NETZWERKAUDIT QUALITÄTSSICHERUNG

Wie sicher ist die IT-Landschaft in unserem Unternehmen? Wie gut sind wir gegen die Angriffe von außen und innen geschützt? Sind unsere Daten schon im Internet verfügbar und wissen wir noch gar nicht davon? Diese oder ähnliche Fragen werden an die IT-Verantwortlichen gestellt, sobald in den Medien mal wieder über die großen Sicherheitsvorfälle diskutiert wird.

Gemeint werden bei solchen Fragen meistens die Anwendungssicherheit und der Schutz von sensiblen Informationen. Netzwerksicherheit bleibt dabei oft auf der Strecke und wird stark vernachlässigt. Können wir uns das erlauben? Die IT-Infrastruktur in einem Unternehmen ist nur so sicher, wie die jeweiligen infrastrukturellen Bestandteile der gesamten IT-Landschaft geschützt sind. Das Netzwerk verbindet unterschiedliche IT-Systeme in einer IT-Landschaft miteinander und stellt Wege für die Anwenderkommunikation und Datenzugriffe bereit.

Jittawit21/ Shutterstock ©

So gesehen kann das Netzwerk als erste Verteidigungslinie einer IT-Landschaft betrachtet werden. Solange wir das Netzwerk nicht schützen, stehen die IT-Systeme offen für mögliche Angriffe auf Anwendungen und sensible Informationen. Auch wenn diese gut geschützt sind, besteht ein großes Risiko, dass die Angriffe in einem „offenen und unsicheren Netz“ erfolgreich sein können.

Wie kann eigentlich ein Netzwerk geschützt werden? Nur sehr wenige Unternehmen kommen in den Genuss, die IT-Landschaft nach einem so genannten „Grüne Wiese“-Ansatz und nach aktuellen Sicherheitsstandards zu planen und aufzubauen. Sehr oft müssen die IT-Verantwortlichen mit einer IT-Infrastruktur zurechtkommen, die über die Jahre in einem Unternehmen gewachsen ist und immer wieder weiterentwickelt wurde. Im Rahmen eines Audits lassen sich die Schwachpunkte der IT-Infrastruktur identifizieren.

Um einen adäquaten Schutz einer IT-Landschaft bieten zu können, müssen als erstes die Maßnahmen identifiziert werden, mit denen die Sicherheitslücken in der aktuellen Infrastruktur geschlossen werden.

dainox GmbH
Magirus-Deutz-Str. 12
89077 Ulm

dainox®
Achievements from Internetworking Experts

NETZWERKAUDIT QUALITÄTSSICHERUNG

Dieses Maßnahmenpaket basiert im Wesentlichen auf den Ergebnissen der Sicherheitsanalyse der Netzwerkumgebung. An dieser Stelle bietet die dainox GmbH eine umfassende Unterstützung für ihre Kunden an.

Audit-Methodik

Der Kunde bestimmt gemeinsam mit der dainox den Scope des Audits und stellt Dokumentationen und Konfigurationen seiner Umgebungen bereit. Basierend auf diesen Informationen wird ein Report erstellt.

Die folgende Tabelle zeigt eine Auswahl an Bewertungskriterien:

I. Review und Bewertung des High Level Design (Grobkonzept)
- Zonierung / Segmentierung
- Redundanzen

II. Review und Bewertung des Proof of Concept (PoC - Verifizierung des Grobkonzeptes auf Basis von Tests)
- Testverfahren

III. Review und Bewertung des Low Level Design (Feinkonzept)
- Konfigurationsreview
- Softwareauswahl
- Auswahl und Dimensionierung der Komponenten

IV. Operative Themen
- Dokumentationen
- Prozesse

dainox GmbH
Magirus-Deutz-Str. 12
89077 Ulm