

Kritis – Schutz kritischer Infrastrukturen

Das Thema Kritische Infrastrukturen ist eines der größten Herausforderungen, mit dem Unternehmen und Behörden in den nächsten Jahren konfrontiert werden. Die Zahl der Regularien und Standards in diesem Bereich wird sich in den kommenden Jahren sehr dynamisch entwickeln und einen enormen Druck ausüben. Verstärkt wird dieser durch die Anforderung der Öffentlichkeit, eine größere Sicherheit bei möglichen terroristischen Anschlägen und Naturkatastrophen zu gewährleisten. Daher ist es wichtig, für diese zukünftige Entwicklung gerüstet zu sein.

Risk, Compliance and Security (RCS)

Mit der RCS Solution bietet BearingPoint als „Trusted Advisor“ seinen Kunden umfassende Beratungsleistungen zu Information Security, Risikomanagement und Compliance Anforderungen von der Strategieentwicklung über Organisationsberatung und -management bis zur technischen Implementierung der Systeme einschließlich der technischen Infrastruktur. Die Beratungsleistungen von RCS decken vier Bereiche ab:

- RCS Governance
- Zertifizierung und Audits
- Identity & Access Management
- Operational RCS

Kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) sind Unternehmen und Behörden mit wichtiger Bedeutung für Deutschland, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen/inneren Sicherheit eintreten würden.

Zu den kritischen Infrastrukturen zählen:

- Energieversorger
- Chemieunternehmen
- Informations- und Telekommunikationskonzerne

- Transportgewerbe
- Finanz-, Geld- und Versicherungsbranche
- Versorgungsunternehmen
- Behörden.

Zum Schutz dieser Infrastrukturen gab das Bundesministerium des Innern den Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) 2005 heraus, der die Grundlage für den Umsetzungsplan KRITIS (UP KRITIS) in 2007 bildete. Dieser Umsetzungsplan beinhaltet Handlungsempfehlungen und konkrete Maßnahmen für privatwirtschaftliche Betreiber kritischer Infrastrukturen.



Die Herausforderung

Ziel ist die Reduzierung der Verwundbarkeit kritischer Infrastrukturen gegenüber natürlichen Ereignissen, Unfällen und fahrlässigem Handeln sowie gegenüber möglichen terroristischen Anschlägen und kriminellen Verhalten.

Der Bedarf für eine Lösung ergibt sich unter anderem aus gesetzlichen Vorschriften und allgemein anerkannten Standards, aber auch aus allgemein anerkannten unternehmerischen Prinzipien eines vorausschauenden Risikomanagements und einer strategischen, auf Erfolg und Kontinuität ausgerichteten Unternehmensplanung.

BearingPoints Beratungsansatz

Es wird die aus der Praxis bewährte Dreiteilung der Projektdurchführung in die Phasen Analyse, Maßnahmenempfehlungen und Unterstützung in der Realisierung verwendet.

- I. Business Impact Analyse
- II. Entwicklung von Schadens- und Bedrohungsszenarien
- III. Durchführung der Ist-Analyse
- IV. Auswertung des Reifegradmodells
- V. Empfehlung von Maßnahmen
- VI. Planung der Umsetzung der Maßnahmen
- VII. Möglichkeit der regelmäßigen Überprüfung dieses Analyse- und Planungsprozesses
- VIII. Verbesserungsvorschläge im Rahmen des Qualitätsmanagements

Als Hilfestellung für die Umsetzung dieser acht Schritte hat BearingPoint ein Tool entwickelt, welches ein strukturiertes Vorgehen ermöglicht.

Das Ergebnis

Das Tool generiert, ausgehend von den kritischen Geschäftsprozessen und den relevanten Gefährdungen für das Unternehmen bzw. die Behörde, eine individuelle Checkliste, welche die wichtigsten Punkte aus den gängigen Standards enthält und so einen umfassenden Analyse-Ansatz ermöglicht.

Das aus der Ist-Analyse gewonnene Bild über die Stärken und Schwächen des Unternehmens bzw. der Behörde wird mittels eines Reifegradmodells visualisiert und erlaubt so einen schnellen Überblick über die gefährdeten Bereiche des Unternehmens bzw. die Behörde. Zu den so erkannten kritischen Bereichen werden gleichzeitig Maßnahmen empfohlen und ein Umsetzungszeitrahmen genannt. Dies ermöglicht ein strukturiertes Einleiten aller weiteren Schritte, um gegen die Schwächen vorgehen zu können.

Zusätzlich erlaubt das Tool, dass sich Unternehmen bzw. Behörden selbst einen Zeitrahmen setzen und ihre Fortschritte dokumentieren können.

Damit bietet BearingPoint Unterstützung dabei, dass Unternehmen bzw. Behörden als kritische Infrastrukturbetreiber konform gemäß den Regularien und Standards handeln und sich selbst schützen können. Zudem können Unternehmen bzw. Behörden mit Hilfe unserer Lösung einen höheren Sicherheitsgrad erzielen.

Ihre Ansprechpartnerin

Caroline Neufert, Senior Manager
BearingPoint GmbH
Kurfürstendamm 207 - 208
10719 Berlin

Tel.: +49 30 88004-2230
caroline.neufert@bearingpoint.com

Wir helfen unseren Kunden, messbare und nachhaltige Ergebnisse zu erzielen

BearingPoint wendet sich als ein führendes Management- und Technologieberatungsunternehmen an die Forbes Global 2.000-Unternehmen sowie viele der weltweit größten öffentlichen Einrichtungen. Unsere ca. 16.000 engagierten und erfahrenen Mitarbeiter unterstützen Organisationen rund um den Globus bei der Lösung ihrer dringendsten und wichtigsten Aufgaben – und das tagtäglich. Durch unseren kooperativen und flexiblen Ansatz helfen wir unseren Kunden, praktische, nachhaltige und messbare Ergebnisse zu erzielen, die richtigen strategischen Entscheidungen zu treffen und die passenden Lösungen umsetzen zu können.

Weitere Informationen finden Sie auf unserer Webseite unter www.bearingpoint.com oder www.bearingpoint.de.

Kontakt:
psmarketinggermany@bearingpoint.com

BearingPoint GmbH
Kurfürstendamm 207 - 208
10719 Berlin – Germany

www.bearingpoint.com

© 2008 BearingPoint GmbH, Wien. Alle Rechte vorbehalten. Gedruckt in der EU. Der Inhalt dieses Dokuments unterliegt dem Urheberrecht. Veränderungen, Kürzungen, Erweiterungen und Ergänzungen, jede Veröffentlichung, Übersetzung oder gewerbliche Nutzung zu Schulungszwecken durch Dritte bedarf der vorherigen schriftlichen Einwilligung durch BearingPoint GmbH, Wien. Jede Vervielfältigung ist zum persönlichen Gebrauch gestattet und nur unter der Bedingung, dass dieser Urheberrechtsvermerk beim Vervielfältigen auf dem Dokument selbst erhalten bleibt. FC 0433 DE