

Herausforderungen

Aufgrund der wachsenden Bedeutung der Informationstechnologie für die Geschäftstätigkeit müssen Unternehmen wie Verwaltungen regelmäßig ihre Maßnahmen im Bereich Information Security auf Angemessenheit prüfen. Ziel ist, die allgemeine Sicherheit der eigenen Systeme, Netzwerke, der Nutzer sowie der internen und externen Prozesse täglicher Arbeitsabläufe zu verbessern.

Um in der hochgradig vernetzten Welt zu bestehen, dürfen sich Unternehmen nicht nur auf bestehende Schutzmaßnahmen für Daten verlassen, sondern müssen jedes einzelne Element ihrer Organisation und Geschäftsprozesse bewerten und überprüfen. Je stärker die Unternehmensabläufe elektronisch geprägt sind (z.B. elektronisch Abwicklung des Kundenmanagements), um so höher ist die Wahrscheinlichkeit, dass Informationen in falsche Hände geraten. Jedes Unternehmen, das Opfer eines „elektronischen“ Angriffs wird, (z.B. durch „Hacker“) muss mit Imageverlusten und damit verbundenen wirtschaftlichen Verlusten rechnen. Auch birgt jede öffentlich wahrgenommene Sicherheitslücke die Gefahr weiterer gesetzlicher Auflagen mit entsprechenden Aufwänden.

Lösungen

Information Security (IS) bietet einen wirksamen Zugang zu Systemen und Datenhaltungen und deckt dabei alle risikorelevanten Herausforderungen innerhalb und außerhalb der Organisation ab. Wir unterstützen Unternehmen dabei, Strategien, Prozesse und Technologien anzuwenden, um die hohen Anforderungen an den Schutz von Informationen zu erfüllen. Zusammen mit unseren Kunden schaffen wir einen Rahmen, der für alle Beteiligten die Konvergenz von Informationssicherheit und Datenschutz gewährleistet. Wir bewerten ihre Informationen und sorgen dafür, dass ihr Informationsmanagement nachhaltig und sicher ist. Im Blickpunkt stehen daher: „Security Governance“, „Business Continuity“, „Information Risk Management“ sowie „Planning and Disaster Recovery“, „Security Assessment“ und „Data Protection“.

Nutzen

Unsere Kunden können aktuelle Bedrohungen pro-aktiv angehen und entwickeln ein Verständnis von Informationssicherheit, die das ganze Unternehmen abdeckt: Mitarbeiter, Prozesse und Technologie - dies bezieht sich auf Produktdaten, Geschäftsstrategien, Finanzinformationen, Mitarbeiter- und Kundendaten/-profile. Zudem ermöglichen unsere Methoden und Instrumente detaillierte Kosten-Nutzen-Analysen der zur Umsetzung vorgesehenen Sicherheitsmaßnahmen.

Beispiele

- Globales Logistikunternehmen: Entwicklung eines Security Repository sowie eines Security Controlling und Reporting auf Basis einer Balanced Scorecard und Vorbereitung des Unternehmens auf eine ISO 27001 Zertifizierung.
- Sicherheitsbehörde des Bundes: Aufbau eines Business Continuity Managements für eine kritische IT-Infrastruktur inkl. eines Krisenreaktionskonzeptes.

Kontakt

EMEA-Solutions@bearingpoint.com



Lösungskomponenten

Security Governance

unterstützt Kunden ihre Organisation, Prozesse und Technologien zu ordnen und transparent zu gestalten, um die Sicherheit der Informationen zu steuern.

Business Continuity

unterstützt Kunden, Planungen für die Wiederherstellung (Contingency and Disaster Recovery Planning) aller oder sehr wichtiger Dienste und Geschäftsprozesse im Falle einer Unterbrechung zu entwerfen und Maßnahmen umzusetzen.

Information Risk Management

ermöglicht Maßnahmen nach Gefahren, Bedrohungen für die Organisation sowie die Schadenshöhe und die Eintrittswahrscheinlichkeit zu bewerten und Risikostrategien umzusetzen.

Security Assessment

bewertet die Effizienz und Effektivität ihrer Sicherheitsorganisation z.B. gemäß ISO 27001.

Data Protection

schützt personenbezogene Informationen vor Missbrauch.

