Westfälische Wilhelms-Universität Münster

Das erste Security-Audit im ZIV

- Ergebnisse, Erfahrungen und Konsequenzen -

Thomas Rensing

Freitag, 12.01.2007

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

Westfälische Wilhelms-Universität Münster

Inhalt

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

Das Security-Audit an WWU und UKM
Ideen und Motivation

In Aller Munde:
Sicherheit in der IV
→ Stand der IV-Sicherheit von großer Bedeutung

Sicherheit:
Eindämmung der Risiken, sodass Restrisiko vertretbar
→ Risikoanalyse
→ Aufwandsabschätzung

→ **Security-Audit:**
Risikoanalyse durch Erfassung und Bewertung des Ist-Zustands der Sicherheit in der IV

3

Das Security-Audit an WWU und UKM
Ziele des Security-Audits

- ***Überprüfung*** des aktuellen *Restrisikos*
- ***Dokumentation*** des aktuellen *Restrisikos*
- ***Aufdecken*** von vorhandenen Sicherheitslücken
- ***Anhebung*** des Sicherheitsniveaus
- ***Sensibilisierung*** der Anwender für sicherheitsrelevante Aspekte

4

Das Audit-Verfahren im Detail
Datenerhebungsstrategie (1)

Datenerhebung auf Basis der Netzdatenbank
→ Systembasierte Erfassung

Datenerhebung durch ausgewählte Auditoren
→ Kein extra Fachpersonal (+)
→ Bewertung u.U. subjektiv (-)

Kategorisierung des Datenendgerätes bzgl.
- *Integrität und Vertraulichkeit*
- *Verfügbarkeit*

der Daten und Dienste

➔ **Risikoanalyse auf Basis der ermittelten Werte**

5

Das Audit-Verfahren im Detail
Datenerhebungsstrategie (2)

***Zweischrittige* Erhebung benötigter Daten:**

1. Fragebogen zur Ermittlung und Bewertung des Schutzbedarfs am IT-Endgerät

2. Fragebögen zur Ermittlung und Bewertung der Sicherheitsvorkehrungen
   - Umfang und Anzahl abhängig von (1.)
   - Schwerpunktmäßig IT-Endgerät

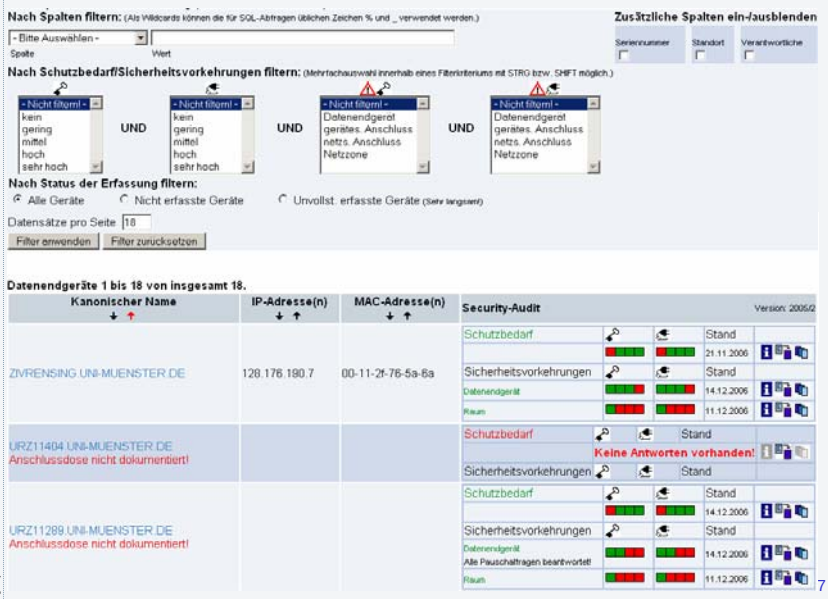
Risikoanalyse:
Vergleich von Schutzbedarfskategorie und getroffenen Sicherheitsvorkehrungen

6

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Fragenkataloge und Ergebnisse



ZENTRUM FÜR INFORMATIONSVERARBEITUNG

7

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Fragenkatalog zum Schutzbedarf (1)

Universeller Fragenkatalog:

- zu jedem Datenendgerät zu beantworten
- 8 Pauschalfragen
- 20 Detailfragen

→ **Ergebnisberechnung:** mind. 80 % Pauschal- **oder** Detailfragen „sinnvoll“ beantwortet

Themengebiete:

- Verstöße gegen Gesetze
- Beeinträchtigung der personellen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Finanzielle Auswirkungen

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

8

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Fragenkatalog zum Schutzbedarf (2)

Finanzielle Auswirkungen durch Verletzung der Integrität und Vertraulichkeit

7 **In welchem Umfang würde die *unbefugte Veränderung oder Veröffentlichung der Daten* auf dem betrachteten System finanzielle Folgeschäden verursachen?**

- Keine Angabe
- Finanzielle Folgeschäden sind auszuschließen.
- Geringe finanzielle Folgeschäden sind möglich.
- Mittel schwere finanzielle Folgeschäden sind möglich.
- Größere finanzielle Folgeschäden sind möglich.
- Schwer wiegende finanzielle Folgeschäden sind anzunehmen.

Diese Frage ist die übergeordnete Frage des siebten Abschnitts. Grundsätzlich ist eine Antwort zu dieser Frage ausreichend, wenn nicht bei den untergeordneten Fragen (7.x) deutlich abweichende Antworten (Zwei oder mehr Stufen!) gegeben werden müssen.

7.1 Welche Regressforderungen kann die **Veröffentlichung vertraulicher oder falscher Informationen** nach sich ziehen?

- Keine Angabe
- Regressforderungen sind auszuschließen.
- Regressforderungen sind unwahrscheinlich aber in minimalem Umfang möglich.
- Regressforderungen sind unwahrscheinlich aber in moderater Höhe möglich.
- Regressforderungen sind wahrscheinlich und in hohem Umfang zu erwarten.
- Regressforderungen sind wahrscheinlich und in sehr hohem Umfang zu erwarten.

7.2 In welchem Umfang können **Dritte durch Kenntnis der Daten auf dem betrachteten System** finanzielle Vorteile ziehen?

- Keine Angabe
- Finanzielle Vorteile sind auszuschließen.
- Finanzielle Vorteile für Dritte sind in geringem Umfang möglich.
- Finanzielle Vorteile sind in mittlerem Umfang möglich.
- Finanzielle Vorteile sind in hohem Umfang möglich.
- Finanzielle Vorteile werden in sehr hohem Umfang entstehen.

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Musterantworten zu Schutzbedarf und Sicherheitsvorkehrungen

Zweck:
vereinfachte Bearbeitung von „homogenen“ Endgeräten

→ 5 Standardmuster vordefiniert
→ Definition von eigenen Mustern möglich
→ Als Basis können andere Muster oder beantwortete Fragen-kataloge dienen

In Arbeit:
„Backtracking“ bei der Anwendung von Mustern

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Musterantworten zu Schutzbedarf und Sicherheitsvorkehrungen

Standardmuster des ZIV			
Arbeitsplatzrechner der Personalverwaltung Stand: 14.10.2005, 13:09 Uhr Zuletzt bearbeitet durch: stolze	Arbeitsplatzrechner mit Zugriff auf persönliches oder vertrauliches Datenmaterial, Ausfall nur sehr begrenzt tolerabel.		
Netzwerkdrucker mit hoher Verfügbarkeitsanforderung Stand: 14.10.2005, 13:09 Uhr Zuletzt bearbeitet durch: stolze	Netzwerkdrucker, bei dem ein Ausfall erheblichen Schaden verursachen würde, kein Ausdruck von persönlichem oder vertraulichem Datenmaterial.		
Server mit Standardfunktionen (Zugriff auf persönliche Daten) Stand: 01.06.2006, 09:22 Uhr Zuletzt bearbeitet durch: kampm	Eine **Verletzung der Integrität und Vertraulichkeit** der Daten hätte gravierende, nicht zu tolerierende Auswirkungen (z.B. Persönliche Daten) Ein vorübergehender Ausfall, in denen die Daten und Dienste nicht verfügbar wären, läge im Toleranzbereich und hätten keine gravierenden Folgen.		
Server mit Standardfunktionen (hohe Verfügbarkeit erforderlich) Stand: 14.10.2005, 13:09 Uhr Zuletzt bearbeitet durch: stolze	Hohe Verfügbarkeit der Daten und Dienste erforderlich, kein Zugriff auf personenbezogene oder vertrauliche Daten.		
Standardarbeitsplatzrechner Stand: 14.10.2005, 13:08 Uhr Zuletzt bearbeitet durch: stolze	Arbeitsplatzrechner ohne Zugriff auf vertrauliches Datenmaterial. Ein vorübergehender Ausfall hätte keine gravierende Folgen.		

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

11

Westfälische Wilhelms-Universität Münster

ISIDOR - Das Audit-Verfahren in der Praxis

Fragenkataloge zu Sicherheitsvorkehrungen (1)

Art und Umfang abhängig von Schutzbedarfskategorie!

Mögliche Fragenkataloge:

- Datenendgerät (Virenscanner, Betreuung,…)
- gerätes. Anschluss (Firewall, Redundanz der Netzw.-Interfaces,…)
- netzs. Anschluss (Redundanz des Anschluss‘, Flusskontrolle,…)
- Netzzone (Netzinfrastruktur: Subnetze, Gateways,…)
- Raum (z.B. Brandschutz, Klimaanlage, Einbruchsicherheit,…)

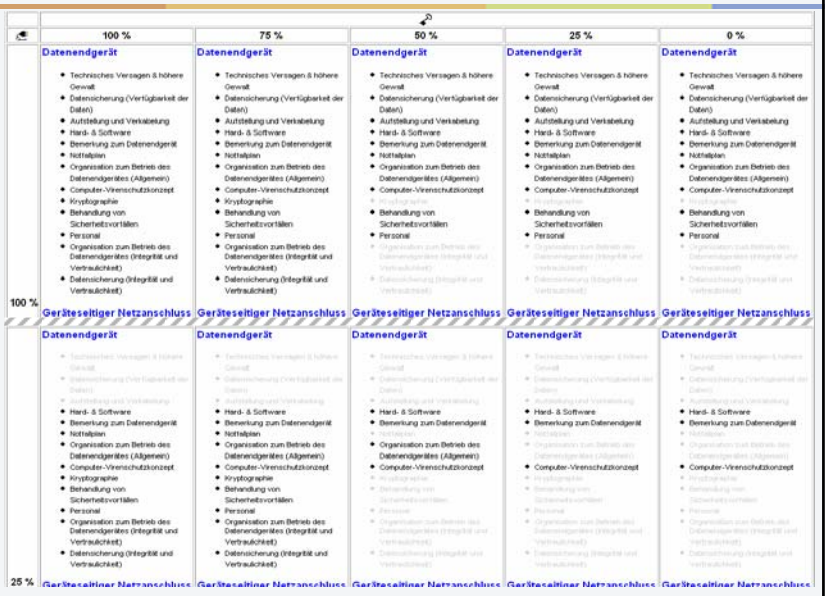
→Tabellarische Übersicht zeigt Fragenkataloge in Abhängigkeit vom Schutzbedarf

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

12

ISIDOR - Das Audit-Verfahren in der Praxis

Fragenkataloge zu Sicherheitsvorkehrungen (2)



ISIDOR - Das Audit-Verfahren in der Praxis

Auswertung der Ergebnisse

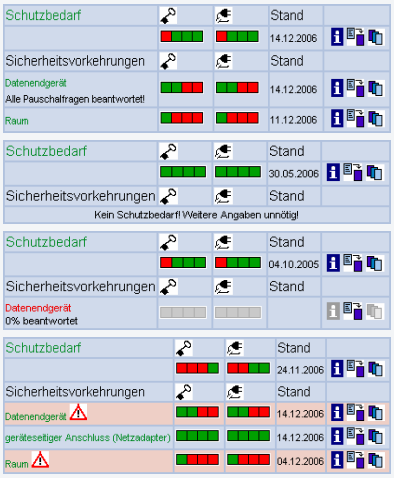
Basis:
Ermittelte Werte für Schutzbedarf und Sicherheitsvorkehrungen

Balken verdeutlichen ermittelte Werte

Kein Schutzbedarf!
→*Weitere Angaben unnötig*

Prozentsatz der beantworteten Fragen
→ *Link rot*

Sicherheitsdefizit (pauschal)!
→ *Tabellenzeile rot*
→ *Warndreieck*



ISIDOR - Das Audit-Verfahren in der Praxis
Die Onlinedokumentation

Zugriff auf Onlinedokumentation:
- „ i “: spezielle Informationen zum ausgewählten Themenbereich
- Direkter Link im Kopf einer jeden Webseite auf komplettes Handbuch

Inhalte der Onlinedokumentation:
- Ziele und Informationen zum Security-Audit
- Verfahrensweise und Handhabung des Online-Verfahrens
- FAQ – Häufig gestellte Fragen
- Glossar – Häufig verwendete Begriffe

Erfahrungen und Ergebnisse aus dem Security-Audit
„Das Audit in Zahlen“ (1)

Stichtag: 22.11.2006

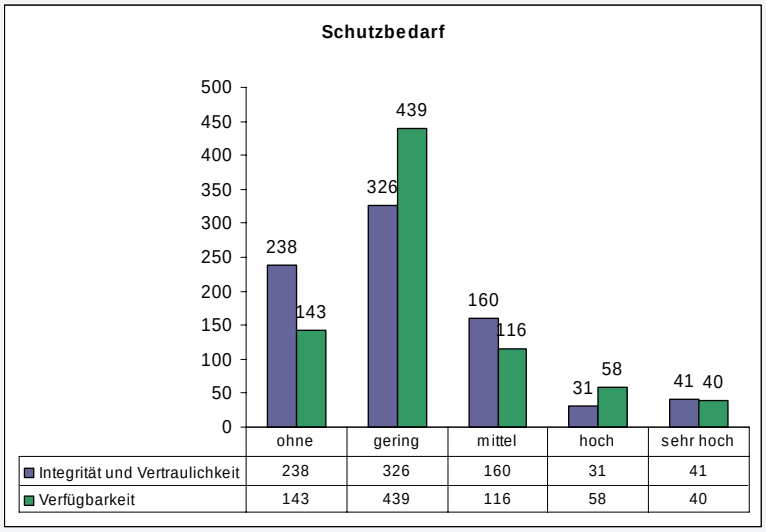
Zu evaluierende Systeme: 813

→*nicht* erfasst: 17
→*unvollständig* erfasst: 124
(maßgebliche Gründe:
- unzureichende Schulung der Auditoren
- Aufbau des Online-Verfahrens (korrigiert!)
- Bug im Berechnungsalgorithmus (korrigiert!))

Erfahrungen und Ergebnisse aus dem Security-Audit

„Das Audit in Zahlen“ (2)

Verteilung der Schutzbedarfskategorien:



Erfahrungen und Ergebnisse aus dem Security-Audit

Ergebnisse aus dem Security-Audit (1)

Real identifizierte Sicherheitsdefizite:

- Systeme mit mangelhaftem oder fehlendem Backupkonzept
- Systeme mit fehlenden Sicherheitspatches
- Systeme mit deaktivierten Firewalls
- Systeme mit veralteter Software
- Fehlende Betriebsvereinbarungen im Störfall (Virenbefall, Rechnerausfall,…)
- Nicht ausreichender Zugangsschutz zu Büros mit sensiblen Systemen (Sekretariatsrechner)
- z.T. kein übergreifendes Kryptokonzept vorhanden (USB-Token,…)

Erfahrungen und Ergebnisse aus dem Security-Audit

Ergebnisse aus dem Security-Audit (2)

Seiteneffekte auf Grund des Verfahrens:

- Konsolidierung der Datenbestände und Dokumentation
- Löschen von Karteileichen
- Identifikation von Daten und Diensten
- Identifikation von mangelhafter oder fehlender Dokumentation von Zuständigkeiten

➔ **(Sicherheits)Defizite oft schon während des Audit-Verfahrens oder unmittelbar danach abgestellt**

Erfahrungen und Ergebnisse aus dem Security-Audit

Erfahrungen aus dem Audit

Erfahrungen das Verfahren betreffend:

- z.T. Hilfestellungen in Form von Antwortprototypen nötig
- z.T. Ausweitung / Abänderung der Fragestellungen nötig
- Erweiterung der Funktionalität des Userinterfaces
- Erweiterung / Änderung des Bewertungsverfahrens

Erfahrungen die Durchführung betreffend:

- Ausführliche Schulung der Auditoren nötig (Vergleichbarkeit!)
- Minimale Zahl an Auditoren (Subjektivität!)
- Möglichst homogene zu bearbeitende Systemlandschaft oder nicht zu große Anzahl an Systemen pro Auditor (Aufwand!)

Fazit aus der Durchführung des Security-Audits

- ***Identifikation*** real existierender Sicherheitsmängel (Firewalls, fehlende Patches, veraltete Software…)
- ***Sensibilisierung*** von Nutzern für Sicherheitsrelevante Gesichtspunkte (Daten ⇔ Backup)

➔ **Erste Ziele des Security-Audits wurden erreicht.**

Roadmap für die Zukunft (1)

ZIV-Intern:

- Abstellen der identifizierten Mängel:
  - Sicherstellen, dass Patches eingespielt, Software up-to-date und Firewalls aktiviert sind
  - Fortsetzung der Netzstrukturierung
  - Einführung eines einheitlichen Kryptokonzepts (Ausstattung der Kollegen mit USB-Token, Konfiguration der Server)
  - Verbesserung des Zugangsschutzes zu Räumen mit sensiblen Systemen
  - Serviceprozeduren für den Störfall erstellen
  - Zuständigkeiten klären
- Erweiterung der Oberfläche für das Online-Verfahren

➔ **Erneute Auditierung der Systeme und Vergleich der Ergebnisse**

Roadmap für die Zukunft (2)

Außerhalb des ZIV:

- Präsentation der Ergebnisse / Erfahrungen
- Auswahl eines Pilot-Fachbereiches an der Uni
- Schulung der Auditoren
- Festsetzung von Fristen und Stichtagen
- Nach Ablauf: Auswertung der Ergebnisse
- …

Danke für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?