

be informed




Liebe Leserin, lieber Leser,
herzlich willkommen zur aktuellen Ausgabe
unseres Newsletters **be informed**.

Unsere heutige Ausgabe beschäftigt sich schwerpunktmäßig mit dem Thema Passwort-Management unter dem Gesichtspunkt von PCI DSS. Neben einem Fachartikel erhalten Sie praktische Hinweise von einem unserer Auditoren. Ich wünsche Ihnen eine anregende Lektüre!

Zum Jahresende möchte ich Ihnen einen Ausblick auf 2010 geben: Wir erwarten vom PCI Council und den Kartenorganisationen verstärkte Aktivitäten bei der Händlerzertifizierung. Außerdem wird das Thema Payment Applikation, deren Zertifizierung und damit die Diskussion über Technologien, die den Einsatz von Kartendaten minimieren, im Vordergrund stehen. Gerne unterstützen wir Sie bei diesen und anderen Fragestellungen!

Herzliche Grüße



Ralph Wörn - Vorstand



*Das Acertigo Team
wünscht Ihnen ein
besinnliches Weihnachtsfest
und einen guten Start ins Jahr
2010.*

Admin-Passwort-Management ist Grundbedingung für PCI-Zertifizierung

Gastartikel von Jochen Koehler / Cyber-Ark

Die Datenschutz-Richtlinien der Kreditkartenindustrie fordern von allen Unternehmen, die Kreditkarten-Transaktionen tätigen, ein striktes Passwort-Management. Dabei besteht aber bei vielen Firmen noch ein erheblicher Nachholbedarf, denn sie vernachlässigen häufig wesentliche Vorschriften.

Besonders privilegierte Accounts, wie sie IT-Administratoren besitzen, stellen in jedem Unternehmen ein erhebliches Sicherheitsrisiko dar. Die Passwörter der administrativen Accounts sind der Schlüssel zu allen unternehmenskritischen Datenbeständen. Ein verantwortungsvoller Umgang mit den Kennwörtern ist jedoch die Ausnahme. Kernproblem ist dabei, dass sich auf den IT-Systemen oft identische und leicht zu entschlüsselnde Passwörter finden, die zudem meistens

dert werden, bedeuten aber auch eine eindeutige Missachtung der PCI-Vorschriften. Eine Lösung der Problematik ist mit der Implementierung einer Applikation möglich, mit der alle privilegierten administrativen Accounts automatisch verwaltet und überwacht werden können. Eine solche Applikation hat in der Regel drei maßgebliche Bestandteile: Geschützte zentrale Speicherung, Policy-gesteuerte automatische Änderung und nachweisbare Protokollierung. Dadurch kann die

Ausgewählte, für das Passwort-Management relevante PCI-Vorschriften im Überblick:

- In Punkt 2 der PCI-Regelungen wird die Änderung von Kennwörtern gefordert. Das heißt, es sollte eine periodische Veränderung von Passwörtern auf Servern und Appliances erfolgen.
- Punkt 8 regelt die Zuweisung einer eindeutigen ID zu jeder Person mit Computerzugriff. Damit wird einerseits sichergestellt, dass alle Aktivitäten, die mit unternehmenskritischen Daten und Systemen zu tun haben, nur von dazu autorisierten Benutzern durchgeführt werden können. Andererseits ist nur so eine Nachvollziehbarkeit bis auf die Personenebene gewährleistet.
- In Punkt 10 wird das Protokollieren und Prüfen aller Zugriffe auf Daten von Kreditkarteninhabern gefordert. Diese Anforderungen müssen mit einer detaillierten, revisionssicheren Protokollierung der Passwortnutzung abgedeckt werden – alle Aktivitäten sollten in einem Audit-Log aufgezeichnet werden.
- Im Unterpunkt 10.1 wird sogar konkret gefordert, dass ein Prozess zu implementieren ist, der es ermöglicht, den Zugriff auf Systemkomponenten – insbesondere

nur selten oder sogar nie geändert werden. Der Grund ist klar: Die Passwörter werden von mehreren Admins benötigt, es ist hier von generischen Benutzerkonten die Rede wie z.B. Root, System, Enable oder SAP. Wenn überhaupt werden deren Passwörter manuell verwaltet und eine regelmäßige Änderung ist mit einem erheblichen zeitlichen Aufwand verbunden.

Identische Passwörter oder solche, die nie geän-

Nutzung von privilegierten Accounts zu jeder Zeit reglementiert und überprüft werden.

Abgesehen von den Administratoren-Passwörtern werden auch die Software oder Application Accounts vielfach vernachlässigt, das heißt die in Anwendungen, Skripten oder Konfigurationsdateien eingebetteten Passwörter. Auch hier können die vorgeschriebenen Änderungsintervalle nicht eingehalten werden, weil der Aufwand dazu in

keinem Verhältnis steht. Noch dazu liegen die Kennwörter meistens im Klartext vor und sind damit oft einer großen Anzahl an Usern wie Systemadministratoren und Entwicklern zugänglich. Auch dies entspricht nicht den Anforderungen des PCI-Standards. Auch hier ist eine Lösung gefragt,

die Klartext-Passwörter in Anwendungen eliminieren kann und die automatische Verwaltung und Änderung solcher Application Accounts sicherstellt.

Über den Autor:

Jochen Koehler hat in den vergangenen 10 Jahren für verschiedene IT-Sicherheitsberatungsunternehmen gearbeitet und sich dabei auf die Einführung innovativer Lösungen im deutschsprachigen Markt fokussiert. Seit 2008 verantwortet er das Business Development für CyberArk in Deutschland, Österreich und der Schweiz.

Weitere Informationen: www.cyber-ark.com



Unternehmensinformation



CyberArk Software ist der führende Anbieter von Lösungen für Privileged Identity Management (PIM) zur sicheren und nachvollziehbaren Verwaltung von administrativen Accounts. Mit dem Enterprise Password Vault werden die sensiblen Zugänge zu IT-Systemen automatisch, regelmäßig und konform zur Security Policy geändert und nur noch berechtigten Personen zur Verfügung gestellt. Auch die bislang häufig vorzufindenden Klartext-Passwörter in Anwendungs-Code können hierüber abgestellt werden. Die detaillierte, revisionssichere Protokollierung der Passwortnutzung entspricht dabei den Anforderungen externer Prüfungen sowie gängigen Compliance Vorgaben.

Im Sensitive Document Vault können CyberArk Kunden außerdem die sensibelsten Informationen ihres Unternehmens schützen, z.B. in den Bereichen Personal, Finanzen, Forschung, Revision oder Vorstand. Der Zugriff wird ähnlich wie bei einem physikalischen Safe stark reglementiert (z.B. 4-Augen-Prinzip) und protokolliert.

Aus der Praxis:

Im Gespräch mit PCI-Auditor Albrecht Dürr zum Thema Passwort-Management

Herr Dürr, wo treten besonders häufig Probleme mit dem Passwort-Management auf?

Gemessen an den üblichen Industriestandards sind die Anforderungen des PCI DSS an Passwortlänge, Komplexität oder Passworthistorie nicht allzu hoch – trotzdem bereitet die Einhaltung dieser Minimalanforderung vor allem denjenigen Kunden Probleme, die Legacy Systeme betreiben, deren Grundsteinlegung deutlich vor dem Jahrtausendwechsel erfolgt ist.

Was genau verursacht diese Probleme?

Häufig lassen sich auf solchen Systemen Passwortlängen von 7 Zeichen nicht verwirklichen oder die Erzwingung von Passwörtern mit numerischen und alphanumerischen Zeichen ist nicht möglich. An eine Passworthistorie – PCI DSS fordert, dass die letzten vier Passwörter nicht wieder verwendet werden können – haben die damaligen Entwickler oftmals nicht gedacht.

Müssen die Kunden also das komplette System erneuern?

Nein, auch wenn sich die Systeme nicht mehr upgraden lassen, gibt es mehrere Lösungen, um nicht gleich komplette Systeme erneuern zu müssen und trotzdem die PCI Compliance zu erlangen.

Was also raten Sie Ihren Kunden?

Der Einsatz eines Terminalservers enthebt einen gleich einer ganzen Menge von Problemen: Hiermit hat man die Chance, die Authentifizierung auf weitere Systeme wie Domäne oder LDAP zu verlagern, was wiederum den PCI-Anforderungen genügt. Ein zusätzlicher Vorteil kann hier auch das sogenannte Single Sign On sein, bei dem sich die Benutzer dann nur ein einziges Passwort merken müssen. Dies gilt gleichzeitig auch für die Zielapplikation. Gerne wird diese Lösung auch dann verwendet, wenn das eigentliche Zielsystem kein Auditlogging von administrativen Tätigkeiten an Bord hat. Hier loggt der Terminalserver dann alle administrativen Aktionen mit.



Relativ neu auf dem Markt sind auch sogenannte Identity Access Management Tools. Hierbei handelt es sich im Wesentlichen um eine Anwendung, die als Mittlerschicht zwischen Anwender und Zielapplikation fungiert. Sie steuert das gesamte Authentifizierungsprozedere und legt die Passwortpolicy fest. Natürlich lässt sich auch dieses System in eine vorhandene Domäne oder LDAP einbinden. Ein zusätzlicher Vorteil besteht darin, dass sich Identity Access Management Tools auch den Anforderungen eines Passwortwechsels nachkommen: Nach spätestens 90 Tagen wechselt das System automatisch das Authentifizierungspasswort des Systemusers in Richtung Zielsystem aus, ohne dass sich jemand darum kümmern muss. Ein genügend kryptisches Passwort wird in einem sicheren Speicher gehalten, falls doch einmal alle Stricke reißen und der Admin sich manuell einloggen muss. Denn gerade hier versagen oftmals sowohl manuelle Prozesse als auch Terminalserver.

Haben Sie einen Lösungsfavoriten?

Nein, eine generelle Favoritenempfehlung lässt sich nicht geben. Wie immer bieten beide Lösungen Vor- und Nachteile. Welche Lösung für welchen Kunden passt, hängt stark von den Startbedingungen und den Kundenerwartungen ab.

Prinzipiell können beide Lösungen die PCI-Anforderungen bezüglich des Passwortmanagements bedienen. Wer es bequemer mag, greift eher zu dem moderneren Identity Access Management Tool. Für den Terminalserver spricht eher der günstigere Preis, bei dem man nicht außer Acht lassen sollte, dass durch das Customizing bei der Inbetriebnahme und dem laufenden Betrieb höhere personelle Aufwände bestehen.

Herr Dürr, vielen Dank für das Gespräch!
Die Fragen stellte Christina Wolf.

Über den Auditor:

Der studierte Nachrichtentechniker blickt auf 16 Jahre Berufserfahrung im technischen Bereich zurück. Seit 1998 liegt sein beruflicher Schwerpunkt in der IT-Sicherheit, insbesondere im Key und Security Management. Vor seinem Wechsel zur Acertigo AG verantwortete er zuletzt als Security Officer die IT-Security für Westeuropa eines amerikanischen Zahlungsdienstleisters. Mit PCI beschäftigt Albrecht Dürr sich seit Etablierung des Standards im Jahre 2004. Als Auditor berät er Acertigo-Kunden und führt Vor-Ort-Audits durch.



News Ticker

+++ Best Practice für Data Field Encryption von Visa Europe +++

Visa Europe hat im Herbst ein Dokument veröffentlicht um eine Hilfestellung zu diesem Thema zu leisten, wie aus Sicht von Visa Data Field Encryption als Best Practice umgesetzt werden kann. Das Dokument richtet sich in erster Linie an Anwender und Entwickler von Systemen und Lösungen für Zahlungsterminals, Kassensysteme, zentrale Transaktionsserver in Unternehmen, sowie im

Processing. Das Ziel ist die Festlegung von end-to-end Verschlüsselungsmethoden entsprechend internationaler Standards.

Dieses Dokument finden Sie auch auf unserer Webseite über den nachfolgenden Link:

<http://www.acertigo.com/docs/Visa-BP-DFE.pdf>

+++ PED heisst jetzt PTS +++

Der bisher unter dem Namen PIN Entry Device (PED) bekannte Standard heißt nun PIN Transaction Security (PTS). Der PTS Standard legt die Anforderungen an Devices wie POS-Terminals und Hardware Security Module fest.

Auf den Seiten des PCI Councils finden Sie alle aktuellen Dokumente zu PTS unter diesem [Link](#).

+++ Informationen vom PCI Community Meeting in Prag +++

- Die Folgekosten einer Kompromittierung können ohne weiteres das 20-fache der Kosten für die Erreichung der PCI Compliance betragen.
- Vierteljährliche Schwachstellen-Scans müssen innerhalb von 30 Tagen abgeschlossen werden. Dies bedeutet, dass Re-Scans nur in diesem Zeitraum möglich sind. Danach wird dieser vierteljährliche Schwachstellen-Scan mit dem entsprechenden Ergebnis compliant oder non-compliant abgeschlossen.
- Händler welche für den Fragebogen C oder D klassifiziert sind, müssen externe Schwachstellen-Scans durchführen.
- Bei der Nutzung von Virtuellen Terminals (Softwareterminals) ist der Fragebogen C oder D relevant.

Impressum

Acertigo AG
Wilhelmsplatz 8
70182 Stuttgart (Germany)
+49 (0)7 11/6 20 30-300
Sitz Stuttgart
HRB 724100, Amtsgericht Stuttgart
Umsatzsteuer-Identifikationsnummer
gemäß § 27 a Umsatzsteuergesetz:
DE 813211856

Vorstand

Ralph Wörn
Dr. Stephan Engelke

Redaktion und Kontakt:

Christina Wolf
christina.wolf@acertigo.com



Hinweise zum Copyright

Die Inhalte dieser Publikation sind urheberrechtlich geschützt. Ohne schriftliche Genehmigung der Acertigo AG dürfen sie in keiner Form verarbeitet oder vervielfältigt werden. Alle Rechte, auch die der Übersetzung, sind vorbehalten.