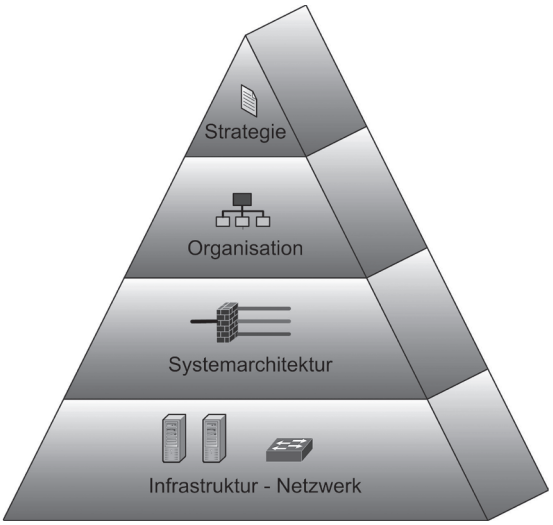
Audit Netzwerk- und Security Labor

Fachgebiet: IT-Security
Betreuer: Hansjürg Wenger
Experte: Prof. Dr. Torsten Braun (IAM, Uni Bern)

Informatik-Systeme sind heute einer grossen Zahl an Bedrohungen ausgesetzt. Selbst mit einer gut organisierten und regelmässig durchgeführten Wartung des ICT-Systems können sich mit der Zeit Fehler - respektive Sicherheitsrisiken einschleichen. Es ist deshalb für ein modernes ICT-System unerlässlich, in regelmässigen Abständen ein umfangreiches Audit durchzuführen.



Ausgangslage

Eine ICT-Infrastruktur, vor allem die Aspekte, welche die Sicherheit betreffen, muss vom Management einer Organisation vollständig gestützt werden. Das heisst, es braucht eine Strategie, in welcher die Sicherheitspolitik definiert ist. Gleichzeitig müssen die organisatorischen Aspekte klar geregelt sein – die oberste Verantwortung für die Sicherheit liegt meist undelegierbar bei der Geschäftsleitung. Damit der Informations-Austausch zwischen Management und den ICT-Diensten angemessen funktionieren kann und der Aspekt «Sicherheit» ernst genommen wird, ist es unumgänglich, dass die verantwortlichen Stellen von der IT bis zum Management definiert sind. Im Organigramm der höchsten Führungsebenen muss also die Sicherheit angemessen verankert sein.

Ein umfassendes Audit beinhaltet alles von der Ebene Management bis hin zur Ebene Endgeräte. Der genaue Scope eines Audits wird zusammen mit dem Auftraggeber abgesteckt.

Aufgabe

Unsere Aufgabe bestand aus 3 Teilen:
- Erarbeiten eines allgemeinen Vorgehens für ein (technisches) Security Audit.
- Durchführen eines Audits.
- Konkrete Umsetzung ausgewählter Massnahmen zur Erhöhung der Sicherheit.

Ablauf

Grundsätzlich gliedert sich ein Security Audit in folgende Teilschritte:
- Audit Planning
- Entrance Conference
- Fieldwork
- Preparing the Report
- Exit Conference
- Report to Management

Nach dem Erstellen des Audit Plannings wurde in Zusammenarbeit mit dem Auftraggeber der Audit Scope definiert. Dabei wurde der technische Umfang auf die zwei Hauptgebiete «Netzwerk-Security» und «Sicherheit auf virtualisierten Plattformen» eingegrenzt. Nach der Bestandesaufnahme wurde die Konfiguration einzelner Devices mit von Security Spezialisten empfohlenen Best Practices und Herstellervorgaben anlaysiert und entsprechend beurteilt. Durch ein Interview mit dem Systemverantwortlichen wurden weitere Fragen zu Themengebieten der ISO-Norm 27002 (IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management) geklärt. Anschliessend wurden die Gesamt-Architektur und das Netzwerk anhand persönlicher Erfahrungen und Überlegungen beurteilt. Gegen einige Systeme wurden verschiedene Scans mit Hilfe diverser Security Tools durchgeführt.

Während dieser Feldarbeit zeigten sich einige Verbesserungsmöglichkeiten, welche in einer Risikoanalyse beurteilt und als Empfehlung dem Auftraggeber abgegeben wurden. Resultierend zeigte sich unter anderem, dass der Aufbau eines Überwachungssystems sinnvoll wäre. Deshalb wurde abschliessend ein entsprechendes Konzept zur Einführung eines solchen Systems erarbeitet.

Karin Kälin

Urs Messerli