MT AG

business by integration

Existiert Ihr Security Konzept auch nur auf dem Papier? Teil 2

Warum werden viele Security Konzepte nur unzureichend umgesetzt?

Ralph Baumbach

München, den 19.05.2015

Security Konzept, nur auf dem Papier?

- Die Kategorien
- Die Hindernisse
- Die Ursachen
- Lösungsansätze
- Methodik
- Beispiele
- Hilfsmittel und Prozesse
- Zusammenfassung

MT AG

Security Konzept, nur auf dem Papier?

Die Kategorien

- Die Schubladen-Konzepte

  Das Sicherheitskonzept wird nicht umgesetzt

- Die Potemkinschen Dörfer

  Die Probleme werden nur oberflächig gelöst (Außenwirkung zählt)

- Die Ausgehöhlten

  Die Umsetzung des Sicherheitskonzeptes erfolgt mit zu vielen Ausnahmen

- Die Soliden

  Das Sicherheitskonzept entspricht im Umfang und Inhalt der Bedrohungslage

MT AG

Security Konzept, nur auf dem Papier?

Mögliche Security Kategorien

Sicherheit in Bezug auf:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Nachvollziehbarkeit

Daten bez. Vertraulichkeit können in vier Stufen eingeteilt werden:

- Öffentlich
- Nur für den internen Gebrauch
- Geheim (Daten sind vertraulich zu behandeln)
- Streng Geheim

Security Konzept, nur auf dem Papier?

Die Hindernisse

- Kein Management Focus (Management Attention)

  “Die Ampel ist grün”

- Fehlende Resourcen

  Wer trägt welche Kosten, wer trägt welche Aufwände

- Fehlende Akzeptanz
  - Zu starke Einschränkungen
  - Unvereinbarkeit von Zielen (“Es darf sich nichts ändern!”)

MT AG

Security Konzept, nur auf dem Papier?

Die Ursachen

- Die Firmen sind Audit getrieben
  - Das Ampel-Denken
  - Schnelle Lösung für isolierte Probleme
    - Auswirkungen auf das Gesamtkonzept werden nicht berücksichtigt
    - Keine Nachhaltigkeit
- Der Hundert Prozent Anspruch
- Die Verallgemeinerung
- Fehlende Akzeptanz
  - Beteiligte werden nicht eingebunden oder deren Interessen nicht berücksichtigt
- Die Primärziele sind nicht bekannt
  - Abstrakte Ziele
  - Ziele berücksichtigen nicht die Gegebenheiten

MT AG

Security Konzept, nur auf dem Papier?

Die Ursachen: Der Hundert Prozent Anspruch / die Verallgemeinerung

- Keine Gewichtung des Gefährdungspotentials
- Keine Berücksichtigung der Gegebenheiten
- Mangelnde Kommunikation
- Kompromisslose Ziele

Typisch bei von Zentralabteilungen vorgegebenen Konzepten

MT AG

Security Konzept, nur auf dem Papier?

Lösungsansätze

- Management Attention erhalten
  - Konkrete Vorfälle nutzen
  - Darstellung des Ist/Soll Zustandes nicht als Ampel
  - Roadmap
- Andere Fachabteilungen einbinden
  - Wer sind die Stakeholder und welche Interessen haben diese?
  - Unterschiedliche Sichtweisen (z.B. beim Gewichten) berücksichtigen
  - Bessere Kommunikation
  - Kompromissbereitschaft
- Abschätzung des Gefährdungspotentials in Abhängigkeit der Gegebenheiten vornehmen
- Mit leicht umsetzbaren Projekten, die große Wirkung erzielen, beginnen

MT AG

Security Konzept, nur auf dem Papier?

Das Anforderungs-Triangle

MT AG

Security Konzept, nur auf dem Papier?

Maßnahmen

- Konzept Mapping
  - Ein konkrete Gegenüberstellung des Ist-Zustandes eines oder weniger Syteme mit dem Soll nach dem Security Konzept
- Konkrete Risikoabschätzung für die geschäftskritischen Systeme
  - Welche Gefahren existieren
  - Wie hoch ist das Risiko
  - Wie hoch ist der zu erwartende Schaden
- Kosten/Nutzen Abschätzung für einzelne Maßnahmen
  - Wie wahrscheinlich kann der Schaden vermieden werden
  - Welche Kosten und welche Aufwände
  - Wer muss welche Kosten und Aufwände tragen

Security Konzept, nur auf dem Papier?

Beispiel: Konzept Mapping

Init.ora /Spfile Parameter	Empfehlung	Anmerkungen	DB1	DB2	DB3
_TRACE_FILES_PUBLIC	FALSE	Trace Files enthalten unter anderem auch sensitive Daten (Werte aus Tabellen). Ein Zugriff für alle sollte daher unterbunden werden.	FALSE	TRUE	TRUE
REMOTE_OS_AUTHENT	FALSE	Eine Authentifizierung durch das Betriebsystem kann leicht gefälscht werden und sollte daher nicht genutzt werden. Anders sieht das aus, wenn ein zentrales Authenifizierungssystem zum Einsatz kommt.	TRUE	TRUE	TRUE
REMOTE_OS_ROLES	FALSE	Dito	TRUE	TRUE	TRUE
AUDIT_TRAIL	OS, DB oder DB_extended	Hier ist OS in Verbindung mit Syslog vorzuzuiehen	NONE	NONE	NONE
OS_AUTHENT_PREFIX	Null	Für REMOTE_OS_AUTHENT, sollte nicht verwendet werden.	OS$	OS$	OS$
OS_ROLES	FALSE	Dito	TRUE	TRUE	TRUE
UTL_FILE_DIR	„ „	Ein alter Mechanismus um auf Files zugreifen zu können.	„/u01/app/oracle/data	„“	„*“
SQL92_SECURITY	TRUE	Erhöhte Sicherheit durch SQL 92 Standard	TRUE	TRUE	TRUE
O7_DICTIONARY_ACCESIBILITY	FALSE	Dictionary Zugriffe nach Oracle 7 sind unsicher und sollten daher nicht genutzt werden	FALSE	TRUE	FALSE
AUDIT_SYS_OPERATIONS	TRUE	Auditierung aller Operationen des Users SYS	NONE	NONE	TRUE

MT AG

Security Konzept, nur auf dem Papier?

Risikoabschätzung

Konkrete Risikoabschätzung für die geschäftskritischen Systeme:

- Risiko
  - Welche Gefahren existieren
  - Wie hoch ist das Risiko
  - Wie hoch ist der zu erwartende Schaden

- Welche Maßnahmen sind möglich
  - Um das Risiko zu vermeiden oder zumindestens zu senken
  - Um den zu erwartende Schaden zu begrenzen

MT AG

Security Konzept, nur auf dem Papier?

Kosten/Nutzen Abschätzung

Für die erfolgversprechensten Ansätze eine Kosten/Nutzen Abschätzung:

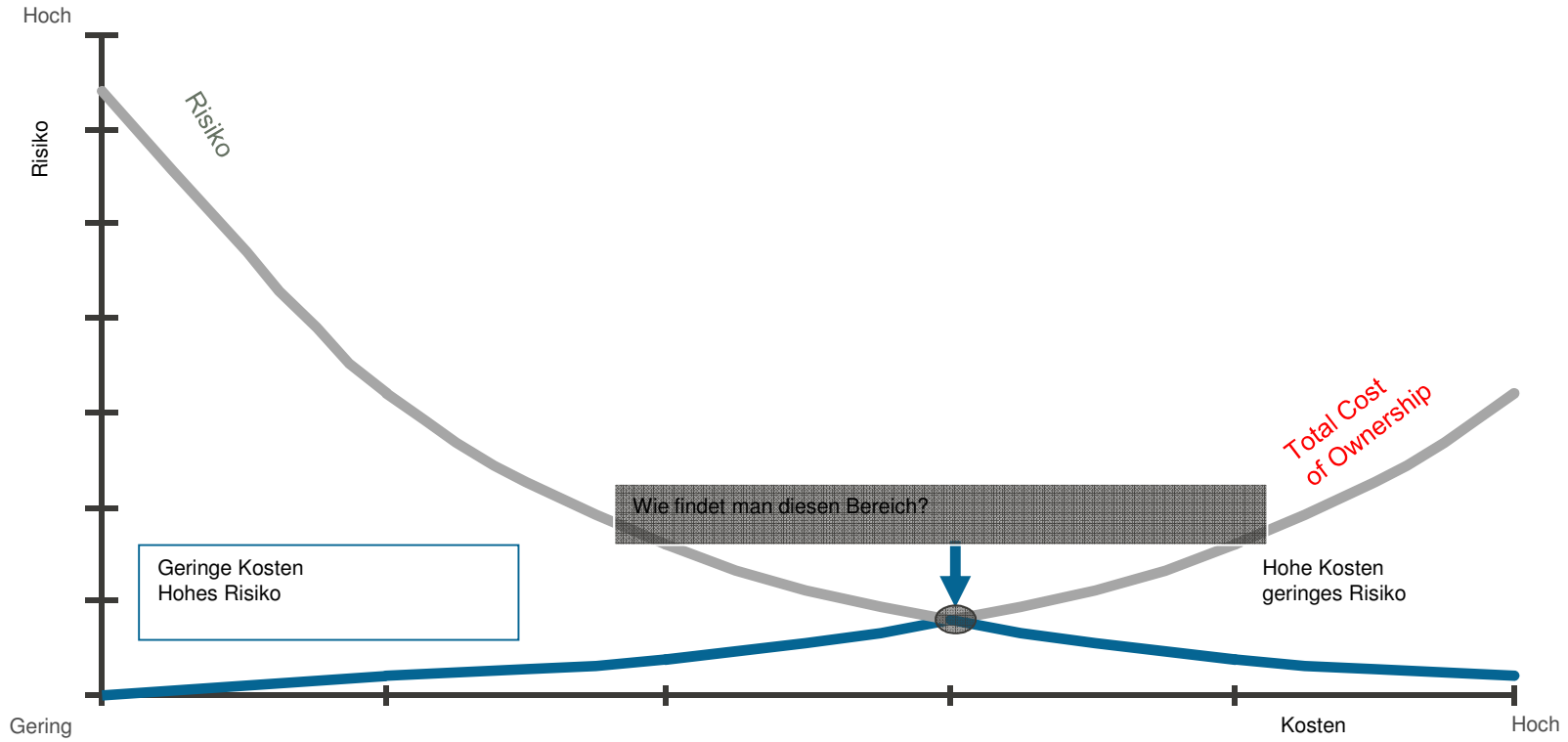
- Nutzen Abschätzung
  - Wie wahrscheinlich kann der Schaden vermieden werden oder
  - Bezugsgröße Schadenswahrscheinlichkeit und Schadenshöhe ermitteln (z.B. Punktesystem)

- Aufwand und Kostenabschätzung:
  - Welche Kosten und welche Aufwände
  - Wer muss welche Kosten und Aufwände tragen

MT AG

Security Konzept, nur auf dem Papier?

Risiko vs. Kosten



MT AG

Security Konzept, nur auf dem Papier?

- Authentifizierung
  - Trennung Technische Accounts und Personalisierte Accounts
  - Account-Management
- Autorisierung
  - Separation of Duty
  - Rechte und Rollen
- Zugriffskontrolle
  - Role Based Access Control vs. Factor Based Access Control
- Überwachung / Auditierung
  - Schnittstellen

MT AG

Security Konzept, nur auf dem Papier?

Methoden

- Datenklassifizierung
- Methoden der Auwirkungs
  - Netzplan
- Scoring
- Roadmap

MT AG

Security Konzept, nur auf dem Papier?

Methodik

- Management und alle Beteiligten (Stakeholder) einholen
  - Akzeptanz
  - Bereitschaft mitzuarbeiten
  - Bereitschaft Veränderungen mitzutragen
- Primärziel definieren
- Randbedingungen klären
  - Organisatorisch
  - Technisch
- Risiko- und Datenmanagement
- Zwischenziele und Anschlussprojekte definieren

MT AG

Security Konzept, nur auf dem Papier?

Methodik

- Datenmanagement und Klassifizierung
  - Wo entstehen die Daten und wer sind die Eigentümer?
  - Wo und wie werden diese genutzt?
  - Klassifikation nach Vertraulichkeit, Integrität und Verfügbarkeit
- Risikobewertungen
  - Einfaches Punktesystem
  - Common Vulnerability Scoring System (CVSS) Ansatz
- Module: Lösungsansätze, die bei entsprechenem Gefährdungspotential angewendet werden können
- Alternativ-Lösungen
- Ergebnisdarstellung

Security Konzept, nur auf dem Papier?

Methodik

Ergebnisdarstellung:

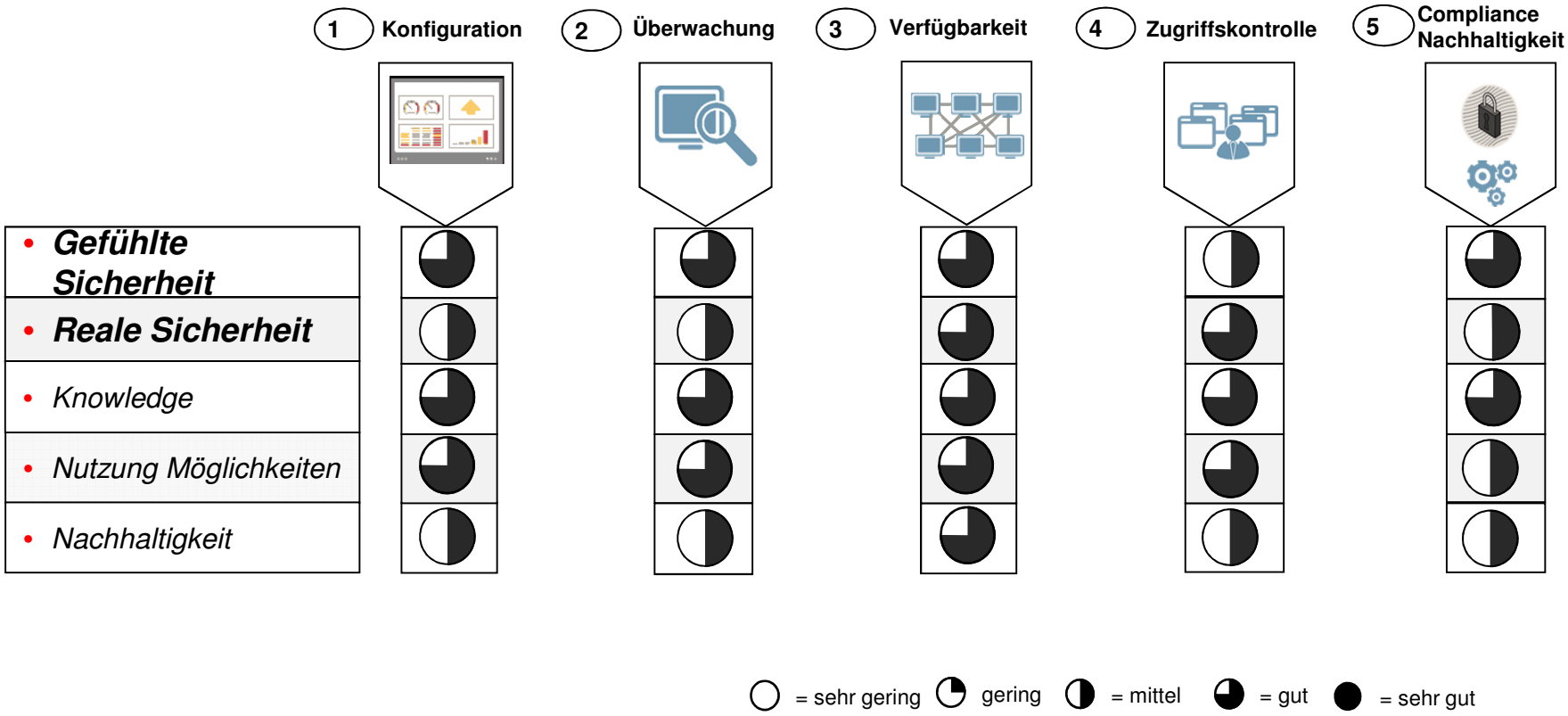
- Keine Ampeln

- Balkenfortschrittsdiagramm
- Scorecard
- Netzdiagramm
- Reifegrad

MT AG

Security Konzept, nur auf dem Papier?

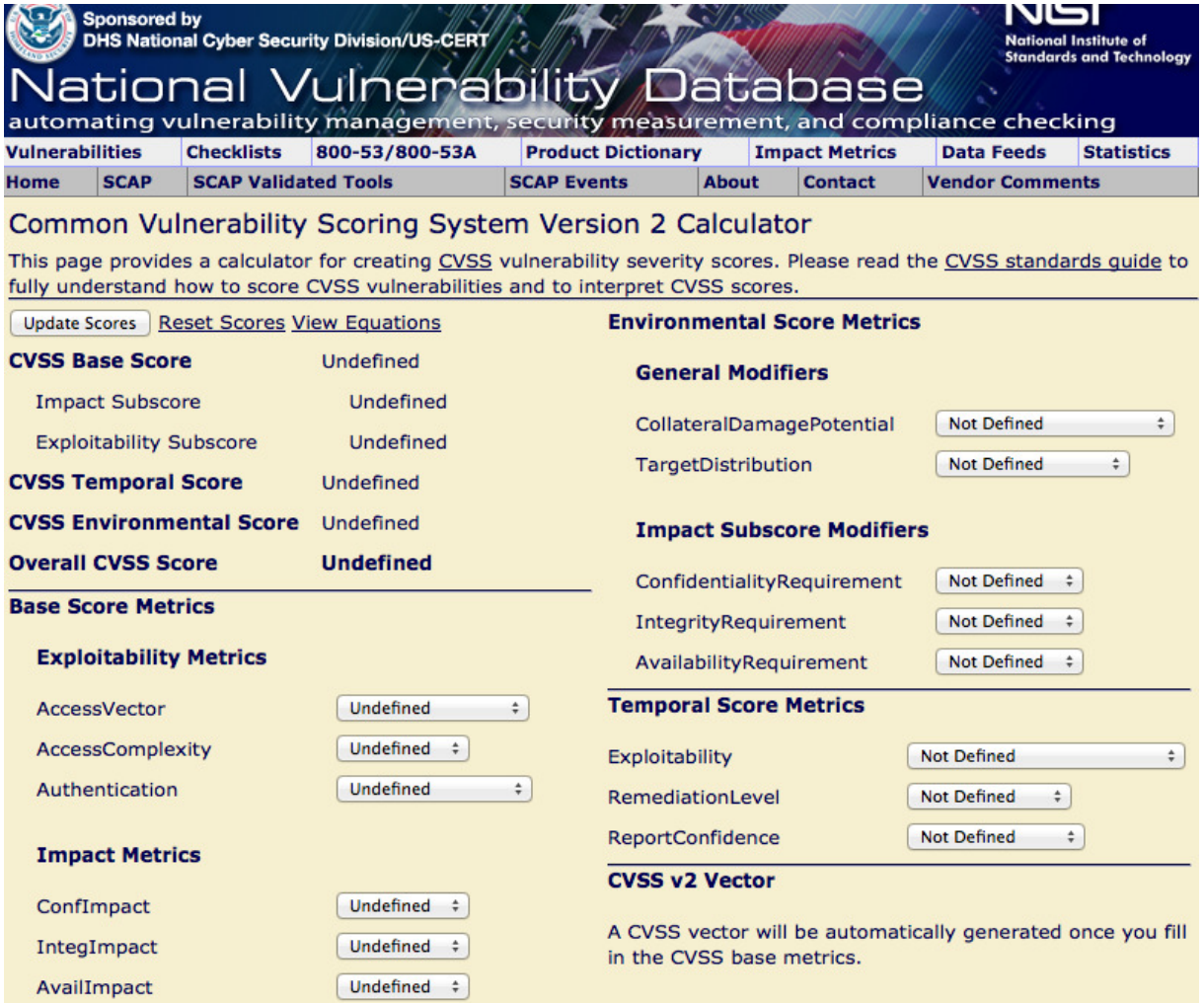
Reifegrad



MT AG

Security Konzept, nur auf dem Papier?

NIST Common Vulnerability Scoring System (CVSS) Calculator



MT AG

Security Konzept, nur auf dem Papier?

Separation of Duty

Was ist erforderlich?

- Rechte passen nicht zu den Business Funktionen
  - Klare Aufgaben und Zuständigkeiten
  - Einfaches Account-Management
- Rechteakumulierung
  - Einfaches Rollen-Management
- Technische Accouts
  - Strikte Trennung von Technischen Accounts und Mitarbeiter-Accounts
  - Technische Accounts sind beschränkt auf den speziellen Einsatzbereich
- Objektowner
  - Ein Account nur für die Business-Objekte

Security Konzept, nur auf dem Papier?

Separation of Duty

Funktions-Rollen rund um die Datenbanken

- Datenbank Administration
- Account Management (User Provisionierung)
- Security-Management
- Applikationsbetreuung (“Applikations-DBAs”)
- Applikations-Objekt-Eigentümer
- Applikationsuser (Endanwender oder Shared Pool Account)

- Server Administration
- Storage Management
- Backup Management

MT AG

Security Konzept, nur auf dem Papier?

Separation of Duty

Hindernisse:

- Unklare Aufgabenteilung
  - Funktionen nicht klar beschrieben
  - Nicht klar, welche Funktionen getrennt werden müssen
- Fürstentümer
  - Aufgaben werden nicht ohne Widerstand abgegeben
- Anforderungen ändern sich schnell
  - Z.B. Virtualisierung (PDBs)

Security Konzept, nur auf dem Papier?

Audit

“Da schalten wir mal das Audit der Datenbank ein”

- Was Auditieren? Wie? (Oracle internes Auditing vs. Third Party Systeme)
- Speicherung
- Zentralisierung, Anbindung an Third Party System
- Sicherheit der Audit Daten
- Aggregierung
- Reports
- Warehouse Prozesse
- Daten anderer Quellen (Enrichment)
- Archivierung
- Housekeeping

MT AG

Security Konzept, nur auf dem Papier?

Hilfsmittel / Prozesse: Ausschnitt aus allgemeine Security Richtlinien

Bereich	Empfehlungen
Applicationen mit Datenbank Zugriff	Es muss überprüft und kontrolliert werden, welche Applikationen auf welche Datenbanken Zugriff haben.
Zugriff auf Produktionsdatenbanken	Datenbank Zugriffe zwischen Entwickungs- und Testdatenbanken auf der einen Seite und Produktion auf der anderen Seite müssen unterbunden werden. Dieses gilt vor allen Dingen auch für Datenbank Links.
Zugriff auf Produktionsdaten durch Import oder Database Cloning	Sollten Datenbanken oder Teile von ihr in den Entwicklungs- oder Testbereich überführt werden, so müssen alle sensitive Daten entfernt oder maskiert werden, bevor die Entwickler oder Tester Zugriff erhalten. Alle Passwörter von importierten Usern müssen geändert werden.
User Rechte	Eine Überprüfung der Rollen und Rechte auf den Test- und Entwicklungsdatenbanken muss erfolgen, um zu verhindern, dass User mit vielen Rechten diese nicht in der Produktion erhalten.
Standort der Produktionsdatenbank	Entwicklung und Test sollten möglichst auch physisch von der Produktion getrennt werden.
Netzwerk Segmente von Produktion und Entwicklung	Wenn möglich sollte die Produktion ein eigenes von Entwicklung und Test getrenntes Netzwerk-Segment nutzen.
Überwachung von Entwicklungstätigkeiten in Produktionsumgebungen	Direkte Entwicklungen in Produktionsdatenbanken sollten nicht stattfinden. Anzeichen von Entwicklungsaktivitäten sollten beobachtet und bei Bestätigung unterbunden werden.
Zugriff von Entwicklern auf Produktionsdatenbanken	Entwickler dürfen keinen direkten Zugriff auf Produktionsdatenbanken erhalten. Bevor eine Datenbank in Produktion genommen wird müssen alle Entwickler-Accounts entfernt werden.
Reporting Tool Interface und Authentifizierung	Jeder Remote-Zugriff auf den Datenbank Server muss überwacht werden, dieses kann durch eine Application-Level Firewall realisiert werden.
Schutz gegen SQL-Injection	Validierung der Input-Daten sollte in der Applikation erfolgen. Ggf. sind weitere Maßnahmen gegen SQL-Injection (z.B. SQL-Firewall) nötig.

MT AG

Security Konzept, nur auf dem Papier?

Hilfsmittel nutzen / Prozesse schaffen

- Eine Systembestands-Datenbank (Asset-DB) mit Informationen über
  - Alle Applikationen
  - Alle Datenbanken
  - Die Schnittstellen untereinander
- Prozesse müssen definiert werden für
  - Das Anlegen eines Test-Systems
    - Hier werden bereits oft die Grundlagen für spätere Probleme in der Produktion gelegt
  - Das Überführen eines Systems in die Produktion
- Überprüfung und Überwachung von
  - Accounts
  - Rechte
  - Schnittstellen

MT AG

Security Konzept, nur auf dem Papier?

Security Konzepte, was ist erforderlich?

- Übergreifendes Security Konzept
  - Database Security ist zu wenig
- Schutz über alle Layer
  - Z.B. auf Protokoll- und Datenbank-Ebene
- Auditierung und Logging der wichtigen Ereignisse
  - Sichtbarkeit der Vorkommnisse inklusive Alarmierung
- Schutz gegen unberechtigten Zugriff in Echtzeit
- Reporting und Assessment der Regelverstöße
- Datenklassifizierung
- Management von Berechtigungen und Konfigurationen

MT AG

Security Konzept, nur auf dem Papier?

Zusammenfassung

- Security ist kein Produkt
- Es gibt keine hundertprozentige Sicherheit
- Die primären Ziele sollten definiert werden
- Abwägen von Aufwand und Nutzen
  (Bedarfsanalyse, Risikobewertung)
- Zielerreichung sollte messbar sein
- Kein Return-of-Investment für Security berechenbar
- Ein fortlaufender Prozess ist erforderlich
  “Stillstand ist Rückschritt”

MT AG

Fragen?

MT AG

MT AG

business by integration

Vielen Dank.

MT AG

Balcke-Dürr-Allee 9
40882 Ratingen

Telefon: +49 (0) 21 02 309 61-0
Telefax: +49 (0) 21 02 309 61-10

E-Mail: info@mt-ag.com
www.mt-ag.com