

IT Audit

Dynamisches IT-Audit als Teil des IT-Sicherheitsmanagements

Automatisierte IT-Überwachung

Viele Unternehmen werden von IT-Sicherheitsmeldungen regelrecht überflutet. IT-Abteilungen haben so gut wie keine Chance, alle Ereignisse mit der gebotenen Sorgfalt auszuwerten. Abhilfe schafft ein automatisches, dynamisches IT-Audit, das sinnvollerweise systemübergreifend laufen sollte.

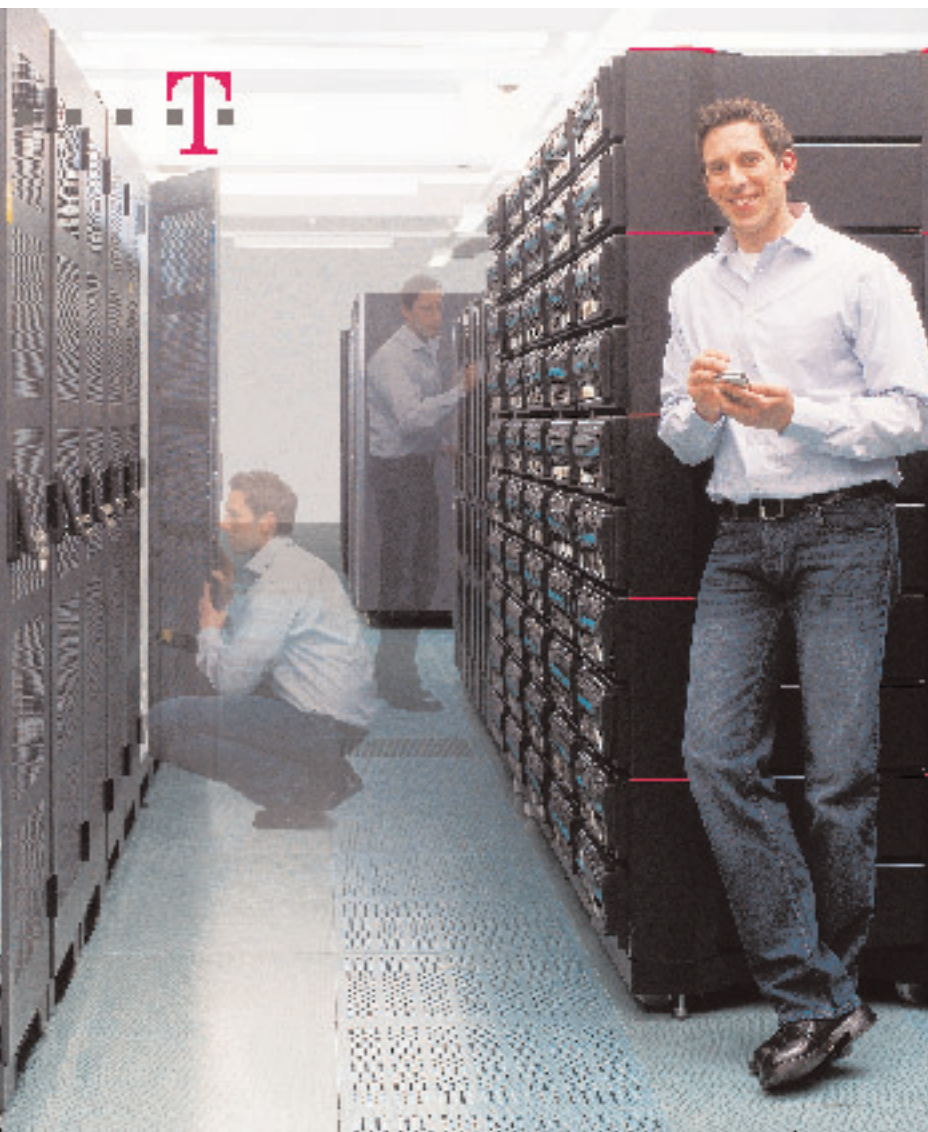
Nach einer Umfrage von Vanson Bourne registrieren fast die Hälfte der 700 befragten europäischen Unternehmen 4000 Security-Events und mehr in der Sekunde – Tendenz steigend. Ob eine Meldung allerdings auf eine Gefährdung hinweist oder harmlos ist, stellt sich erst bei näherer Betrachtung heraus. Und hier sitzt das Problem: Bis zu 40 Prozent ihrer Arbeitszeit verwenden IT-Abteilungen laut Studie für die Auswertung von Sicherheitsdaten. Und dennoch – ein Drittel der Befragten gab zu, dass die Datenmenge viel zu groß sei, um sie sorgfältig sammeln, abgleichen und analysieren zu können, um Sicherheitsbedrohungen zuverlässig zu identifizieren. Dabei ist eine Auswertung der IT-Meldungen von Server, Firewall, Software etc. sinnvoll und not-

wendig, um Schäden zu verhindern oder – wenn das Kind schon in den Brunnen gefallen ist – wenigstens abzumildern. Während kleinere Folgen wie fehlerhafter Datenzugriff oft noch keine größeren Schäden anrichten, können beispielsweise Maschinenstillstände oder Datenverluste das Schicksal des Unternehmens massiv beeinflussen.

Deshalb fordern auch immer öfter Gesetze und Richtlinien, dass die IT-Infrastruktur in der Organisation zu schützen und daher zu überwachen ist. Das Aktiengesetz und das GmbH-Gesetz etwa fordern die Einrichtung von Frühwarnsystemen, um existenzgefährdende Entwicklungen frühzeitig zu erkennen. Bei Nichteinhaltung drohen persönliche Haftungsprobleme gegebenenfalls

sogar Rückgriff auf das Privatvermögen. Ähnliches gilt nach dem US-Wertpapier-Gesetz SOX (Sarbanes Oxley Act) für US-börsennotierte Unternehmen und deren Tochtergesellschaften auf der ganzen Welt.

Auch unabhängig von äußerem Zwang interessieren sich mehr und mehr Unternehmen für ein effektives IT-Sicherheitsmanagement. Eine geringere Störungshäufigkeit bedeutet steigende Produktivität. Und spätestens seit die Kreditinstitute aufgrund von Basel II den Faktor der IT-Sicherheit zur Bewertung bei der Kreditvergabe heran ziehen, erkennen die Unternehmen, dass Vertrauenswürdigkeit und IT-Sicherheit ein entscheidender Wettbewerbsvorteil sein können.



TK-Qualifizierung: Geschwindigkeit zählt, Kompetenz entscheidet.

Hohe Dynamik, neue Trends: Wer in der Telekommunikation zu Hause ist, muss sicher und schnell agieren. Kompetenz und Wissen sind dabei entscheidende Erfolgsfaktoren.

Telekom Training setzt Maßstäbe in der TK-Qualifizierung. Praxisnah und immer am Puls der Zeit – in allen Bereichen, die in Ihrem Business entscheidend sind:

- IT/TK-Vernetzung
- IP-Security
- Voice over IP
- Wireless LAN

Gehören Sie zu denen, denen die Zukunft gehört.
www.training.telekom.de/tk-qualifizierung

Telekom Training
Gut sein – besser werden.

IT-Sicherheitsmanagement

Bleibt die Frage, wie ein konkretes IT-Sicherheitsmanagement entwickelt und umgesetzt werden kann? In den entsprechenden Gesetzestexten selbst ist dazu nichts zu finden, denn hier geht es nur um das „Was“. Das „Wie“ obliegt jedem Unternehmen allein. Hilfreich sind anerkannte Regelwerke wie ISO 27001 oder die IT-Grundschutzkataloge des BSI (Bundesamt für Sicherheit in der Informationstechnologie). Hiermit stehen den Organisationen überprüfbare Kriterienwerke zur Verfügung, deren Umsetzung auf Wunsch mit einem Zertifikat testiert werden kann. Hier zeigt sich aber ein weiteres Problem: Zertifizierungen dieser Art erfolgen im Sinne eines statischen Audits. Sie belegen mit einer stichprobenartigen Überprüfung ein definiertes Sicherheitsniveau zu einem bestimmten Zeitpunkt. Diese Momentaufnahme ist, auch im Sinne des Gesetzgebers (z.B. AktG § 91: „...Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten...“), für ein zuverlässig funktionierendes IT-Sicherheitsmanagement nicht ausreichend.

Systemübergreifendes dynamisches Audit

Die IT-Sicherheit ist etwas Flüchtiges und Sicherheitslücken können nicht dauerhaft durch eine einmalige Überprüfung gebannt werden. IT-Systeme und -Anwendungen

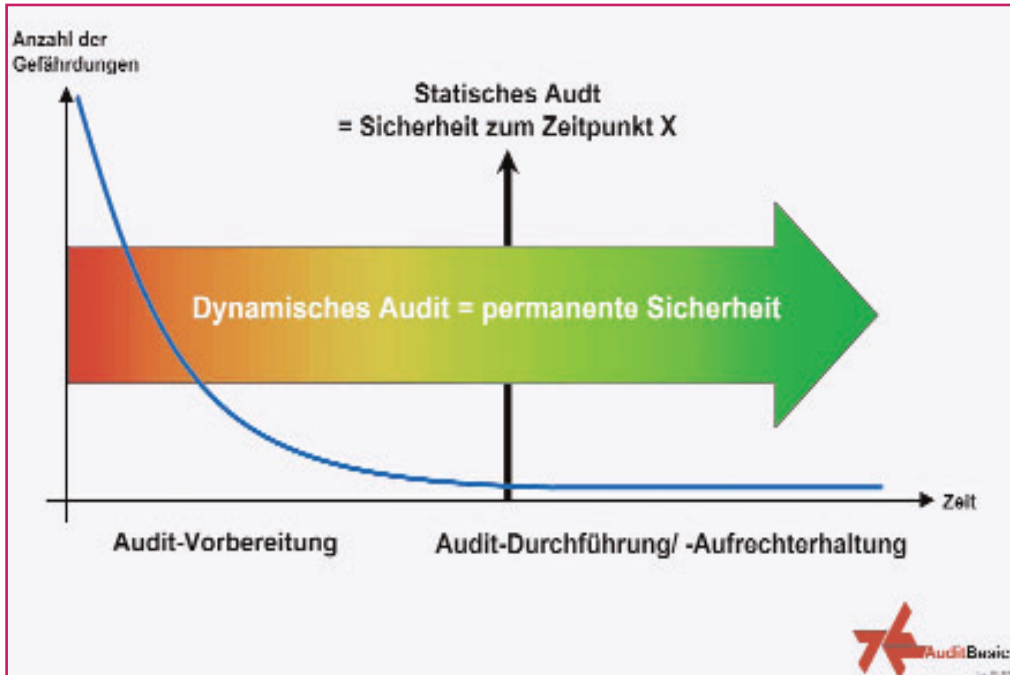
befinden sich in einem dynamischen, sich ständig ändernden Prozess. Ein effektives und rechtskonformes IT-Sicherheits-Audit sollte demnach nicht nur eine Momentaufnahme, sondern eine Zeitrumbetrachtung gewährleisten. Dazu ist es notwendig, auch die relevanten IT-Sicherheitsmeldungen permanent und umfassend auszufiltern und die Ergebnisse, wie es beispielsweise SOX fordert, nachvollziehbar zu dokumentieren. Ein dynamisches Audit zielt daher auf den gesamten Auditprozess ab – von der Erstanalyse über ein statisches Audit bis hin zur dauerhaften Überwachung einmal getätigter Einstellungen. Wie schwierig das aufgrund der schiereren Menge der auszuwertenden Daten ist, zeigt die eingangs zitierte Umfrage. Zwar besitzt jede Anwendung oft ihr eigenes Überwachungs- und Analyse-Werkzeug, das die Arbeit in diesem Punkt wesentlich erleichtert. Sobald es sich aber um eine heterogene IT-Unternehmens-Infrastruktur handelt und verschiedene Systeme wie Windows, UNIX, zOS und andere gleichzeitig im Einsatz sind, liegt der Fall erheblich schwieriger. Hier muss das Ziel lauten, die Meldungen systemübergreifend zu verknüpfen. Die Daten aller Systeme sollten also nicht nur aufbereitet und nach Relevanz gewichtet werden, sondern auch miteinander in Verbindung gesetzt und fortwährend analysiert werden. Zeigen sich dann Schwachstellen, können konkrete Handlungsempfehlungen abgeleitet wer-

den. Nur bei diesem Vorgehen kann von einem echten systemübergreifenden, dynamischen IT-Audit gesprochen werden. Bestandsgefährdende Entwicklungen lassen sich so im Kontext der unterschiedlichsten Systeme frühzeitig erkennen. Potenzielle Störungen werden minimiert, die Auswirkungen von Sicherheitsvorfällen auf das Unternehmen gemildert, sämtliche Betriebsabläufe rasch wiederhergestellt. Auf diese Weise ist für die volle Verfügbarkeit aller relevanten Informationen gesorgt.

So klar das Ziel ist, so problematisch ist die Umsetzung und Durchführung eines solchen dynamischen Audits. Durch manuelle Arbeit ist das Sammeln, Abgleichen und Analysieren der Daten kaum zu schaffen.

Die Lösung: Software, die solche Analysen regelmäßig und fehlerfrei durchführt wie zum Beispiel AuditBasics von Demal. Das Überwachungs- und Analyse-Tool muss die Daten der verschiedenen Systeme einlesen, komplex verknüpfte Kontrollen und Auswertungen durchführen und dabei auch sehr große Datenmengen automatisiert verarbeiten. Als Ergebnis sollten Berichte erzeugt werden, die Schwachstellen und Abweichungen von Sicherheitsrichtlinien oder gesetzlichen Bestimmungen dokumentieren, am besten so, dass sie auch für das fachlich nicht involvierte Management im Unternehmen leicht verständlich sind.

Die eventuell bereits bestehenden system-internen Security-Technologien werden dadurch nicht überflüssig, sondern vielmehr mit allen Informationsquellen in einer zentralen Audit-Gesamtoberfläche zusammengefasst. Im Falle von AuditBasics helfen vorgefertigte Policies, um das System schnell einsetzen zu können. In Zusammenarbeit mit Partnern aus der freien Wirtschaft wie FinanzIT Berlin und staatlich geprüften BSI-Auditoren hat Demal bereits eine Vielzahl der am häufigsten benötigten und wichtigsten Auswertungsrichtlinien entwickelt. Die „Top30“-Policies stehen für die Systeme z/OS, Windows, UNIX und OS/400 bzw. i5/OS zur Verfügung. Eine so verbreitete Software kann damit bereits für die Ist-Analyse, also schon zu Beginn eines Auditprozesses, ohne weitere Vorarbeit effektiv eingesetzt werden.



Permanentes IT-Audit ist manuell nicht zu bewerkstelligen. Abhilfe schafft eine Automatisierungssoftware wie zum Beispiel AuditBasics von Demal.

Nils Wegner, Marketing Manager

Andreas Grimme, Datenschutzbeauftragter