

Schwachstellenmanagement als Sicherheitsmaßnahme im Sicherheitsmanagementprozess



Christian Husemeyer, Dimension Data Germany

13. September 2011



Referent:

- Christian Husemeyer
- Security Consultant
- Dipl.-Ing. (FH), M.Sc.
- ISO 27001 Auditor

Unternehmen:

- Dimension Data Germany AG & Co.KG
- 6 Standorte in Deutschland
- ca. 400 Mitarbeiter
- Weltweit über 12.300 Mitarbeiter in 49 Ländern
- Sicherheitszertifiziert nach ISO/IEC 27001

Was ist Schwachstellenmanagement?

- **Kein** Penetrationstest
- **Kein** Patchmanagement
- Schwachstellenmanagement ist eine präventive Sicherheitsmaßnahme zur
 - › Identifizierung,
 - › Priorisierung
 - › und Behebung
- von Schwachstellen durch die Benutzung **automatisierter Scans**
- Zentrales Ziel:
 - › **Überblick** über den aktuellen Sicherheitsstatus der Organisation (Schwachstellen)
 - › somit das Schaffen von **Transparenz**

Was ist Schwachstellenmanagement? II

- Implementierungsansätze
 - › Lokale Scan-Server bzw. –Appliances
 - » Open-Source-Lösungen
 - » Kommerzielle Lösungen
 - › Software as a Service (Saas)
- Vorgehensweise
 - › “Assetscan” (Bestandsaufnahme)
 - › Schwachstellenscan
 - › Auswertung und Maßnahmendefinition
 - › Umsetzung von Gegenmaßnahmen
 - » Integration mit Ticketsystem
 - » Folgescans zur Erfolgskontrolle

Ist das überhaupt relevant für mich?

Beispiele weit verbreiteter Schwachstellen

Betriebssystem-Schwachstellen

Sicherheitsupdates nicht eingespielt oder inaktiv (fehlender Neustart, Installationsproblem...), unsichere **Konfigurationen** (nicht benötigte Dienste o. Applikationen, falsche Rechtevergabe)

Datenbank-Schwachstellen

Fehlende Sicherheitsupdates, aktive **Testkonten**, administrative Konten mit schwachen **Passwörtern**

Webserver-Schwachstellen

Angriffsfläche für **SQL-Injections** und **XSS-Angriffe**, unsichere **Verschlüsselung** (schwache Algorithmen oder Zertifikate), unerkannte Kompromittierung (Folge: Drive-by-Downloads)

Schwachstellen auf Netzwerkkomponenten

Veraltete Software auf Netzkomponenten ermöglicht Angriffe, unauthorisierte **WLAN-Hotspots** gefährden Sicherheit des Netzes

Schwachstellen auf Client-Computern u. Notebooks

Fehlende oder fehlgeschlagene Sicherheitsupdates, nicht autorisierte Software, auf "Außeneinsätzen" **infizierte** Notebooks => Ausnutzung solcher Schwachstellen für Wirtschaftsspionage

ISMS-Anforderungen an Schwachstellenmanagement

Sowohl IT-Grundschutzkataloge, als auch native ISO 27001-Herangehensweise fordern einen bewussten, nachvollziehbaren Umgang mit Risiken/Schwachstellen.

- IT-Grundschutz
 - › M 2.282 Regelmäßige Kontrolle von Routern und Switches
 - › M 5.150 Durchführung von Penetrationstests
 - › M 5.141 Regelmäßige Sicherheitschecks in WLANs
 - › M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches
 - › ...
- ISO 27001
 - › 12.6.1 Kontrolle technischer Schwachstellen
 - › 15.2.2 Prüfung der Einhaltung technischer Vorgaben
- Grundlage aller Standards und Vorgehensweisen:
 - › **Um Risiken bewerten und behandeln zu können, muss man sie zunächst kennen!**

Schwachstellen-Management innerhalb des ISMS

- Ein “sauber” implementiertes Schwachstellen-Management unterstützt bei der Umsetzung bzw. Überwachung vieler anderer ISO-Controls oder Grundschutzmaßnahmen!
- Etablierung als vollständiger Prozess, z.B. mit den folgenden Teilschritten:
 - Inventarisierung der vorhandenen IT-Ressourcen
 - Identifizieren von Schwachstellen in den vorhandenen IT-Ressourcen
 - Priorisierung der Schwachstellenbehebung
 - Behebung der Schwachstellen gemäß der ermittelten Relevanz
 - Prüfung der durchgeführten Maßnahmen



- **Schnittstellen und Abhängigkeiten**

- › ISMS setzt zur Maßnahmendefinition die Ermittlung und Bewertung von Risiken voraus
- › ISMS definiert den Rahmen und organisatorische Parameter
- › Schwachstellen-Mgmt. deckt Risiken auf und
 - › unterstützt bei Bewertung und Priorisierung
 - › Maßnahmendefinition auf Grundlage der Risikobewertung (u.a. Patchmanagement)
 - › Nach Umsetzung von Maßnahmen: schnelle Erfolgskontrolle
 - › Unterstützung von ISMS-Prozessen/Audits durch Automatisierung
 - › Regelmäßige, automatisierte Aktualisierung der Datenbasis hinsichtlich
 - » neu hinzugekommener IT-Systeme
 - » bestehender, bekannter und neuer Schwachstellen
 - » Effektivität der Gegenmaßnahmen und resultierendem Gesamtsicherheitsniveau

Ergebnis:

**Hohe Transparenz durch stets aktuelle, objektiv
überprüfbare Werte zu Standard-Konformität / Compliance**

Aktuelles Negativbeispiel

- DigiNotar (CA, u.a. von niederländischen Behörden genutzt): gehackt im Juli 2011
 - › Veraltete Software auf Webservern
 - › Keine Virens Scanner auf diesen und weiteren zentralen Servern
 - › Schwache Passworte in CA-Domäne
 - › Zentraler Zugriff über unsicheres Management-LAN
- Ironie am Rande: TEMPEST-Richtlinien wurden eingehalten!
- Zahllose weitere Beispiele belegen die Relevanz
 - › Neckermann
 - › REWE
 - › Sony
 - › u.v.m.

Projekt-Beispiel: Überprüfung von 25.000 IP-Adressen

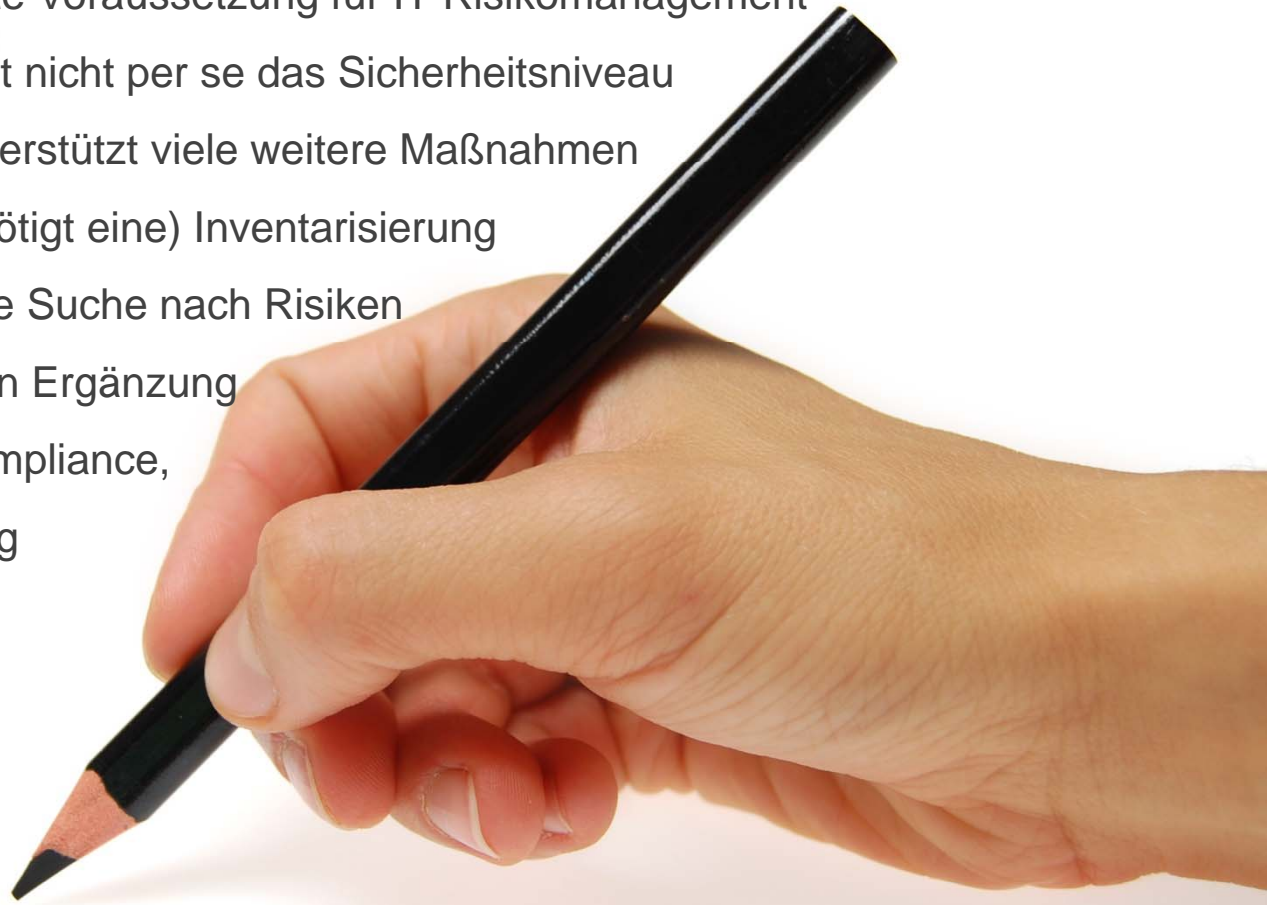
Konkrete Kundenanforderungen im Rahmen eines Projekts von Dimension Data Germany im Jahr 2011

- Planung, Implementierung und Betrieb eines Systems zum Schwachstellen-Management
- Design und Definition der Anforderungen an das Schwachstellen-Mgmt.
 - › Assetdefinition & Scan-Definition (Komponentengruppen, Geschäftsbereiche, Scans...)
 - › Benutzer-Definition (Rollen- u. Berechtigungskonzept, Authentisierungsmechanismen...)
 - › Definition der Anforderungen
- Durchführung von Scans
 - › „Rollout“ und Anpassung der Lösung
 - › Terminierung u. Koordinierung von Scans
 - › Konfiguration, Anpassung und Durchführung von Scans
 - › Klassifizierung u. Priorisierung von Ergebnissen
- Reporting und Unterstützung bei Maßnahmendefinition
- Prüfung auf Umsetzung der notwendigen Maßnahmen

Fazit

Was Sie bzgl. Schwachstellenmanagement “mitnehmen” sollten:

- Transparenz ist die wichtigste Voraussetzung für IT-Risikomanagement
- Schwachstellenmgmt. erhöht nicht per se das Sicherheitsniveau
- Implementierter Prozess unterstützt viele weitere Maßnahmen
- Unterstützt bei der (und benötigt eine) Inventarisierung
- Ermöglicht die automatisierte Suche nach Risiken
- Kein Pentest-Ersatz, sondern Ergänzung
- Ermöglicht Aussagen zu Compliance,
- die regelmäßige Überprüfung
outsourcter IT-Leistungen
- Automatisiertes Reporting



Fragen?

Vielen Dank für Ihre Aufmerksamkeit!

Kennen Sie Ihr IT-Risiko? Und wie lautet die Lösung?

Kennen Sie Ihre IT-Infrastruktur und alle vorhandenen Risiken?

- Sie haben eine Schatten-IT, auch wenn Sie es nicht glauben

Wie können Sie die Einhaltung von Vorgaben aus Richtlinien überprüfen?

- Von Vorgaben abweichende Systeme automatisiert erkannt werden
- Wichtig für Aufbau und Betrieb eines Internen Kontroll Systems (IKS)

Sind Sie zu anerkannten Standards und Frameworks konform (compliant)?

- Nachweise werden immer wichtiger für's tägliche Geschäft (Audits, Zertifizierungen)

Wie können Sie Ihren Patchprozess priorisieren und verifizieren?

- Patchmanagementsysteme sagen oft nicht die Wahrheit

Sind „Penetrationstests“ wirtschaftlich sinnvoll, effektiv und effizient?

- Ergebnisse sind Schnappschüsse, meist nur einmal pro Jahr und auf ausgewählte Ziele

Wie können Sie outgesourcete Systemumgebungen überprüfen?

- Blindes Vertrauen in die Einhaltung von SLAs ist keine Option

Was können Sie zur Reduzierung Ihres IT-Risikos unternehmen?

- IT-Risikomanagement ist zentraler Bestandteil des Unternehmens-Risikomanagements