BearingPoint
RCS Capability Statement

- Cyber-Sicherheitscheck -

Juli 2015

BearingPoint®

Inhalt

Cyber-Sicherheit – eine Definition

Cyber-Sicherheit in Deutschland ist der anzustrebende Zustand der IT-Sicherheitslage, in dem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit (in Deutschland) entsteht durch die Summe von geeigneten und angemessenen Maßnahmen.

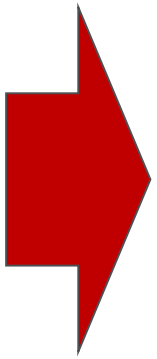
Cyber-Sicherheit basiert neben der Technik/IT und der generellen Kommunikationsinfrastruktur vor allem auf dem Faktor Mensch und umfasst weiterhin die sichere Verbindung physischer Einheiten (z.B. Maschinen und Steuerungseinheiten) mit dem Cyber-Raum.

Cyber-Sicherheit erweitert das Aktionsfeld der klassischen IT-Sicherheit auf den gesamten Cyber-Raum. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene IT und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

Es gibt einige Initiativen zur Cyber-Sicherheit in Deutschland

Definition von Anforderungen

- Nationaler Plan zum Schutz der Informationsinfrastrukturen
  - UP Bund
  - UP KRITIS
- Cyber-Strategie des Bundes
- Digitale Agenda
- Leitlinie IT-Sicherheit (IT-Planungsrat)
- eGov-Gesetz
- IT-SiG

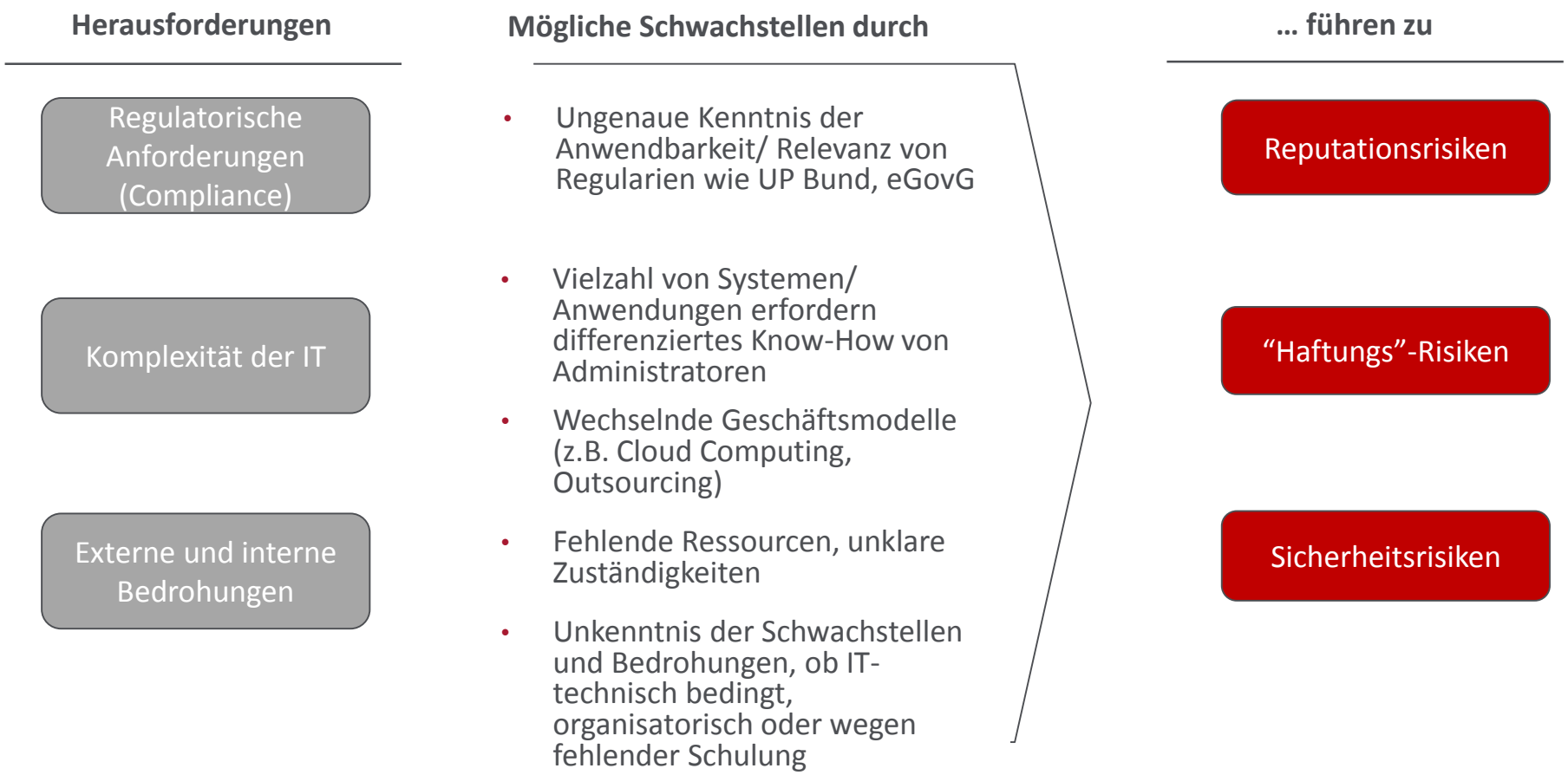


Umsetzung der Anforderungen

- Task-Force IT-Sicherheit
- Nationales Cyber-Abwehrzentrum
- Innenministerkonferenz der Länder
- Computer Emergency Response Team (CERT)
- LÜKEX
- Cyber-Allianz mit dem Cyber-Sicherheitscheck (in Zusammenarbeit mit ISACA)

Trotz dieser Initiativen zur Erhöhung der Cyber-Sicherheit …

sieht sich jede einzelne Behörde großen Herausforderungen gegenüber.



Übersicht des Methodenbaukasten für Assessments und Checks

Die Anwendung des Methodenbaukasten hat das Ziel einer bedarfsgenauen Analyse.

Dimension	Gestaltungsoptionen (Kurzbeschreibung)		
Welche Organisationseinheit wird untersucht?	Sparte / Bereich	Abteilung	Behörde
Wie wird die Untersuchung strukturiert?	Methoden-basiert: ISO / CS-Basischeck / COBIT, PCI-DSS		Kernfragen-/ Tool-basiert (Schwachstellen)
Wie wird untersucht?	Dokumentensichtung	Interviews / Workshops	OnSite-Test
Wie wird bewertet?	Best Practices (z.B. Standards)	Good Practices (Unternehmensbeispiele)	Benchmarks (Kennzahlen)
Wie werden die Ergebnisse strukturiert?	Analyse-Ergebnisse: Interner Fokus / Vergleichend	Optimierungs-Maßnahmen: Bewertet / Priorisiert / Operationalisiert	
Wie werden die Ergebnisse aufbereitet?	Abschlusspräsentation	Abschlussbericht	

Unsere Antwort auf diese Herausforderungen

Wir ermöglichen mit dem Cyber-Sicherheitscheck nachvollziehbare Lösungen und ein einheitliches Verständnis der Sicherheitssituation in einer Behörde.

Umfang des Checks Flexibilität in der Umsetzung

- Der Scope des Checks ist flexibel. Basis ist der Check der Cyber-Allianz
- Wir zeigen Vor- und Nachteile des jeweiligen Scopes auf.
- Umfang, Dimension und Tiefe sind frei wählbar.

Reifegrad-analyse

Geprüft wird anhand Mindestanforderungen des Basissicherheitschecks Ggf. ergänzt um BSI 100-2 Maßnahmen. Dies ergibt den Reifegrad.

Wechselwirkungs- und Risikoanalyse

- Abhängigkeiten und Schnittstellen werden erfasst und analysiert
- Diese Analyse wird den Risiken gegenübergestellt und bewertet.

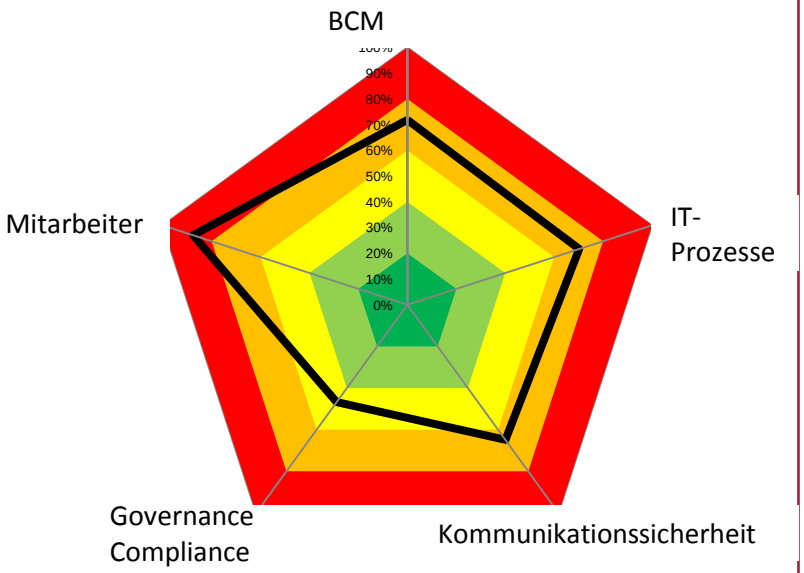
Maßnahmenempfehlung

- Maßnahmen auf Grundlage des Cyber-Allianz Basissicher-heitschecks
- Empfehlungen:
  - Roadmap
  - Bewertete Priorisierung

Risikoanalyse beim Cyber-Sicherheitscheck

Das Risikoprofil wird nach der Reifegradanalyse erstellt, um effektive Maßnahmen empfehlen zu können.

Risikoprofil (Bsp.)

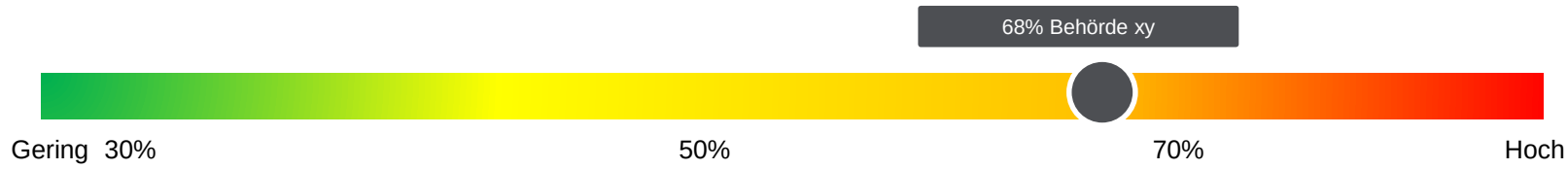


Zusammenfassung

Behörde xy sieht sich diversen Gefahren ausgesetzt, die bezogen auf verschiedene Domänen ein Risikoprofil ergeben. In diesem Beispiel hat die Behörde ein Risikolevel von 68%.

- Mitarbeiter kennen Cyber-Bedrohungen zu wenig.
- IT-Prozesse sind kritisch aufgrund interner und externer Abhängigkeiten und geeignete Maßnahmen für die kritischen Verwaltungsprozesse sind nicht ausreichend etabliert.
- Kommunikationsverbindungen und Authentifizierungsmechanismen sind z.T. ungenügend.
- Compliance ist größtenteils erreicht, aber nicht gesteuert und gemanagt.
- BCM wird nicht getestet.

Risikolevel



Unsere Methodik erlaubt horizontale (Vielfalt und Breite) und vertikale (Tiefe der Untersuchungsbereiche) Skalierung.

Cyber-Sicherheitscheck

Phase 1: Planung

Bestimmung von:

- Scope
- Ressourcen
- Zeit
- Umfang
- Tools
- …

Phase 2: Durchführung

Dokumenten-Check → Interview-Check → On-Site Check

1. Überprüfung der
   - Organisationsstrukturen zur Cyber-Sicherheit
   - Anwendbarkeit relevanter Regularien
   - Sicherheitsprozesse
   - Security-Produktportfolio
   - IT-Schwachstellen (APT, Botnetz etc.)

   → Feststellung des Reifegrades
2. Ermittlung von Bedrohungen

   → Risikoprofil
3. *Technischer Systemcheck (optional mit CP)*

Phase 3: Auswertung

Auswertung nach

- Kritikalität
- Wechselwirkung
- Reifegrad
- Priorität

Phase 4: Empfehlung

Ergebnisdarstellung

Umsetzungsplanung

Management Summary

Ergänzung des Basis Cyber-Sicherheitschecks

Mit dem Cyber-Sicherheitscheck nach BSI/ISACA bieten wir eine technische Überprüfung der Infrastruktur mit unserem Partner Checkpoint an.

In fünf Schritten zum technischen Security-Check mit Check Point SOFTWARE TECHNOLOGIES LTD.

1. Abgleich des Umfangs des technischen Sicherheitschecks auf Basis der Planungen des Basissicherheitschecks
2. Installation der Software Appliances für ein bis zwei Wochen
3. Test der Infrastruktur
   - Access Control
   - Threat Prevention (Botnet, Web Security Events etc.)
   - Endpoint Security
   - Compliance Check bezogen auf implementierte Policies
4. Auswertung (s. Bild)
5. Empfehlungen zur Reduzierung der Findings und Integration der Ergebnisse in den Abschlussbericht.

Application / Site	Matched Category	App Risk	Sources	Traffic	Number of Events
Tor	Anonymizer	Critical	35	149 MB	228
Ultrasurf	Anonymizer	Critical	33	1 GB	51
Coralcdn	Anonymizer	Critical	2	2 MB	45
VTunnel	Anonymizer	Critical	1	24 MB	18
Kugou	P2P File Sharing	Critical	2	7 MB	15
Suresome	Anonymizer	Critical	7	1 MB	9
Hola	Anonymizer	Critical	3	98 KB	4
PacketiX VPN	Anonymizer	Critical	2	3 KB	2
Kproxy	Anonymizer	Critical	1	4 KB	2
Sopcast	P2P File Sharing	Critical	1	61 KB	1
DarkComet-RAT	Remote Administration	Critical	1	561 Bytes	1
Dropbox	File Storage and Sharing	High	3573	37 GB	19443
GoToAssist-RemoteSupport	Remote Administration	High	1573	4 GB	5733
Lync	Instant Messaging	High	118	934 MB	1144
TeamViewer	Remote Administration	High	182	831 MB	768
BitTorrent Protocol	P2P File Sharing	High	113	168 MB	464
Lync-sharing	Instant Messaging	High	93	70 MB	443
uTorrent	P2P File Sharing	High	2	21 MB	327
QQ IM	Instant Messaging	High	30	26 MB	294
Free Download Manager	Download Manager	High	6	373 MB	257
AOL Desktop	Anonymizer	High	47	2 MB	233
ad.adlegend.com/iframe	Spam	High	3	32 MB	228
linkuryjs.info	Spam	High	2	85 MB	227
Dropbox-web download	File Storage and Sharing	High	2	3 MB	193
LogMeIn	Remote Administration	High	39	30 MB	179
digsby	Instant Messaging	High	36	5 MB	166
ZumoDrive	File Storage and Sharing	High	17	3 MB	148
AliWangWang	Instant Messaging	High	2	3 MB	140

Bsp. Findings

Unser Cyber-Sicherheitscheck ermöglicht auf effiziente und effektive Art und Weise die Ermittlung von Schwachstellen und Bedrohungen im relevanten Scope.

Nutzen

- Sie erhalten ein **vollständiges Bild** des Status Quo zur Cyber-Sicherheit (Lagebild) sowie Ihrer aktuellen Fähigkeiten und der Reife Ihrer Prozesse und Strukturen in Bezug dazu.
- Unser **strukturiertes und skalierbares Vorgehen** ermöglicht sowohl Effizienz als auch Effektivität bei gleichzeitiger Wahrung von Sorgfalt und Transparenz.
- **Individuelle Ansätze** sind realisierbar, bspw. kann ein technischer Check (Test der Systeme) mit unserem Partner Checkpoint erfolgen.
- Mit Hilfe des Cyber-Sicherheitschecks lassen sich die Mindestanforderungen als Key Performance Indikatoren definieren und für das **interne Monitoring** (Internen Kontrollsystems) nutzen.
- BearingPoint als Partner der Cyber-Allianz bringt Erkenntnisse und Erfahrungen aus erster Hand in das Projekt ein.

Ihre Ansprechpartnerin:

BearingPoint

Caroline Neufert
Senior Manager
BearingPoint
Kurfürstendamm 207-208
10719 Berlin
Germany

T +49 30 88004 2230
F +49 30 88004 100
M +49 174 33 51 127

www.bearingpoint.com

caroline.neufert@bearingpoint.com

BearingPoint®