

Der dynamische IT-Auditprozess mit AuditBasics

Die Auditierungs-Software für Organisationen und BSI-Auditoren.



AuditBasics begleitet den dynamischen Auditprozess und sichert die IT-Systeme - vor und nach der Zertifizierung.

Das plattformübergreifende und systemunabhängige Software-Tool AuditBasics unterstützt Unternehmen und Institutionen bei der Durchführung eines IT-Sicherheits-Audits auf Basis der IT-Grundschutz-Methodik. Gleichzeitig dient es BSI-Auditoren als Prüfungstool für Zertifizierungsaudits. Dabei ist AuditBasics im Sinne eines dynamischen Audits im gesamten Auditprozess einsetzbar.

Stufe 1



Stufe 2



Audit

Prozess



Stufe 3

Stufe 4

Stufe 1: Grundanalyse der IT-Systeme



Der dynamische Auditprozess beginnt mit einer Grundanalyse der IT-Landschaft. Diese Auswertung dient dazu grundlegende Sicherheitslücken in den IT-Systemen anhand definierter, standardisierter Kriterien zu identifizieren.

AuditBasics wird in dieser Phase zur schnellen und effektiven Überprüfung von unterschiedlichen Systemen wie Windows, Linux, AS400, iSeries und zOS eingesetzt. Als Regelwerke, nach denen AuditBasics die IT-Systeme analysiert, stehen die vorgefertigten Top30-Policies, die dreißig häufigst benötigten Auswertungsvorschriften nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) zur Verfügung. Diese wurden von der DEMAL mit Hilfe von staatlich geprüften BSI-Auditoren und Partnern aus der freien Wirtschaft entwickelt. Die Ergebnisse dienen als erste Einschätzung der Sicherheitssituation in der Organisation und als Grundstock für die Umsetzung des IT-Grundschutzes.

Stufe 2: IT-Sicherheitskonzept nach IT-Grundschutz



Ziel der zweiten Phase ist die Entwicklung eines umfassenden IT-Sicherheitskonzepts, um somit die Basis für eine mögliche ISO 27001-Zertifizierung nach IT-Grundschutz zu schaffen. Die IT-Grundschutzkataloge bieten dazu eine stufenweise Methodik sowie konkrete und umfassende Maßnahmen an, die Schritt für Schritt durchzuführen und zu dokumentieren sind.

Viele der geforderten Maßnahmen können mit AuditBasics über die Auswertung von Log- und Konfigurationsdateien gewonnen werden. Auswertungsvorschriften, so genannte Policies, die auf Basis der IT-Grundschutz-Maßnahmen oder auch individueller Anforderungen formuliert werden, bilden die Richtlinien, nach denen AuditBasics die Auswertungen vornimmt. Die Software fungiert somit als Erfolgskontrolle bei der sukzessiven Umsetzung der Maßnahmen. Gleichzeitig werden einmal realisierte Einstellungen mit AuditBasics kontinuierlich auf ihre Einhaltung überwacht.

Besondere Bedeutung findet AuditBasics bei der Durchführung des Basis-Sicherheitschecks, der finale, interne Soll-Ist-Vergleich. Hierbei wird eine Prüfung der umgesetzten Maßnahmen durchgeführt um heraus zu finden, welche Sicherheitsmaßnahmen ausreichend oder nur unzureichend umgesetzt wurden. Der Status aller, mit Policies hinterlegten, Maßnahmen kann mit AuditBasics auf einen Blick überprüft werden. Der Basis-Sicherheitscheck dient quasi als internes "Vor-Audit" für die eigentliche Zertifizierung und gilt als wichtiges Referenzdokument für den BSI-Auditor.

Stufe 3: ISO 27001-/IT-Grundschutz-Zertifizierung



Nach der Umsetzung der IT-Grundschutz-Anforderungen beauftragt die Institution einen lizenzierten, unabhängigen Auditor, den Status der IT-Sicherheit zu verifizieren. Durch die ISO 27001- bzw. IT-Grundschutz-Zertifizierung werden die Bemühungen um die IT-Sicherheit und die erfolgreiche Umsetzung nationaler und internationaler Normen nach innen und außen dokumentiert.

Die Prüfung erfolgt in zwei Teilschritten. Im ersten Schritt sichtet der Prüfer die Referenzdokumente, welche die Organisation selbst teilweise mit AuditBasics erstellt hat. Im zweiten Teilschritt führt er eine Vorort-Prüfung durch und begutachtet selbst die tatsächliche Umsetzung der dokumentierten Sachverhalte.

Unter Zuhilfenahme von AuditBasics kann die Überprüfung erheblich effektiver gestaltet werden. Der Einsatz von AuditBasics durch die Organisation (Stufe 2) und den Prüfer (Stufe 3) schafft somit eine einheitliche Prüfbasis. Komplikationen und Missverständnisse werden minimiert, der Zertifizierungsprozess verläuft schneller und günstiger.

Stufe 4: Permanente Sicherheit der IT-Systeme



In dieser Phase zeigt sich ein weiterer entscheidender Vorteil des dynamischen Audits mit AuditBasics: die Zeitrumbetrachtung. Die Prüfung des Sicherheitsstatus zu einem bestimmten Zeitpunkt, wie es bei Zertifizierungen der Fall sein kann, stellt ein statisches Audit dar. Das statische Audit gewährleistet jedoch keine dauerhafte Sicherung, da die IT-Sicherheit etwas Flüchtliges ist und Sicherheitslücken nicht durch eine einmalige Überprüfung gebannt werden können. Ein effektives IT-Sicherheits-Audit sollte demnach nicht nur eine Momentaufnahme, sondern eine Zeitrumbetrachtung gewährleisten.

Genau dies ist mit AuditBasics möglich. AuditBasics überwacht permanent alle Sicherheitseinstellungen und Policies an den IT-Systemen. Die Berichte werden zeitgesteuert mit den relevanten, auffälligen Sicherheitsmeldungen an die jeweiligen Verantwortlichen versendet. Bestandsgefährdende Entwicklungen und kritische Zustände können somit frühzeitig erkannt werden. Dadurch wird in den IT-Systemen eine permanente Sicherheit wie am Tag des Zertifizierungsaudits erreicht - mühelos und ohne Aufwand wertvoller Ressourcen. Durch diese kontinuierliche Überwachung und Dokumentation der IT-Sicherheit werden sogar die strengen Anforderungen nach permanenten Überwachungssystemen erfüllt, wie es vermehrt von nationalen und internationalen Gesetzen und Richtlinien gefordert wird.

Für weitere Informationen stehen wir Ihnen gerne zur Verfügung!



DEMAL GmbH

Hembacher Str. 2b • 90592 Schwarzenbruck
Telefon: 09183 - 90 31 32 • Fax: 09183 - 90 30 75
info@demal-gmbh.de • www.demal-gmbh.de

