Kundeninformation "KRITIS"

id newmedia KnowHow - für *Sie ...*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

Was sind "Kritische IT Infrastrukturen" ?

Kritische Infrastrukturen sind Anlagen, Systeme oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionen nicht aufrechterhalten werden könnten. Infrastrukturen sind jedermann zugängliche staatliche oder private Anlagen oder Einrichtungen, die in einem festgelegten organisatorischen und/oder geographischen Bereich Dienstleistungen zur Verfügung stellen.

Dazu gehören auch die ablaufenden Prozesse, die eingesetzte Informationstechnik sowie die tätigen Arbeitskräfte. Kritische Infrastrukturen sind dementsprechend „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

"Kritisch“ bezieht sich auf die Systemrelevanz der Infrastrukturen, also auf die für das Gesamtsystem und die Daseinsvorsorge besonders bedeutsamen Einrichtungen.

Es bedarf auch des Schutzes kritischer Informationsinfrastrukturen (englisch *Critical Information Infrastructure Protection*, CIIP). „Kritisch“ meint hierbei nicht, dass die Eintrittswahrscheinlichkeit von Störungen hoch ist. Es ist vielmehr so zu verstehen, dass Störungen oder Ausfälle weitreichende Folgen bis hin zu katastrophalen Auswirkungen für Staat, Wirtschaft und/oder große Teile der Bevölkerung haben können.

 im Januar 2021

Über die Bedeutung

Kritische Infrastrukturen setzen sich zusammen aus technischen Basisinfrastrukturen und sozioökonomischen Infrastrukturen.

Technische Basisinfrastrukturen gewährleisten die Energieversorgung, die Trinkwasserversorgung sowie die Abwasserentsorgung und ermöglichen den Informationsaustausch, die Kommunikation sowie den Transport und den Verkehr bis hin zu Absatz- und Lieferketten.

Sozioökonomische Infrastrukturen betreffen die Nahrungsmittelversorgung, das Finanzwesen, die Rettungsdienste sowie die Versorgung mit Massenmedien und Kultur. Teilweise sind sie interdependent wie beispielsweise Transport und Nahrungsmittelversorgung (Lieferketten).

Aufgrund der Vernetzung kritischer Infrastrukturen sowohl sektorübergreifend als auch grenzüberschreitend bestehen starke, nicht-lineare Interdependenzen. Dies kann dazu führen, dass sich eine Störung von einem Betreiber einer kritischen Infrastruktur durch Kaskadeneffekt auf andere Betreiber ausbreitet und somit die Bevölkerung gefährdet.

Betreiber ist nach § 1 Nr. 2 BSI-KritisV eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.

Also auch ein "kleines" Unternehmen, welches sehr schnell "systemrelevant" werden kann.

Ein Risikomanagement-Prozeß umfasst im Einzelnen:

- Identifikation der Risiken, Beschreibung ihrer Art, der Ursachen und Auswirkungen

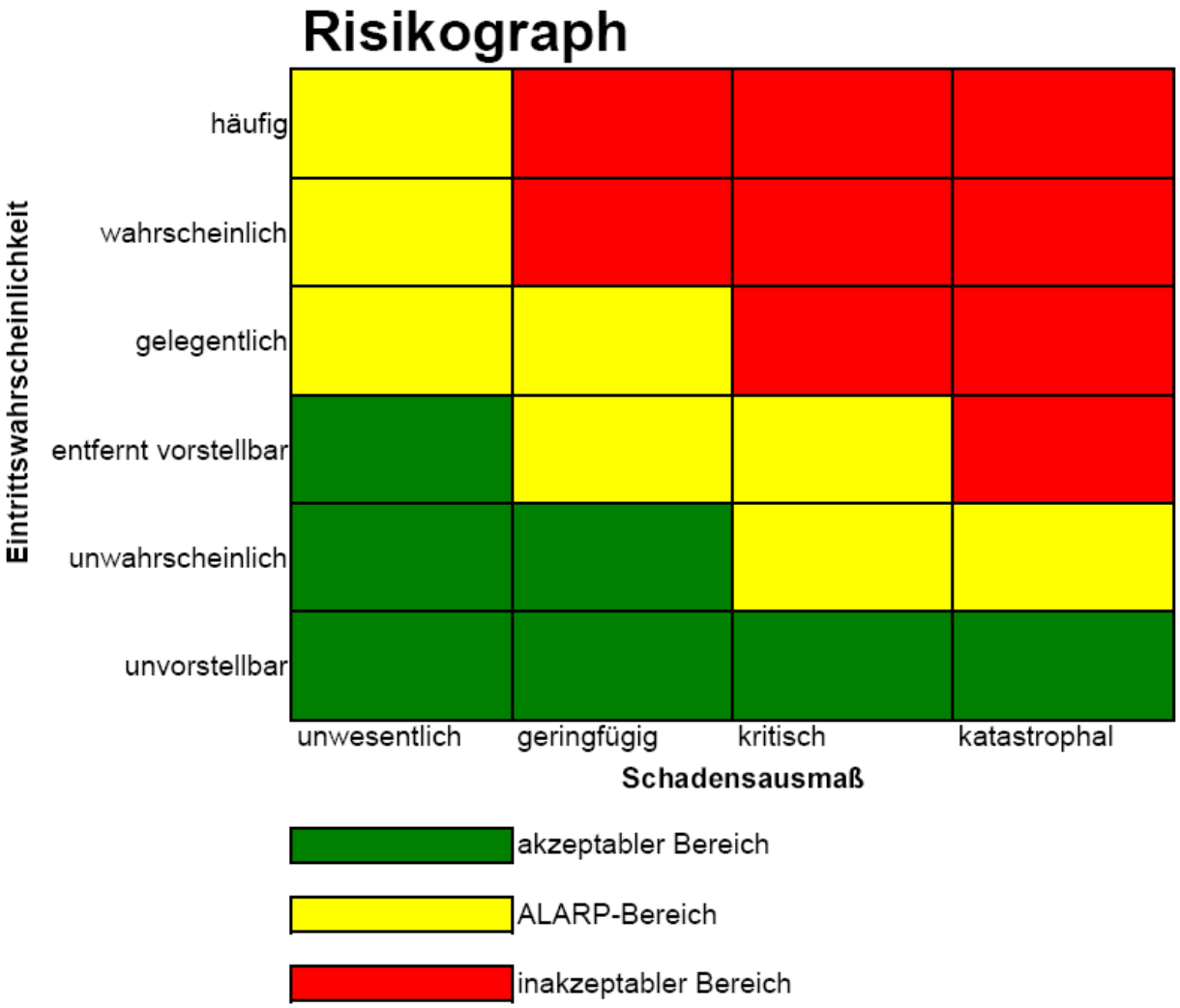
- Analyse der identifizierten Risiken hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen

- Risikobewertung durch Vergleich mit zuvor festzulegenden Kriterien der Risiko-Akzeptanz (z. B. aus Standards und Normen)

- Risikobewältigung/Risikobeherrschung durch Maßnahmen, die Gefahren und/oder Eintrittswahrscheinlichkeiten reduzieren oder die Folgen beherrschbar machen

- Risikoüberwachung mit Hilfe von Parametern, die Aufschluß über die aktuellen Risiken geben (Risikoindikatoren)

- Risikoaufzeichnungen zur Dokumentation aller Vorgänge, die im Zusammenhang der Risikoanalyse und -beurteilung stattfinden (ALARP : As Low As Reasonably Practicable).

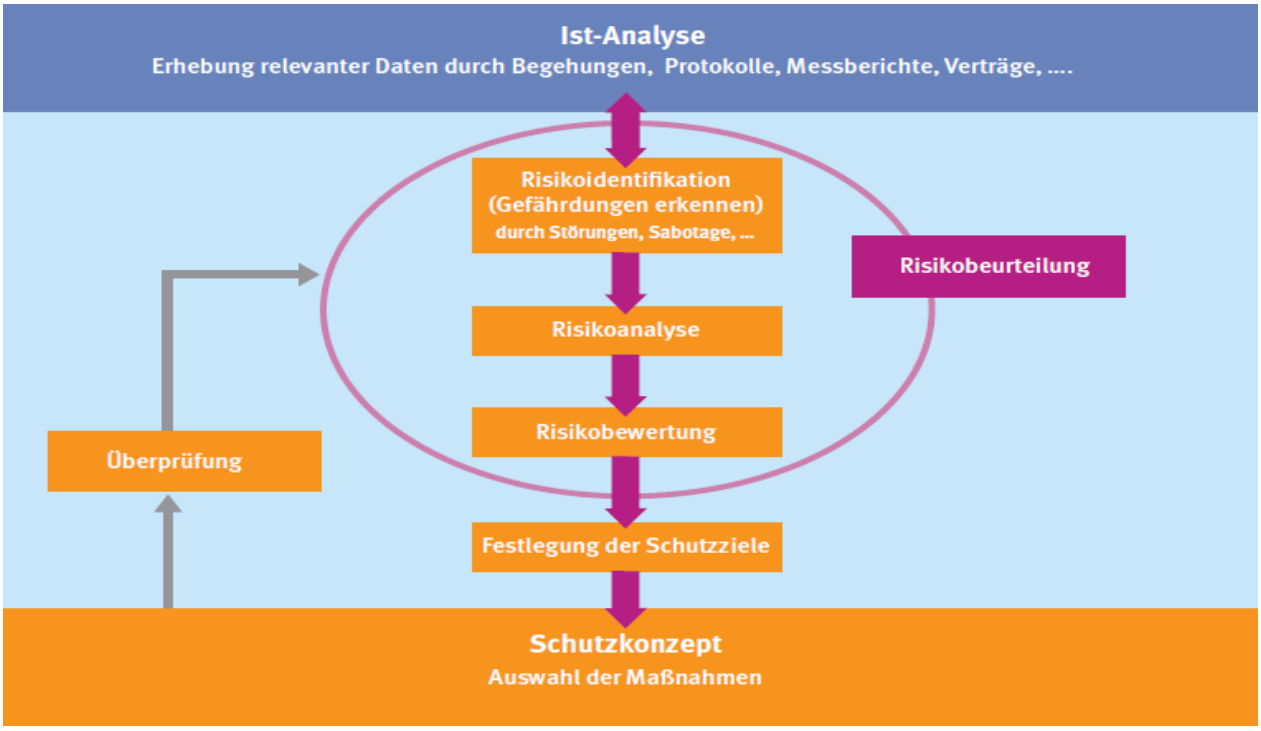


Wir unterstützen Sie bei :

der Prävention …
… so daß vorhandenen und zu erwartenden IT-Risiken im Vorfeld erkannt sowie kritische Elemente und Prozesse identifiziert werden, gravierende Störungen und Ausfälle von wichtigen Infrastrukturleistungen durch eine umfassende IT-Schutzvorkehr möglichst vermieden und durch ein vorhandenes effizientes Risiko- und Krisenmanagement sowie adäquate Handlungsoptionen auf ein Mindestmaß beschränkt werden.

der Reaktion …
… so daß Folgen von gravierenden Störungen und Ausfällen durch ein effektives Notfall- und Krisenmanagement und effiziente Redundanzen sowie eine wirkungsvolle Selbsthilfekapazität der unmittelbar Betroffenen so gering wie möglich gehalten werden; alle Aktivitäten im Stör- oder Schadensfall müssen darauf ausgerichtet sein, über ein Höchstmaß an Wirkung zu verfügen, damit der Regelbetrieb möglichst umgehend wiederaufgenommen werden kann.

der Nachhaltigkeit …
… so daß aus laufend fortgeschriebenen Gefährdungsanalysen sowie den Analysen von Störfällen und anderen Ereignissen im In- und Ausland Erfahrungen für den verbesserten Schutz Kritischer Infrastrukturen gewonnen und in gemeinsam mit Ihnen zu entwickelnde Schutzstandards wirtschaftlich verträglich umgesetzt werden können.



Quellen :
www.bmi.bund.de
www.bsi.de
id-newmedia "sichere IT-Infrastrukturen"