epas

Enterprise Password Assessment Solution

Sichere Daten durch starke Passwörter

EPAS Audit

Das mit Abstand höchste Risiko für eine IT-Sicherheitsinfrastruktur ist und bleibt der menschliche Faktor – insbesondere wenn Benutzer durch die Verwendung von Passwörtern mit Ihrer IT-Umgebung interagieren. Es gibt viele effektive Maßnahmen zum Schutz der IT-Infrastruktur, wie z.B. Antivirus Programme, Firewalls oder den Einsatz von Verschlüsselungstechnologien. Schwache Passwörter hingegen stellen nach wie vor ein unkalkulierbar hohes Risiko dar. Und hier setzen Angreifer an.

Mindestens 60 % der in Unternehmen eingesetzten Passwörter genügen nicht den sicherheitstechnischen Mindestanforderungen.

EPAS ist eine gemeinsame Entwicklung der Detack GmbH und der Praetors AG, ihrem Schweizer Partner. EPAS ist eine „On-Premises SaaS" Lösung zur automatischen und regelmäßigen Prüfung der unternehmensweiten Passwort-Qualität. Diese bislang nahezu unlösbare Aufgabe, allein aufgrund der über viele Jahre gewachsenen Systemlandschaften - welche von Microsoft A/D über IBM System z, SAP und mehr reichen - wird von EPAS gelöst. Mit einer speziell für Unternehmen entwickelten Technologie extrahiert EPAS 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 der verschlüsselten Daten. Somit entsteht kein Risiko für die Systemstabilität der ausgewählten Zielsysteme.

Passwort Stärke

Passwort Policies setzen Anforderungen an Länge und Zusammensetzung eines Passwortes. Die Effektivität einer Policy gegen Passwort-Angriffe ist dennoch nachweislich gering. Angreifer verwenden unterschiedliche Methoden, um Passwörter wiederherzustellen. Die am häufigsten verwendete Methode ist die Wörterbuch-Attacke. Millionen von Wörtern aus Wörterbüchern – einschließlich Literatur und bereits veröffentlichter Passwörter von Passwort-Leaks aus dem Internet – werden herangezogen, um Passwort-Hashes zu erstellen, die dann mit den auf einem Server gespeicherten Passwort-Hashes verglichen werden. Eine Policy regelt nicht die Verwendung von Wörtern aus Wörterbüchern oder bekannter Abwandlungen, z.B. des @-Zeichens anstelle eines „a". Die echte Widerstandsfähigkeit eines Passwortes gegen Angriffe wird daher am besten durch strukturelle Entropie bewertet.

Universelle Passwortprüfung

EPAS analysiert die objektive Stärke der Passwörter ausgewählter Zielsysteme. EPAS kann sowohl unsalted, statically salted, dynamically salted Passwort-Hashes, sowie auch systemspezifische Verschlüsselungen prüfen. Hierbei werden auch System-Accounts und technische Accounts evaluiert.

Detailliertes und rechtssicheres Reporting

EPAS erstellt für jeden Audit-Job einen Auditbericht. In einem Executive Summary werden alle Berichtsdaten grafisch aufbereitet und mit Erklärungen ergänzt. Enthalten sind Gründe für die Wiederherstellbarkeit der Passwörter, Struktur, Konformität zur Policy und verschiedene statistische Daten. Die Passwörter selber werden niemals im Klartext angezeigt.

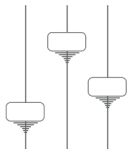
Entwickelt aus 15 Jahren IT-Security Erfahrung

EPAS resultiert aus mehr als 15 Jahren Erfahrung im IT-Security Auditing. Erfahrungen aus manuellen Penetrationstests zeigen, dass jegliche Sicherheitsvorkehrungen ohne starke Passwörter versagen. EPAS ist weltweit die einzige Lösung, die die Widerstandsfähigkeit der Passwortlandschaft eines Unternehmens gegen Angriffe bewerten und damit verbessern kann.

Für Unternehmen entwickelt

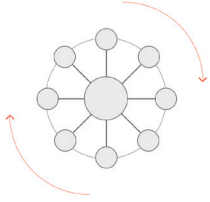
EPAS wurde speziell auf die Bedürfnisse von Unternehmen zugeschnitten. Mehr als 30 verschiedene Systeme und Datenbanken werden von EPAS adressiert. Das Reporting ist datenschutzkonform und genügt allen Anforderungen eines Betriebsrates.

Kundenspezifische Passwortprüfung



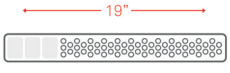
Passwörter werden gegen vielfältige Kriterien geprüft: eine individuell einstellbare Passwort-Policy und zahlreiche objektive, auf struktureller Entropie basierende Regeln. Zur Simulation von Wörterbuchattacken werden Wörterbücher kundenspezifisch in Bezug auf Sprache und unternehmenseigene Begriffe definiert.

Mehrfachverwendung von Passwörtern



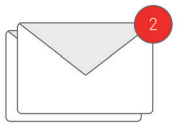
Passwörter werden auf Mehrfachverwendung geprüft. EPAS erkennt, wenn ein User ein und dasselbe Passwort für mehrere Systeme verwendet oder ob viele User ein und dasselbe Passwort haben. Beide Situationen stellen ein unkalkulierbar hohes Sicherheitsrisiko dar.

Technische und System-Accounts



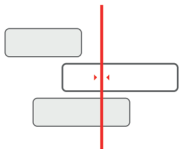
EPAS bewertet zusätzlich alle technischen Accounts. Diese haben meist einfache, manchmal gar keine Passwörter oder Default-Passwörter vom Hersteller und sind unter Umständen von einer Policy ausgenommen. Zudem haben sie die größten Berechtigungen und stellen aus Sicht eines Angreifers die attraktivsten Ziele dar.

Sensibilisierung per E-Mail



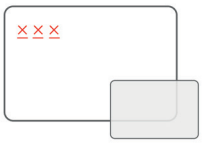
EPAS fordert den Benutzer automatisch auf, sein Passwort zu ändern, falls dieses den auditspezifischen Anforderungen nicht genügt oder nicht Policy-konform ist. Über dieselbe Funktion wird auch der EPAS Administrator über ein abgeschlossenes Passwort-Audit und die Verfügbarkeit des Berichts benachrichtigt.

Audit Jobs & Job Queuing



Ein intelligentes Job- und Queuing-System sorgt dafür, dass regelmäßige Passwort-Audits voreingestellt und terminiert werden können und Job-Kollisionen ausgeschlossen werden. EPAS ist voll skalierbar und kann simultane Audits über Millionen von Benutzerkonten durchführen.

Trusted Computing und Verschlüsselung



Alle Daten, die von EPAS verarbeitet werden, sind permanent verschlüsselt. Das Trusted Computing Prinzip wird zur Versiegelung der Plattform angewendet, ein zusätzlicher TPM Chip sorgt mittels kryptografischer Verfahren für Software- und Datenintegrität. Mögliche physische oder Software-Manipulationen werden durch ausfallsichere Sicherheitsmechanismen registriert, welche das System im Falle eines Eindringversuches automatisch herunterfahren.

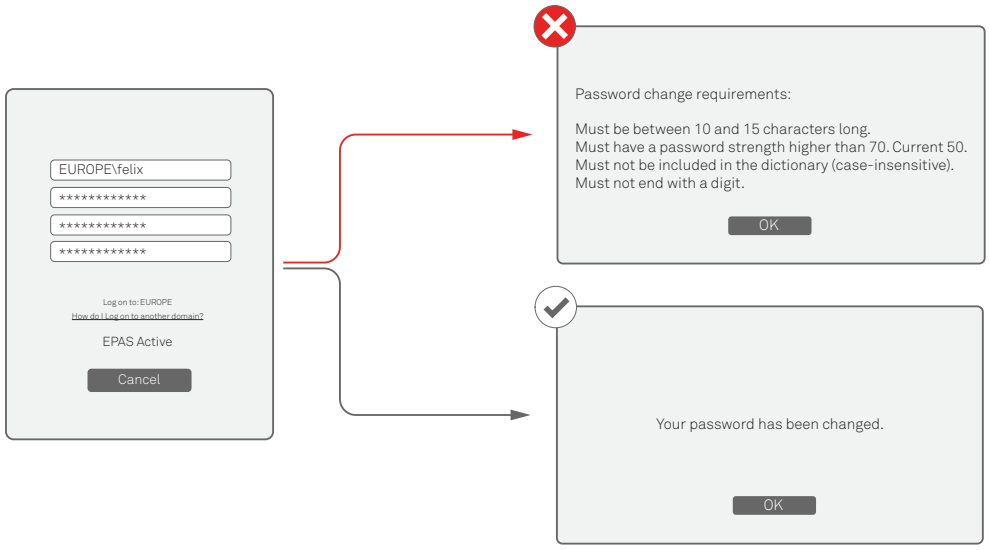
EPAS Enforcer

Der EPAS Enforcer ist ein in EPAS verfügbares Modul zum Password Quality Enforcement. Eine einzelne, hoch verfügbare EPAS Instanz verwaltet zentral Passwort-Changes aller unterstützten Systeme. Das aktuelle Release unterstützt Microsoft Produkte. Support für weitere Plattformen befindet sich bereits in der Entwicklung. Der EPAS Enforcer wird als LSA Filter in die Domain Controller einer Microsoft A/D Umgebung integriert und prüft bei neu gesetzten Passwörtern und Password-Changes, ob die Sicherheit des neu gewählten Passwortes einer zentralisierten Policy und den Sicherheitsanforderungen entspricht.
Die Sicherheitsanforderungen für ein Passwort ergeben sich aus kundenspezifischen und gruppenspezifischen Sicherheitseinstufungen sowie der Risikokategorie der zu schützenden Daten. Das neue Passwort wird mittels der EPAS eigenen Bewertungsmechanismen evaluiert und auf seine Widerstandsfähigkeit gegen echte Angriffe geprüft. Für den Endbenutzer heißt das, dass früher erlaubte Passwörter wie „Passwort123“ oder „Geheim!“ nicht mehr akzeptiert werden. 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 darf nicht in einem Wörterbuch enthalten sein.“).

„Mit dem EPAS Enforcer stellen wir schon beim Passwort-Change sicher, dass es tatsächlich ein starkes Passwort ist – stark heißt, widerstandsfähig gegen reale Angriffe.“

Workflow Password-Change Windows Active Directory

Technisch gesehen besteht für in diese Domain eingebundene Rechner und Systeme kein Unterschied zu einer Standard Windows A/D Installation. Der EPAS Enforcer integriert sich nahtlos in das System. Ein User verwendet den bekannten Standard-Windows Mechanismus, um das Passwort zu ändern.



EPAS

EPAS ist eine „On-Premises“ Lösung ohne externen Zugriff, die das Problem von schwachen und vorhersehbaren Passwörtern unternehmensweit angeht.
EPAS führt automatische und regelmäßige Prüfungen der unternehmensweiten Passwort-Qualität durch und hilft dabei, sichere Passwörter in großen und heterogenen Umgebungen durchzusetzen. EPAS ist skalierbar und auditiert regelmäßig Millionen von User Accounts sowie technische Accounts. Objektive Passwortstärke, Länge, Zusammensetzung der Zeichen sowie Policy Compliance sind einige der Bewertungskriterien von EPAS.
Die Lösung kommt bereits in über 30 Ländern zum Einsatz.

1. User sendet Anfrage zur Passwortänderung an den Domain Controller.
2. Der Domain Controller aktiviert den EPAS Filter, welcher zusätzliche User Informationen abruft, wie zum Beispiel Gruppenzugehörigkeit, Standort und andere relevante Eigenschaften.
3. Der EPAS Filter fasst alle abgerufenen Informationen zusammen und sendet sie über eine verschlüsselte, authentifizierte Verbindung zur nahegelegensten EPAS Appliance. Die EPAS Appliance überprüft Username, Gruppeninformationen und Passwort auf Policy Compliance, berechnet die Passwortstärke und führt alle anderen konfigurierten Prüfungen, die für diese spezielle Account-Kategorie definiert sind, aus. Das Ergebnis wird an den Domain Controller zurück geschickt.
4. Das Ergebnis des Passwort-Genehmigungs-Prozesses wird als true / false Statement zum Arbeitsplatzrechner gesendet.
5. Falls aktiviert zeigt ein auf dem Arbeitsplatzrechner installierter EPAS Credential Provider den Grund für einen gescheiterten Passwortänderungs-Versuch im Detail auf, ohne dabei eine Verbindung mit der EPAS Appliance zu benötigen. Die Benachrichtigung ist an die entsprechende Sprache und Region des Users angepasst.

Beispiel einer Policy:

1. Zeichenwiederholung: Das Passwort darf keine Zeichenfolgen aus 3 oder mehr aufeinanderfolgenden, gleichen Zeichen enthalten.
2. Länge: Das Passwort muss zwischen 10 und 15 Zeichen lang sein.
3. Aufeinanderfolgende Zeichen: Das Passwort darf keine Zeichenfolgen aus 3 oder mehr aufeinanderfolgende Zeichenfolgen, wie Tastatur-Reihenfolgen (z.B. „asdf“), enthalten.
4. Stärke: Die Passwortstärke muss > 70 sein.
5. Passwort Verlauf: Das Passwort muss sich von den letzten 10 verwendeten Passwörtern unterscheiden.
6. Wörterbuch: Das Passwort darf nicht in einem unternehmensspezifischen Wörterbuch gefunden werden.

„EPAS: Eine praxisgerechte, kostengünstige, international bewährte Lösung, die Spitzentechnologie einsetzt, um die Sicherheit von Benutzerkonten systemisch zu erhöhen – Stand der Technik.“

On-Premises SaaS

EPAS ist eine On-Premises SaaS Lösung und wird in Form eines oder mehrerer Hardwaremodule in das Rechenzentrum des Kunden integriert. Alle Daten liegen zu jeder Zeit ausschließlich beim Kunden, niemals in der Cloud.

EPAS ist abonnement-basiert, d.h. die Hardware bleibt jederzeit Eigentum der Detack GmbH. Eine jährliche Service-Gebühr enthält sowohl Software Updates wie auch Hardware Upgrades.

Unterstützte Standard Zielsysteme

IBM System i - iSeries - AS/400
IBM System p - pSeries - RS/6000 AIX
Mass definition possible]
IBM System z - zSeries - S/390 RACF (z/OS, z/VM)
IBM Lotus Domino Application Server Microsoft Active Directory Accounts Microsoft Windows Local Accounts [Mass definition possible]
BSD Operating System [Mass definition possible]
Linux Operating System [Mass definition possible]
Sun Solaris – SunOS [Mass definition possible]
Apache Basic - htpasswd SAP NetWeaver - ABAP AS LDAP Authentication Server

Unterstützte anwendungsspezifische Datenspeicherung

MSSQL System Accounts [Mass definition possible]
MySQL System Accounts [Mass definition possible]
Oracle System Accounts [Mass definition possible]
PostgreSQL System Accounts [Mass definition possible]
Sybase ASE System Accounts [Mass definition possible]
DB2 Database Custom Application
Informix Database Custom Application
MaxDB Database Custom Application
MSSQL Custom Database Application
MySQL Database Custom Application
Oracle Database Custom Application
PostgreSQL Custom Database Application
Sybase ASA Database Custom Application
Sybase ASE Database Custom Application

> *“ EPAS hat uns geholfen, unsere Passwortsicherheit enorm zu steigern – ein Sicherheitsrisiko, welches uns bewusst war und das wir lösen mussten, wir aber bislang weder überwachen noch kontrollieren konnten.”*
>
> - EINE GROßE INTERNATIONALE VERSICHERUNGSGESELLSCHAFT

DETACK GmbH
Königsallee 43
D-71638 Ludwigsburg
Phone: +49 (0) 7141 125-150
Fax: +49 (0) 7141 125-155
e-mail: info@detack.de
Web: www.epas.de