SECURITY CHECK

Eine sichere IT ist die Basis für Ihren Geschäftserfolg. Neben den technischen Aspekten sind für den Betrieb eines sicheren IT-Systems vor allem auch organisatorische, personelle und bauliche Aspekte zu berücksichtigen.
Beim Security Check prüfen und bewerten wir alle relevanten Aspekte und geben Ihnen neben einem umfassenden Überblick auch geeignete Tools für die Organisation Ihrer IT in die Hand.

Ist Ihre IT sicher?
Wir prüfen sie.

Blackbox-Test
Im ersten Schritt des Security Checks versuchen wir, so viele Informationen wie möglich über Ihr EDV-System in Erfahrung zu bringen. Bei der indirekten Aufklärung durchsuchen wir zunächst alle öffentlich zugänglichen Datenbanken nach brauchbaren Informationen, bei der direkten Aufklärung werden schließlich die Zielsysteme selbst inspiziert. Neben Banner-Grabbing, Application-Mapping und anderen Verfahren unternehmen wir auf Wunsch auch aktive Eindringversuche, um Schwachstellen in Ihrem System zu finden und aufzuzeigen. Unsere Aktivitäten erfolgen natürlich immer in enger Absprache mit Ihrer IT-Mannschaft und werden auf Wunsch auch außerhalb der Betriebszeiten Ihres Unternehmens durchgeführt, um den Betrieb nicht zu beeinträchtigen. Als Ergebnis des Blackbox-Tests erhalten Sie eine umfangreiche Auswertung mit allen Daten der durchgeführten Analysen, eine Auflistung der ermittelten Schwachstellen und unsere Vorschläge, wie Sie Ihr System optimieren können.

Grundschutzhandbuch des Deutschen Bundesamtes für Sicherheit in der Informationstechnik

Whitebox-Test
Bei diesem Test überprüfen wir den Aufbau Ihrer EDV-Infrastruktur auf Schwachstellen und Designfehler sowie fehlerhaftes Verhalten von Teilkomponenten auf Basis der bestehenden Unterlagen und der aktuellen Konfigurationen. Im Gegensatz zum Blackbox-Test ist uns hier der Aufbau Ihrer Infrastruktur bekannt, anhand der bestehenden Detailpläne wird das Netzwerk konsequent durchgecheckt. Weiters bewerten wir im Zuge dieses Tests die physische Sicherheit der einzelnen Systemkomponenten sowie die Dokumentation der Systeme auf Basis der Vorgaben des BSI Grundschutzhandbuches (Deutsches Bundesamt für Sicherheit in der Informationstechnik). Als Ergebnis des Whitebox-Tests erhalten Sie eine umfangreiche softwaregestützte Dokumentation aller überprüften Systeme mit unseren Empfehlungen für die Umsetzung und Weiterführung durch Ihre IT-Mannschaft.

Ablauf des Security Checks

Wir gehen bei der Durchführung des Security Checks nach dem BSI Grundschutzhandbuch vor. Der Test läuft dabei in folgenden Phasen ab:

1. Vorbereitung

Zunächst definieren wir gemeinsam mit Ihrer IT-Mannschaft die Ziele des Tests. Dabei legen wir die Zielsysteme fest und definieren den Testumfang für jedes einzelne Ziel genau. Besonderes Augenmerk legen wir dabei auf eventuelle Testrisiken sowie auf Maßnahmen, die im Notfall ergriffen werden müssen.

2. Informationsbeschaffung

In dieser Phase werten wir erste Informationen über Ihre Systeme aus und unterziehen sie einer eingehenden Prüfung. Darüber hinaus versuchen wir, mittels offensichtlichen oder verdeckten Maßnahmen Informationen über die zu prüfenden Systeme zu erlangen. Mit einer Recherche der Schwachstellen schließen wir die Informationsbeschaffung ab.

3. Informationsbewertung und Risikoanalyse

Auf Basis der erhaltenen Informationen bewerten wir die Schwachstellen und Bedrohungen in Ihrem System und definieren Prioritäten für die aktiven Eindringversuche unter Berücksichtigung der diskutierten Risiken.

4. Aktive Eindringversuche

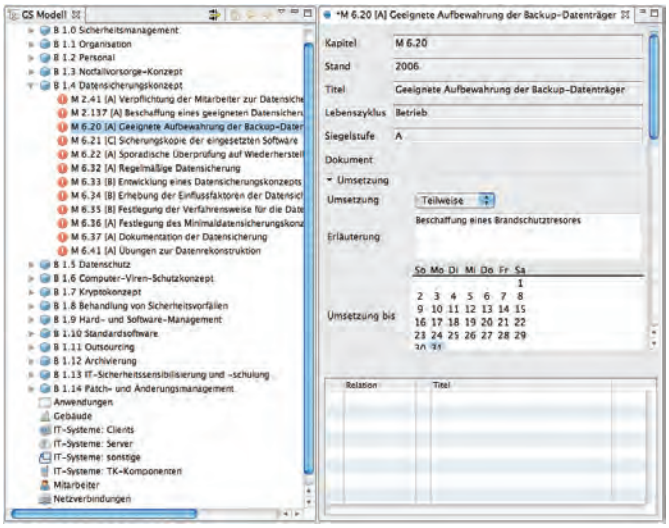
In dieser Phase versuchen wir, die administrative Gewalt über Teile Ihrer EDV-Infrastruktur zu erlangen, Passwörter zu entschlüsseln bzw. das System abzuhören oder auf andere Art und Weise zu kompromittieren.

5. Abschlussanalyse

In der abschließenden Phase bewerten wir die gesammelten Ergebnisse und stellen für Sie die daraus resultierenden Risiken dar. Auf Basis dieser Informationen geben wir Empfehlungen ab und entwickeln gemeinsam mit Ihrer IT-Mannschaft Aktionspläne für die Umsetzung unserer Vorschläge.

Eingesetzte Tools

Nach Abschluß des Security Checks haben wir die Basis für ein ISMS (Information-Security-Management-System) geschaffen. Basierend auf dem BSI Grundschutzhandbuch bildet dieses System alle IT-relevanten Komponenten in einer Datenbank ab, wo sie von Ihrer IT-Mannschaft laufend analysiert und verwaltet werden können.



ISMS-Datenbank mit allen IT-relevanten Komponenten

In der von uns zur Verfügung gestellten ISMS-Datenbank werden alle Sicherheitsaspekte getrennt betrachtet und mit den jeweils relevanten Themen des BSI-Grundschutzhandbuchs verknüpft. So werden etwa die Mitarbeiter mit den dazugehörigen organisatorischen Themen, die Server und Netzwerkgeräte mit den relevanten technischen Kapiteln des Handbuchs verknüpft. Die einzelnen Punkte sind nach ihrem Status als "erledigt", "nicht erledigt", "teilweise" oder "entbehrlich" gekennzeichnet, mit Hilfe der Software können Sie damit automatisierte Auswertungen über die relevanten Punkte durchführen und den aktuellen Status Ihrer IT jederzeit abrufen.

Bei der eingesetzten Datenbank handelt es sich um eine lizenzfreie Open-Source Software, die von einer breiten Community entwickelt und getestet wurde.