pallas

Security Consulting

Passende Module für die IT-Sicherheit

Die Pallas-Experten sorgen für Ihre IT-Sicherheit

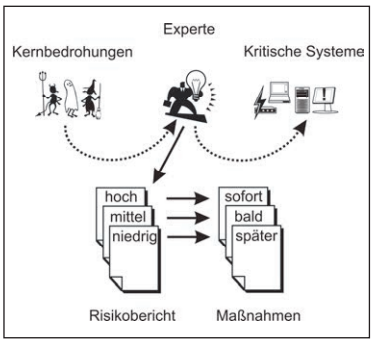
Eine gute und angemessene IT-Sicherheit braucht passende technische Komponenten und ein geeignetes organisatorisches Gerüst. Beides kann mit dem aus dem Qualitätsmanagement bekannten PLAN-DO-CHECK-ACT-Zyklus (PDCA) nachhaltig gesteuert werden, weil man die IT-Sicherheit als Qualitätsdimension der IT auffassen kann. Für die Phasen PLAN und CHECK ist externes Experten-Know-how angeraten, damit der Blick über den eigenen Tellerrand hinausgeht.

Die Pallas-Experten bringen in die Consulting-Projekte nicht nur Faktenwissen, sondern umfangreiche Erfahrungen aus Einrichtung und Betrieb von IT-Sicherheitssystemen, dem TÜV-geprüften Managed Security Service mit. Wir wissen also ganz praktisch, wovon wir sprechen.

Pallas hat drei Module definiert, um den Beratungseinstieg leicht zu machen, aber auch bei einem kompletten Information Security Management System die perfekte Unterstützung zu ermöglichen.

Modul 1: Schwachstellenanalyse

Der beste Einstieg in die Verbesserung der IT-Sicherheit ist die Schwachstellenanalyse. Dabei überprüft ein Experte mit einem Basis-Check das IT-Management und durch eine Begehung exemplarisch die gesamte IT-Infrastruktur (Netzwerkkomponenten, Server- und Arbeitsplatzsysteme sowie die Umgebungsinfrastruktur). Die Konzentration auf Kernbedrohungen und kritische Systeme sorgt für niedrige Kosten. Ergebnis ist ein Bericht, der die sicherheitskritischen Schwachstellen nach Risikoklassen bewertet. Maßnahmen zur Milderung oder Behebung der Schwachstellen in einer der Kritizität entsprechenden Reihenfolge werden ebenfalls festgehalten.



Die Schwachstellenanalyse schärft das Verständnis der Geschäftsleitung für die für das Business wirklich kritischen Risiken und macht Geschäftsleitung und IT-Personal die beiderseitige Verantwortlichkeit bewusst.

Modul 2: Security Audit

Ein Security Audit ist ein regelmäßiges Überprüfungsverfahren, das eines oder mehrere der folgenden Ziele verfolgt:

- Überprüfung vorhandener Sicherheitsprozesse auf ihren Erfüllungsgrad
- Erhöhung des Reifegrades eines Prozessmodells (z.B. nach ITIL) und Unterstützung der regelmäßigen Verbesserungen
- Identifizierung von Systemlücken, die Risiken verdecken

Das Security Audit geht auf einzelne Aspekte der IT-Sicherheit vertieft ein und nutzt Checklisten zur Erhebung. Wir gehen dabei in den folgenden Schritten vor:

1. Bewertung vorhandener Prozesse und ihrer aktuellen Ergebnisse durch einen Soll-Ist-Vergleich
2. Heranziehung komplementärer Dokumente, die auf die Sicherheitssituation Einfluss haben können
3. Interview mit Prozess- und Ergebnisverantwortlichen
4. Befragung weiterer Kommunikationspartner im Unternehmen
5. Niederlegung der Ergebnisse im Audit-Report
6. Präsentation und Diskussion der Ergebnisse

Der Audit-Report hält geprüfte Elemente, potentielle Sicherheitsrisiken sowie Ziele und Maßnahmen zur Mitigation oder Behebung von Risiken nebst Priorisierung fest.

Modul 3: Information Security Management System

Das Pallas Security Consulting reicht über den Analyse- und Prüfbereich hinaus bis zur Konzeption von Sicherheitskomponenten und -prozessen, z.B. der Entwicklung eines Betriebs- oder Notfallkonzepts. Eine organisatorisch dauerhaft gut fundierte IT-Sicherheit erreicht man am besten mit einem Information Security Management System (ISMS). Ein solches ISMS sichert

- die schriftliche Fixierung von Sicherheitszielen nebst zugehörigen Konzepten und Prozessen sowie technischen Anweisungen und Protokollen,
- einen jährlichen PDCA-Zyklus und damit letztlich
- die systematische Betrachtung und Verbesserung der IT-Sicherheit.

Für ein ISMS bildet die Norm DIN ISO/IEC 27001 oder der BSI-Standard 100-1 eine verlässliche Basis. Beim Start verfügt ein Unternehmen kaum über Erfahrungswissen, deshalb liegt es nahe, die Pallas-Experten hinzuzuziehen. KMU-tauglich wird das ISMS durch das Pallas-Modellkonzept:

O Organisatorische Festlegungen
P Prozessbeschreibungen für Security-Management und Risikoanalyse
E Einzelrisikobewertungen für die Assets unter bestimmten Security-Szenarien und durch die in der Norm vorgegebenen Maßnahmen-Controls
S Einführung eines Softwaretools zur Unterstützung des ISMS (optional)

Als Ergebnis fördert das ISMS den bewussten Umgang mit und die Reduktion von Risiken. Diese ganzheitliche Betrachtung sorgt für eine bessere Koordination von Sicherheitsmaßnahmen und vermeidet Lücken genauso wie Überschneidungen. Nicht zuletzt wird so die Erfüllung gesetzlicher und vertraglicher Anforderungen sichergestellt.

pallas
Pallas GmbH • Hermülheimer Str. 8a • 50321 Brühl
www.pallas.de • information (at) pallas.de
Tel: 02232-1896-0 • Fax: 02232-1896-29

TÜV SAARLAND Geprüfte Managed Services