

Praktische Anwendung des IT-Grundschutzhandbuches auf einen WEB-Server des Fachbereichs Wirtschaft

Projektarbeit vorgelegt von: Patrick Lausch & Daniel von Berg im Fach „Netzwerksicherheit 1“

Aufgabenstellung

Die Aufgabe bestand darin, den Webserver des Fachbereichs Wirtschaft der Fachhochschule Brandenburg nach dem theoretischen Ansatz des IT-Grundschutzhandbuchs vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zu überprüfen.

Arbeitsansatz:

Als Ausgangspunkt unserer Untersuchung knüpften wir an eine Projektarbeit aus dem Wintersemester 2007/2008 an. Die Arbeit wurde im April 2008 eingereicht und war für uns, auf Grund ihrer Aktualität und Vorarbeit zur Thematik, in Teilgebieten hilfreich.

Der Versuch, mit dem Grundschutzhandbuch direkt zu arbeiten, scheiterte an der Unübersichtlichkeit und an der Größe des (Maßnahmen-)Kataloges von über 3000 Seiten. Maßgeblich für unsere Arbeit war das Open Source Tool „Verinice“, das durch seine logische Struktur und die unterteilte Ansichtweise auf einzelne Komponenten des IT-Grundschutzhandbuchs unsere Arbeit mit der Thematik erheblich vereinfachte.

Für die Untersuchung des Webservers wurden die folgenden Bausteine des BSI-Grundschutzkataloges eingesetzt:

- B 2.4 Serverraum
- B 2.7 Schutzschranke
- B 3.101 Allgemeiner Server
- B 3.102 Server unter Unix
- B 5.7 Datenbanken
- B 5.11 Apache Webserver

Auf Grund des enormen Umfangs unserer Untersuchungen, aber der zeitlichen Begrenzung, wurden insbesondere die Bausteine B 2.4, B 2.7, B 3.101 und B 3.102 betrachtet. Der Baustein 5.7 (Datenbanken) wurde ausgekoppelt. Der Baustein B 5.11 enthält tiefgehende technische Aspekte zur Apache-Konfiguration, die speziell vom Tool „Verinice“ nur teilweise behandelt werden. Hier könnten folgende Jahrgänge im Fach „Netzwerksicherheit“ an unsere Arbeitsvorlage anknüpfen.

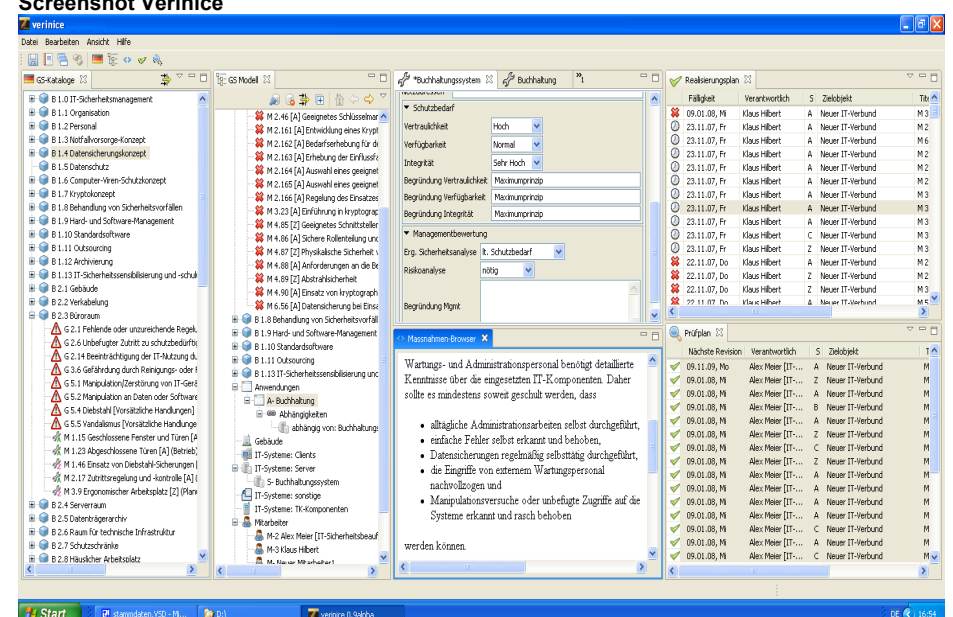
Bei der Untersuchung des Servers wurden teilweise erhebliche Mängel im Bereich der Infrastruktur und in den Organisationsabläufen festgestellt. Die fachliche und technische Absicherung des Servers stellte sich hingegen als gut heraus. Dies liegt nicht zuletzt an der hohen fachlichen Kompetenz der Mitarbeiter der FH Brandenburg.

Um den Standard des BSI einhalten zu können, muss vor allem bei den Verantwortlichen angesetzt werden. Zum einen müssten umfangreiche Dokumentationen angelegt werden, zum anderen müssten die Organisationsstrukturen an die Vorgaben der Grundschutzkataloge angepasst werden. Auch baulich wären einige Veränderung nötig, möchte man eine Zertifizierung durch das BSI erhalten.

Was ist Verinice?

Verinice ist ein freies ISMS-Tool für Audits nach ISO 27001, das antritt, die Arbeit des Sicherheitsbeauftragten zu vereinfachen. Das einfach zu bedienende Tool ist zum Verwalten von Angaben zur Sicherheit in Unternehmen und Behörden konzipiert worden. Die einzelnen Bausteine und Komponenten der Grundschutzkataloge des BSI können problemlos in das Programm integriert werden. Verinice ist überschaubar und für Erstnutzer einfach handzuhaben und zu verstehen, was es zu einem sinnvollen Arbeitswerkzeug macht.

Screenshot Verinice



Ergebnis unserer Untersuchung