



# KRITIS – Schutz kritischer Infrastrukturen

## Herausforderungen

Der Schutz kritischer Infrastrukturen ist eine der größten Herausforderungen, mit denen Unternehmen, insbesondere Energieversorger, in den nächsten Jahren konfrontiert werden. Regularien und Standards in diesem Bereich werden sich sehr dynamisch entwickeln und enormen Druck ausüben. Noch in 2014 plant die Bundesregierung, ein IT-Sicherheitsgesetz zu verabschieden, das insbesondere Regelungen für kritische Infrastrukturbetreiber, wie Energieversorger, beinhalten wird. So ist unter anderem geplant,

- branchenspezifische IT-Sicherheits-Mindestniveaus,
- regelmäßige Sicherheitsaudits und
- Meldepflichten

einzuführen.

Verstärkt wird der Druck durch die Forderung der Öffentlichkeit nach größerer Sicherheit vor möglichen Naturkatastrophen und terroristischen Anschlägen, die immer häufiger durch Angriffe im Cyber-Raum ausgelöst werden. Für diese zukünftigen Entwicklungen müssen Unternehmen gerüstet sein.

## Lösungen

BearingPoint bietet zum Schutz kritischer Infrastrukturen eine Paketlösung an, die die Fortführung des Geschäftsbetriebs in Krisensituationen oder nach unerwarteten Schadensereignissen sicherstellt.

Die Lösung verwendet die in der Praxis bewährte Projektdurchführung mit Analysen, Maßnahmenempfehlungen und Unterstützung in der Realisierung. Diese beziehen sich insbesondere auf die Anforderungen der Informationssicherheit und Business Continuity. Sie ist modular aufgebaut, branchenbezogen sowie sektoren- und kernprozessspezifisch:

- I. Business Impact-Analyse
- II. Entwicklung von Schadens- und Bedrohungsszenarien
- III. Ist-Analyse
- IV. Auswertung nach Reifegradmodell
- V. Maßnahmenempfehlung
- VI. Planung der Maßnahmenumsetzung
- VII. Regelmäßige Überprüfung des Analyse- und Planungsprozesses
- VIII. Qualitätsmanagement

Für die Umsetzung dieser acht Schritte nutzt BearingPoint ein Tool, das ein strukturiertes Vorgehen ermöglicht. Für kritische Geschäftsprozesse und relevante Gefährdungen des Unternehmens generiert das Tool eine individuelle Checkliste, die die wichtigsten Punkte der gängigen Standards und notwendigen Regularien enthält und einen umfassenden Analyse-Ansatz ermöglicht. So kann das aus der Ist-Analyse gewonnene Bild über Stärken und Schwächen des Unternehmens mittels eines Reifegradmodells visualisiert werden. Damit wird ein schneller Überblick über gefährdete Bereiche des Unternehmens bzw. der Behörde erlaubt. Notwendige Maßnahmen sind hinterlegt und die Umsetzungsplanung kann generiert werden.

## Über BearingPoint

BearingPoint Berater haben immer im Blick, dass sich die wirtschaftlichen Rahmenbedingungen permanent verändern und die daraus entstehenden komplexen Systeme flexible, fokussierte und individuelle Lösungswege erfordern. Unsere Kunden, ob aus Industrie und Handel, der Finanz- und Versicherungswirtschaft oder aus der öffentlichen Verwaltung, profitieren von messbaren Ergebnissen, wenn sie mit uns zusammenarbeiten. Wir kombinieren branchenspezifische Management- und Fachkompetenz mit neuen technischen Möglichkeiten und eigenen Produkt-Entwicklungen, um unsere Lösungen an die individuellen Fragestellungen unserer Kunden anzupassen. Dieser partnerschaftliche, ergebnisorientierte Ansatz bildet das Herz unserer Unternehmenskultur und hat zu nachhaltigen Beziehungen mit vielen der weltweit führenden Unternehmen und Organisationen geführt. Unsere 3.350 Mitarbeiter unterstützen zusammen mit unserem globalen Beratungs-Netzwerk Kunden in über 70 Ländern und engagieren sich gemeinsam mit ihnen für einen messbaren und langfristigen Geschäftserfolg.

## Nutzen

Unsere modularen Lösungen können kritischen Infrastrukturbetreibern wie Energieversorgern helfen:

- durch Check des IT-Sicherheitsniveaus notwendige Maßnahmen einzuleiten,
- die Compliance zu verbessern und
- Business Continuity zu erreichen.

---

## Kontakt

Jens Raschke  
Partner  
jens.raschke@bearingpoint.com

[www.bearingpoint.com](http://www.bearingpoint.com)