, Namen, Geburtsdaten sowie Tastaturmustern wie „asdf“, muss vermieden werden. Dies kann z.B. verhindert werden, indem Passwörter bei Eingabe gegen Listen von Trivialpasswörtern bzw. Listen von öffentlich bekannt gewordenen Passwörtern geprüft werden.“[2]

EPAS Audit analysiert die Kennwortqualität, indem es einen echten Angriff simuliert, ohne die Kennwörter jemals offenzulegen oder zu speichern und ohne die Verfügbarkeit des Zielsystems zu gefährden. EPAS bietet eine effektive Qualitätssicherung für die passwortbasierte Authentifizierung.
EPAS Enforcer prüft bei neu gesetzten Passwörtern und Passwortwechsel, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht. Für den Endbenutzer heißt das, dass früher erlaubte triviale Passwörter wie „Passwort123“ oder „Geheim!“ nicht mehr akzeptiert werden.

„Die Benutzer sollten bei der Änderung eines Passwortes durch Hinweise zur Passwort-Güte unterstützt werden, die diese Anforderungen beachtet.“[2]

EPAS Enforcer prüft bei neu gesetzten Passwörtern und Passwortwechsel, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht. EPAS Enforcer unterstützt das Generieren eines sichere neue Passwort.

„Es sollte nur Software eingesetzt werden, die die gesamte Benutzereingabe für das Passwort auch tatsächlich verwendet. Sollte es eine maximale Anzahl an Zeichen geben, sollte dieser Umstand dem Benutzer bewusst gemacht werden.“[2]

Ist der Passwortwechsel nicht erfolgreich, so ermöglicht ein optionales Feature im EPAS Enforcer, dass Benutzer über die Gründe für fehlgeschlagene Passwortänderungen informiert werden (z.B.: „Das Passwort ist nicht stark/ lang genug für den Arbeitsplatz-PC – Richtlinien“/ oder „Das Passwort darf nicht in einem Wörterbuch enthalten sein.“ Die Sicherheitsanforderungen für ein Passwort ergeben sich aus kundenspezifischen und gruppenspezifischen Sicherheitseinstufungen sowie der Risikokategorie der zu schützenden Daten.

„IT-Systeme oder Anwendungen sollten Anwender nur mit einem validen Grund auffordern, das Passwort zu wechseln, reine zeitgesteuerte Wechsel werden nicht empfohlen.“[2]

EPAS Audit identifiziert bereits gefährdete oder auf der schwarzen Liste (einschließlich aller bekannten geleakten Passwörter) stehende Passwörter sowie alle verwendeten kurzen Passwörter. EPAS Enforcer ermöglicht das Blacklisting aller versprochenen Passwörter und das Festlegen der Mindestanforderungen für die Passwortlänge.

„Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen, z.B. parallele Anmeldungen von verschiedenen Systemen oder Standorten, Häufung von Fehleingaben usw. Wenn keine ausreichenden Maßnahmen zum Erkennen von Kompromittierung von Passwörtern möglich sind, so ist zu überlegen, ob die Nachteile eines zeitgesteuerten Passwortwechsels in diesem Fall in Kauf genommen werden können und Passwörter in gewissen Abständen, z.B. alle 6 Monate, gewechselt werden sollen.“[2]

Das EPAS Audit umfasst regelmäßig aktualisierte kompromittierte/ geleakte Passwörter, die aufgrund bekannter Sicherheitsvorfälle auftreten. Diese werden auch regelmäßig upgedatet. Diese Daten werden vom Auditprozess verwendet, um festzustellen, ob eines der Konten offen gelegte/ kompromittierte Informationen/ Passwörter verwendet. Diese Konten werden sofort markiert, um den Korrekturprozess zu starten.

„Die Passwörter dürfen im IT-System nicht im Klartext gespeichert werden, sie sollten z. B. mittels sicherer Einweg-Funktion (Hashfunktionen mit Salt und ggf. Pepper) geschützt werden.“[2]

EPAS erkennt und meldet Klartext-Passwörter, Passwörter mit reversibler Verschlüsselung sowie Passwörter, die mit schwachen/ unsicheren Hashing-Algorithmen gespeichert sind. Reporting-Metriken, über alle von einer Identität verwendeten Kennwortalgorithmen, sind in den Report zu finden.

„Die Wiederholung alter Passwörter beim Passwortwechsel muss vom IT-System verhindert werden (Passwort-Historie).“[2]

EPAS Enforcer kann die Wiederholung alter Passwörter beim Passwortwechsel vollständig blockieren.

„Passwörter für Dienste oder technische Benutzer, die meist in Konfigurationsdateien auf einem System hinterlegt sind, müssen so sicher wie möglich gespeichert werden. Konfigurationsdateien können z. B. über Zugriffsrechte abgesichert werden. Für die Erstanmeldung neuer Benutzer sollten Initial-Passwörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen. Für die Erstanmeldung muss für jeden neuen Benutzer ein individuelles Passwort verwendet und dieses nach dem einmaligen Gebrauch geändert werden.“[2]

Mit EPAS Audit können strengere Klassen der Passwortstärke für privilegierte Konten definiert werden. Automatische Benachrichtigungen über Verstöße und fortlaufende Metriken werden verwendet, um eine nachweislich starke Authentifizierung privilegierter Konten nachzuweisen.
Mit EPAS Enforcer werden strengere Richtlinien definiert, die für privilegierte Konten durchgesetzt werden sollen. EPAS-Komponenten - Audit und Enforcer - werden entweder unabhängig voneinander verwendet oder ergänzen PAM (Privileged Access Management)) Lösungen.
EPAS-Reports enthalten detaillierte Informationen zur Mitgliedschaft in Gruppen und Organisationseinheiten, einschließlich auch gemischter Gruppen. Dies ermöglicht die schnelle Identifizierung vertraulicher Benutzerrechte zusammen mit den Passwortsicherheitsmetriken für alle Konten, einschließlich technischer und schwer identifizierbarer Konten
Die EPAS-Reports bieten sofortige Einblicke in die sicherheitsrelevanten Aktivitäten von Konten, z. B. letzte Kennwortänderung, letzte Anmeldung, Sperrstatus und Informationen zu Berechtigungen. Diese Daten tragen dazu bei, nicht verwendete Konten zu erkennen und zu entfernen, die noch aktiviert sind und häufig über hohe Berechtigungen verfügen
Die Benutzerregistrierung in einer Institution umfasst die Erstellung eines Kontos und die Zuweisung eines anfänglichen Passworts, das so schnell wie möglich geändert werden muss. EPAS Audit ermittelt, ob anfängliche Kennwörter noch verwendet werden, ob sie von Benutzern mit mehreren Dateien gemeinsam genutzt werden und wann solche Kennwörter geändert wurden. EPAS Audit-Daten können verwendet werden, um die Registrierung / Abmeldung von Konten mit den tatsächlichen Identitäten im Benutzer-Repository zu korrelieren.

DETACK GmbH
Königsallee 43
71638 Ludwigsburg, Germany
Phone: +49 7141 69 62 65 0
Fax: +49 7141 69 62 65 5
info@detack.de
www.epas.de

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig