

## Privileged Passwort-Management

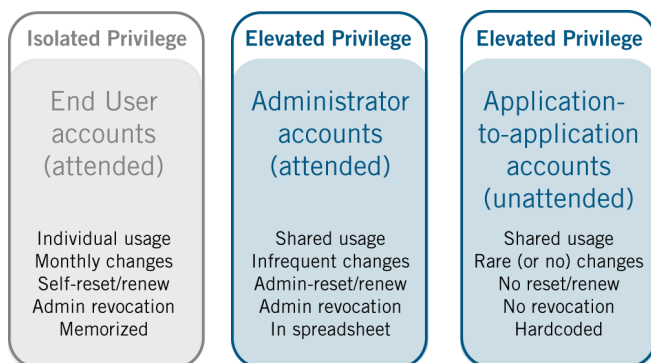
André Frehse  
Manager Business Development it.sec GmbH & Co. KG

Administrative Accounts besitzen eine weitreichende Macht – diesen Anwendern zu vertrauen ist gut aber nicht ausreichend. Das Risiko eines Missbrauchs ist hier relativ hoch. Oft verfügen Unternehmen über keine ausreichend umfassende Passwort-Management-Policie. Im einfachsten Fall werden privilegierte Passworte (wie Windows Administrator, UNIX root, Oracle sa) nur in einem Excel-Sheet verwaltet. Die Aktualität hinkt dann oft der implementierten Passwortrealität hinterher und die Konsistenz geht somit verloren.

Aber auch organisatorische Maßnahmen wie Passwortnomenklaturen hängen oft stark vom guten Willen der beteiligten Personen ab. Oft verbreitet sich so ein „Standard-Passwort“ unter mehreren Verantwortlichen für eine bestimmte Umgebung, was dann häufig auch nicht mehr geändert wird. Noch risikoreicher ist es, wenn der betreffende Mitarbeiter das Unternehmen verlässt und die Passworte somit auch in die Falschen Hände geraten können.

Hinzu kommt das Paradoxon bei zu anspruchsvollen Passwort Policies, dabei führt eine zu Hohe Anforderung in der Nomenklatur dazu, das Passworte verstärkt an wieder unsicheren Orten notiert werden. Letztendlich ist damit die Möglichkeit einer korrekten und konsistenten Umsetzung der Passwortpolicie und eine Risikoüberwachung kaum sinnvoll möglich. Oft verschwinden die Probleme förmlich aus den Augen der Manager und auch der Auditoren.

### Account-Typen



Auch die Menge an privilegierten Passwort-Accounts wird häufig falsch eingeschätzt – diese können je nach Unternehmen und Branche, schnell mal 40% oder mehr ausmachen. Neben den typischen Administrator-Accounts, existieren noch so genannte Application-to-Application-(A2A) und Application-to-Database-Accounts (A2D). Diese etablieren automatisch (unattended) und „hard coded“ per Skript in der Applikation verankert eine

Verbindung zu einer anderen Applikation oder einer Datenbank. Ein manuelles Management der A2A- oder A2D-Credentials findet selten statt und ist kosten-, zeitintensiv und fehleranfällig. Denn die Applikationen und Skripts müssen entsprechend modifiziert werden. Oft sind diese Credentials nicht einmal bekannt und liegen ggf. noch bei Entwicklerfirmen vor. Hinzu kommen diverse Accounts mit Default-Passworten, die unerkannt in den Systemen ruhen.

Der Druck dieses Thema in den Griff zu bekommen wächst somit stetig an. Hersteller von Perimeter- oder Client-Security Lösungen bieten Stand heute, hierzu keine Produktübergreifenden Lösungen an.

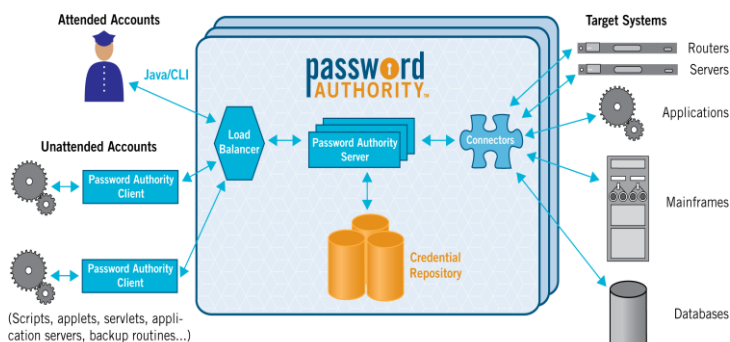
Aber auch Regelwerke wie PCI DSS oder SarbOx fordern eine Darlegung, wie der Zugriff auf schützenswerte Informationen kontrolliert wird. Neben den Anforderungen die sich aus der Business Kontinuität ergeben, sind auch die internen und externen IT-GRC (IT Governancen, Risk, Compliance) Erfordernisse zu erfüllen. Der Payment Card Industry Data Security Standard fordert hier z. B. ganz konkret: „Zuteilen einer eindeutigen Benutzererkennung für jede Person mit Rechnerzugang“

Wer die mächtigen Benutzer und ihre Rechte in den Griff bekommen möchte, muss im Grunde mehrere Punkte klären. Der Hersteller Cloakware hat diese Punkte in einem Lebenszyklus abgebildet und in vier grundlegende Aufgaben aufgeteilt, die das Passwort-Management zu erfüllen hat. Der Hersteller spricht im Detail von **Assess**, **Automate**, **Assure** und **Audit**.

- **Assess:** Hierbei werden die individuellen Anforderungen der Firma hinsichtlich der Identity-Management-Risiken im gesamten Passwort-Lifecycle bewertet.
- **Automate:** Hierunter ist die Automatisierung des Passwort-Managements gefasst. Auf diese Weise lassen sich Kosten und Downtimes reduzieren, die mit der manuellen Änderung von A2A- und A2D-Passwörtern einhergehen. Außerdem sind so jene Systemausfälle ausgeschlossen, die falsche oder fehlende Credentials (Benutzername/ Passwort) verursachen. Das Passwort-Management spart Zeit und Geld, während es zugleich die Service-Levels und Verfügbarkeit steigert.
- **Assure:** Hierunter ist die Sicherstellung von Compliance-Anforderungen und der operativen Systemverfügbarkeit zusammengefasst.
- **Audit:** Detailliertes Reporting und Beweissicherung erlauben die objektive Überprüfung der Einhaltung von Compliance-Richtlinien. Das Passwort-Managementsystem muss auch Applikationen von Drittanbietern einbinden können, um deren Daten ein

## Lebenszyklus eingehalten

Der Hersteller Cloakware hat sich bei der Entwicklung des »Password Authority«-Tools (CPA) an diese eigenen Vorgaben gehalten. Das CPA speichert Passwörter von Administratoren und Applikationen in einer mit dem AES-Algorithmus verschlüsselten Datenbank ab. Die zentrale Datenhaltung erlaubt die Pflege und Durchsetzung von Policies auf allen Geräten. Die Zugriffe auf diese Datenbank werden natürlich streng geregelt, da hier die mächtigsten Zugangsdaten im Netz vereint sind. Die Authentisierung der CPA-Administratoren wird anhand folgender starker Methoden abgewickelt: ID, Passwort, LDAP, RSA-SecurID, Active-Directory, X.509-Zertifikate, Kerberos und eine Auswahl mehrerer proprietärer Methoden. Die Applikationspasswörter werden automatisch und sicher abgefragt. Hart kodierte Credentials in Anwendungen werden dabei vollständig eliminiert. Ein autorisierter Server fragt die Zugangsdaten direkt beim CPA-Server ab. Danach erst verbindet er sich entsprechend stark authentifiziert und autorisiert mit anderen Applikationen und Datenbanken. CPA lässt sich sowohl über eine GUI als auch über eine Java-Schnittstelle ansteuern. Diese beherrscht die Ad-hoc-Abfrage von Passwörtern beim Zugriff auf einen Server, eine Datenbank oder eine Infrastrukturkomponente. Außerdem unterstützt sie Batch-Abfragen des CPA-Servers, bei denen die Credentials von Applikationen, Datenbanken oder eigenen Administrationskonsolen abgeglichen werden. Das Passwort-Management-System ist selbst hochverfügbar ausgelegt. Datenbank-Clustering, Load-Balancing und erweiterbare Servlet-Container lassen die CPA ausfallsicher arbeiten. Der CPA-Server lässt sich auf einer Standard Datenbank wie Oracle, MySQL oder MS-SQL installieren.



## Funktionsweise

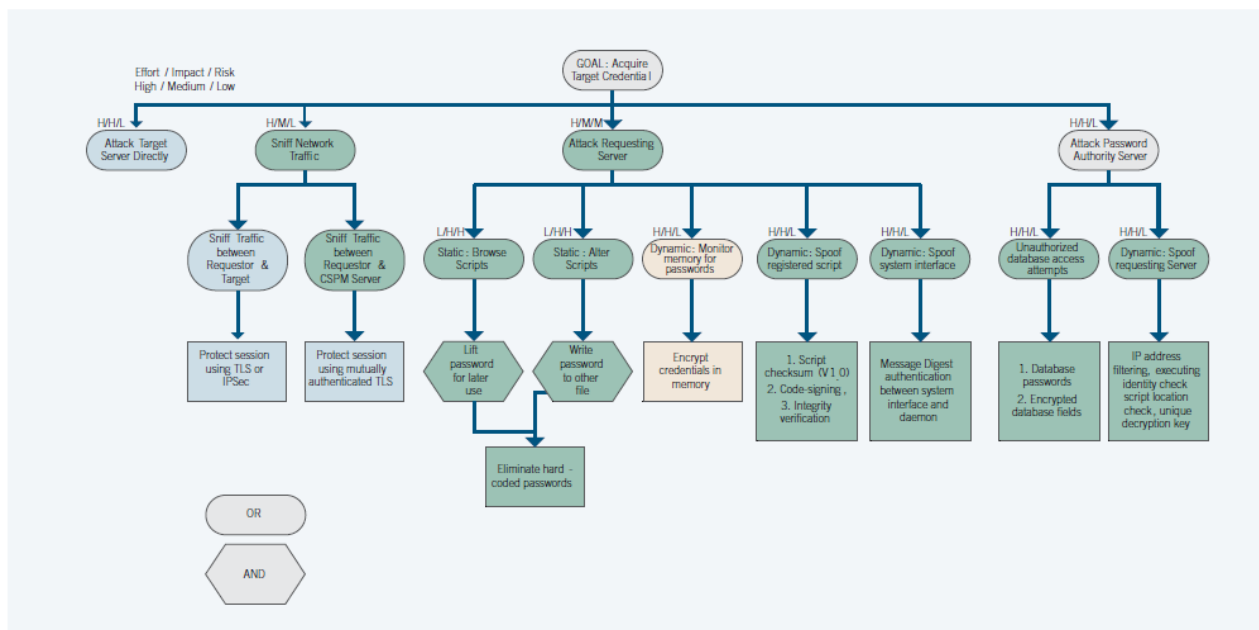
Die privilegierten Benutzer, seien es Administratoren, Applikationen oder Skripts, beziehen ihre Passwörter direkt beim CPA-Server. Erst dann können sie auf das eigentliche Zielsystem (Target-System) zugreifen. Das Passwort selbst liegt AES-verschlüsselt in der Datenbank (Credential-Repository). Administratoren (Attended-Accounts) greifen auf den CPA-Server zu und fordern das Passwort für ein Zielsystem an. Um sich an dem CPA-Server anzumelden, muss sich der Anfragende mit verschiedenen Mechanismen authentisieren. Falls der Benutzer eine Berechtigung für das Zielsystem hat, erhält er das entsprechende Passwort via Web- GUI, Command-Line-Interface (CLI) oder Java-API. Der CPA unterstützt prinzipiell alle Zielsysteme, die die Änderung von Passwörtern durch eine HTML-GUI oder eine Command-Shell zulassen. Standard-Konnektoren unterstützen unter anderem Oracle, Unix, Windows-Server, locale Windows-Administratoren, Active-Directory, LDAP, Cisco oder Juniper. Der privilegierte Anwender benutzt weiterhin seine gewohnten Applikationen, um auf die Zielsysteme zuzugreifen. Der einzige Unterschied liegt für ihn darin, dass er sich das Passwort nicht mehr merken muss, sondern dieses vom CPA auf Anfrage erhält. Er benötigt nur noch einen sicheren Zugriff auf den CPA-Server. Unattended-Accounts, also beispielweise eine Applikation, die Zugriff auf eine Datenbank benötigt, werden auf dem CPA-Server als authentische Anwendung registriert. Während der Registrierung werden ein Hardware-Fingerprint und ein Integritätswert für die Applikation oder das Skript generiert. Ein CPA-Administrator muss diese Applikation dann zusätzlich als authentisch freigeben. Auf dem anfragenden System wird hierzu ein CPA-Client installiert, die Zielsysteme benötigen keine zusätzliche Software. Passwörter können automatisch in frei definierbaren Intervallen, nach einem gewissen Zeitraum der letzten Benutzung und anhand vieler weiterer Kriterien geändert werden. Dabei werden sie nach vorgegebener Nomenklatur generiert. So lassen sich Policies für Länge und Komplexität zentral durchsetzen. Es ist weiterhin möglich, exklusiven Zugang zu einem System beispielsweise für Wartungsarbeiten zu erhalten. Cloakware nennt das hier eingesetzte Verfahren »Check-In«, »Check-Out«. Auf dem CPA-Server werden die Rechte privilegierter Benutzern auf Zielsysteme generell granular und anhand von Rollen verwaltet.

André Frehse  
Manager Business Development

Die CPA Cloakware Password Authority™ Architektur ist durch die Anwendung verschiedenster Sicherheitstechniken sehr gut gegen diverse Angriffe (siehe Abbildung 2) geschützt.

- **Transport layer security**  
Gegenseitig authentifizierte Sessions
- **Code obfuscation**  
Java byte-code obfuscation verhindert ein Reverse Engineering
- **White-box cryptography**  
Spezielle Code Transformation Technik die ein „auftauchen“ geheimer Schlüssel im Arbeitsspeicher verhindert

Figure 2. Server/application credentials attack graph



## Über it.sec

Die it.sec ist auf Sicherheitsberatungen und Komplettlösungen rund um das Thema der Informationssicherheit spezialisiert. Das Unternehmen wurde 1996 von Holger Heimann in Ulm gegründet und realisiert seitdem ganzheitliche Security-Konzepte für namhafte Unternehmen im In- und Ausland. Das Portfolio umfasst umfassende Beratungsleistungen rund um das Thema der IT-Sicherheit und Verfügbarkeit. Die Schwerpunkte bilden die Themen: Informationssicherheit, Datenschutzberatungen, IT-Risk-Management, Security Governance/Risk- & Compliance Consulting, Penetrationstest, IT-Forensics, Security Architecture Design und Reviews, ISO/IEC 2700x, BCM, BSI Grundschriftkataloge, Security GRC in SCADA Systems, Web-Application Security, Data Integrity, Hardening, PCI-Security, SOA and Web Services Security, Security Products: Web Application Firewall, IDS/IPS, SIEM, Content Security, Authentication & Authorization, PKI, Verschlüsselung, Firewall, HSM ( Application & Transaction Security)

## Kontakt

### Hauptsitz

it.sec GmbH & Co. KG  
Einsteinstrasse 55  
D-89077 Ulm

Fon +49(0)731-20589-0  
Fax +49(0)731-20589-29

### Office München

Trimbургstrasse 2  
D-81249 München

Fon +49(0)89-680940-30  
Fax +49(0)89-680940-31

eMail [info@it-sec.de](mailto:info@it-sec.de)  
[http:// www.it-sec.de](http://www.it-sec.de)