FU

IT-Verantwortlicher des Fachbereichs
Fachbereich Veterinärmedizin
Oertzenweg 19b
D-14163 Berlin Ruf: 030/838-62429, FAX: -62431

Logfile-Audit mit der Software Audit-Basics

1. Einführung

IT-Sicherheit hat eine technische, eine organisatorische und eine rechtliche Seite.
Die technische Seite wird an der FU durch das IT-Sicherheitsrahmenkonzept flankiert. Ohne diese wäre ein geordneter IT-Betrieb an der FU nicht denkbar. Vorbereitend aber auch ergänzend kann ein IT-Sicherheitsaudit durchgeführt und dokumentiert werden. Nur auf diesem Weg ist es zuverlässig möglich, im Streitfall einen (Entlastungs-)Beweis zu führen, die gesetzlichen Anforderungen an die IT-Sicherheit erfüllt zu haben. Hauptquelle eines IT-Sicherheitsaudits sind Logfiles, die bei den meisten IT-gestützten Befehlen anfallen.

> Eine **Logdatei** (engl. *log file*) ist das automatisch erstellte Protokoll aller oder bestimmter Aktionen von einem oder mehreren Nutzern an einem Rechner (Server wie Workstation), ohne dass diese davon etwas mitbekommen oder ihre Arbeit beeinflusst wird. Wesentlich ist das System-Logbuch. Darin werden u.a. die Anmeldungen am System protokolliert, aber auch weitere wichtige Informationen abgelegt. Praktisch alle Hintergrundprogramme (so auch das Betriebssystem selbst - der Kernel) z.B. der E-Mail-Server, der Proxyserver u. a. m. schreiben in eine Logdatei. Logdateien werden auch bei Webservern, SQL-Servern usw. erstellt. Logdateien werden beim **Logfile-Audit** bzw. der **Logfile-Analyse** untersucht. Dies kann manuell oder mittels geeigneter Software erfolgen.

Im unternehmerischen Bereich besteht bereits seit 01.05.1998 über das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) im Recht der Aktiengesellschaft die Pflicht zur Entwicklung eines internen Risikofrüherkennungssystems. Auch im universitären Umfeld empfiehlt sich dieses Vorgehen da sich jedes Unternehmen, das keine geeigneten Tools einsetzt, um Sicherheitsaspekte der IT-Infrastruktur im Griff zu haben und Schwachstellen im System aufzuspüren letztlich dem Vorwurf mangelnder Professionalität stellen muss.

2. Das Programm Audit-Basics

Die Software Audit-Basics macht Informationen, die im System (gleich welcher Betriebssysytemarchitektur) bereits vorhanden sind, an zentraler Stelle verfügbar. Es kann nur Dateien verarbeiten, die zuvor in Audit-Basics importiert wurden. Dabei kann es sich um Eventlogs von Servern aber auch Konfigurationsfiles von Workstation handeln. Die Inhalte können strukturiert (z.B. kommasepariert) aber auch nahezu unstrukturiertem Inhalt (z.B. Fließtext) handeln. Über definierte Regeln und Filter (z.B. in Anlehnung an das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik/BSI) lassen sich Zustände auf einfache und standardisierte Weise (zuvor z.B. durch den Personalrat abgesegnet) erfassen und interpretieren. Damit wird der Bereich in dem dieses Werkzeug zum Einsatz kommt erstmals in die Lage versetzt, dem geforderten IT-Grundschutz wirklich gerecht werden. Eine Auswertung der Files von Hand in der Art – suche was nicht sein darf - ist aufgrund des personellen wie zeitlichen Aufwands der hierfür zu veranschlagen wäre eine nur theoretische Möglichkeit. Sie kann nur einen Bruchteil der Qualität und Quantität einer derartig softwareunterstützten Lösung bieten.
Da die Nutzbarkeit der Software donglegestützt auf wendige PC beschränkt ist und darüber hinaus über ein eingeständiges Nutzermanagement verfügt, in dem verschiedene Rollen definiert werden, ist eine missbräuchliche Nutzung der Software ausgeschlossen.