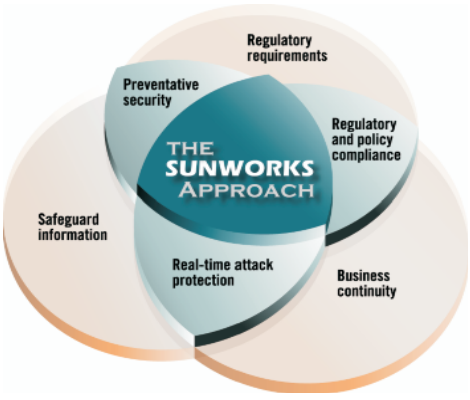
Security Audit

Interne Schwachstellenanalyse
Management- und IT-Summary

Warum ein Security-Audit?

Die Systemlandschaft der meisten Unternehmen ist historisch gewachsen und die Administration der Netzwerkinfrastruktur wird immer umfangreicher und unübersichtlicher. Mit zunehmender Abhängigkeit der Geschäftsprozesse von den IT-Systemen erhöhen sich auch die Sicherheitsanforderungen. Darüber hinaus fordern Gesetze und Wirtschaftsprüfer das Vorhandensein und die kontinuierliche Überprüfung eines funktionieren-den IT-Sicherheitsmanagements und der umgesetzten IT-Sicherheitsmassnahmen durch ein Internes Kontrollsystem

Im Rahmen eines IT-Sicherheitsaudits wird die aktuelle IT-Sicherheitslage in Ihrem Unternehmen analysiert. Um die Sicherheitsziele Vertraulichkeit, Integrität und Verbindlichkeit der Unternehmensinformationen zu gewährleisten, orientieren sich die Audits am individuellen Schutzbedarf der zu überprüfenden IT-Systeme.



Das aktuelle IT-Sicherheitsniveau im Unternehmen wird sowohl durch die Analyse der vorhandenen Security Policy, Richtlinien und Verfahren, als auch mit Hilfe von Interviews und Gebäudebegehungen nach anerkannten Standards und Grundsätzen überprüft.

Ziel des Security Audits

Sie erhalten einen umfangreichen Ergebnisbericht mit Management Summary, der die aktuelle Sicherheitssituation Ihres Unternehmens darlegt und vorhandene Schwachstellen entsprechend ihrem Risiko aufzeigt. Dieser Ergebnisbericht dient Ihnen auch als Grundlage für die weitere Sicherheitskonzeption in Ihrem Unternehmen und unterstützt Sie bei der Durchsetzung von IT-Sicherheitsinvestitionen.

Die IT-Security Audits orientieren sich an anerkannten Sicherheitsstandards wie:

- IT-Grundschutz nach BSI (Bundesamt für Sicherheit in der Informations-Technik) und ordnungsgemässer DV-gestützter Buchführungssysteme)
- ISO 27001, 17799, 13335
- DSG (Datenschutzgesetz)
- Basel II
- Sarbanes Oxley Act

Sie erhalten einen Überblicks über das IT-Sicherheitsniveau in den wichtigsten organisatorischen und technischen Bereichen (z.B. Sicherheits-Richtlinien, Zugangs-, Zugriffsschutz, Datensicher-ung) in kurzer Zeit:

- Überprüfung des Unternehmens anhand von Checklisten
- Aufzeigen von Schwachstellen und Risiken für den Geschäftsbetrieb
- Dokumentation der erkannten Schwachstellen in Checklistenform mit Management Summary

Durchführung des Audits

Gemeinsam mit dem Kunden erarbeiten wir in einem Initialgespräch die Prioritäten für das Security-Audit. Als Referenz verwenden wir dazu unsere Working-Docs welche auf den BSI-Standards basieren. Danach definieren wir einen Zeitraum für den Einsatz unserer SecAudit-Appliance um eine umfangreiche Schwachstellen-überprüfung zu realisieren.

Während dieser Testdauer werden parallel alle "weichen" Faktoren überprüft um auch über diesen Bereich ein gutes Abbild der Firma inklusive der vorhandenen Sicherheitskultur zu erhalten. Detaillierte Informationen dazu geben wir Ihnen gerne in einem gemeinsamen Gespräch weiter.

Nach Ablauf der definierten Testperiode werten wir die erhaltenen Resultate aus und bereiten sie für einen Management-Summary auf mit einem Katalog von Massnahmen für eine gewünschte Verbesserung des Sicherheits-Dispositivs des Kunden.

Somit erhält der Kunde einen klar abgefassten Prüfungsbericht und einen Katalog mit kurz- und mittel- oder langfristigen Verbesserungen seiner vorhandenen Infrastruktur.