Cyber-Index

Cyber-Sicherheit objektiv messen und vergleichen

Februar 2021

Sicherheit
Vergleichbarkeit
Transparenz

Cyber-Rating ist mehr als ein Fragebogen, Cyber-Rating ist ein Analyse-Instrument, zur Bestimmung der Unternehmenskultur in Bezug auf Datenschutz und Datensicherheit.

Technical problems can be remediated.
A dishonest corporate culture is much harder to fix.

Bruce Schneier, der „Security Guru“ (The Economist)

Glossar

Das Glossar enthält sprachliche Erläuterungen zu den im Text verwendeten (Fach)-Begriffen, um ein eindeutiges Verständnis zu ermöglichen.

Organisation	Als Organisation werden Unternehmen, Verwaltungen, Behörden, Vereine und wissenschaftliche Einrichtungen verstanden.
IT-Risikomanagement	Das IT-Risikomanagement besteht aus Risikoidentifikation, Risikoanalyse, Risikoquantifizierung, Risikoaggregation, Risikobeurteilung, Risikobewertung, Risikokommunikation und abschließender Risikobewältigung.
Zu schützende Werte (Assets)	hier: IT-Systeme, Daten, Software
Risiko	bezeichnet den möglichen Eintritt eines Schadensereignisses und ergibt sich aus der Summe der möglichen Schäden multipliziert mit der jeweiligen Eintrittswahrscheinlichkeit oder Risiko ist die Auswirkung von Unsicherheit auf Ziele $= \sum_{i=1}^{n} (LGEi \; x \; PEi)$ PE = Probability of Loss Events (Schadenseintrittswahrscheinlichkeit) LGE = Loss Given Event (Verlust bei Schadenseintritt = Schaden))
Operationelles Risiko	die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten.
Risikoart des operationellen Risikos	Risiken aufgrund von menschlichem und technischem Versagen oder externen Ereignissen

Kritischer Geschäftsprozess	Jeder Geschäftsprozess gilt als kritisch, dessen Zeitspanne zwischen Ausfall oder Störung und geregeltem Wiederanlauf zu einer nicht tolerierbaren Unterbrechung des operativen Geschäftsbetriebes führt.
Gefährdung	Die Gefährdung ist der Wahrscheinlichkeitswert einer Bedrohung bei Eintritt und setzt eine notwendige Anfälligkeit eines IT-/Informationsobjektes (Schwachstelle) voraus.
Schwachstellen	Schwachstellen im Unternehmen sind (noch) nicht geschlossene Sicherheitslücken Beispiele: nicht sensibilisierte Mitarbeiter, ungenügende Absicherung mobiler Endgeräte, unsichere Authentifizierung, keine Vorsorge, unsichere Kommunikation, …) Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.
Bedrohung	Potentielle Ursache für ein ungewolltes Ereignis, durch das dem Unternehmen, handelnden Personen oder Dritten Schaden entstehen könnte.
Schaden	Ein Schaden als materieller oder immaterieller Nachteil bezieht sich auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit.
Vertraulichkeit	Neben Verfügbarkeit und Integrität das wichtigste Sachziele in der Informationssicherheit: Schutz vor unbefugter Preisgabe
Verfügbarkeit	Das Maß oder die Wahrscheinlichkeit, mit der dem Benutzer Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung stehen.
Integrität	steht für die Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Einer Information können in der Informationstechnik bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder der Zeitpunkt der Erstellung manipuliert wurden.
Schutzbedarf	Der Schutzbedarf eines Objekts orientiert sich an dem Ausmaß der Schäden, die entstehen können, wenn seine Funktionsweise beeinträchtigt ist.
Schutzniveau	Ein hohes Schutzniveau bedingt ein geringes Risiko

Inhaltsverzeichnis

Glossar 3
Inhaltsverzeichnis 5
Situationsbeschreibung 6
Cyber-Rating, ein standardisiertes Verfahren 8
Aufbau des Cyber-Index 9
Außendarstellung 9
Schutzerfüllungsgrad 10
Schwachstellen-Scan 10
Verfahrensbeschreibung 11
Kategorieklassifizierung 13
Beispiel 14
Gesamtbewertung 16
Der Vergleich 18
Das Marketing 19
Foundation 19
Standard 19
Firmendarstellung 21
GSG Global Service Group GmbH 21
Prinzipien 22
Impressum 23

Situationsbeschreibung

Die technologischen Entwicklungen sind rasant und verändern alle Bereiche unseres Lebens, auch in der Wirtschaft. Grundsätzlich ermöglichen sie vielen Menschen mehr Wohlstand und mehr Lebensqualität. Doch die Chancen der Digitalisierung erkennt man auch auf der „dunklen Seite der Macht“. Dort werden Angriffsmethoden entwickelt und Bedrohungs-Szenarien geschaffen, um eigene wirtschaftliche Interessen zu verfolgen (Cyber-Kriminalität) sowie andere Unternehmen und Volkswirtschaften zu schädigen (Cyber-Sabotage).

Während also die Angriffsvektoren immer raffinierter und gefährlicher werden, müssen Unternehmen ihre Vermögenswerte, Daten, Mitarbeiter und Kunden mit wirksamen und angemessenen Sicherheits-Komponenten schützen.

Doch wie kann eine vernünftige Balance zwischen Wirtschaftlichkeit und Sicherheit aussehen?

Fehleinschätzungen und falsche Entscheidungen zur Unternehmenssicherheit können ein Unternehmen in eine ernste Schieflage bringen, obwohl alle wirtschaftlichen Kennzahlen stimmen. Der positiv ausgefallene Bonitätsindex konnte die drohende Gefahr aus dem Cyber-Raum nicht erkennen. Die aktuell zur Verfügung stehenden Instrumente zur Risikobewertung von Unternehmen sind also nicht mehr ausreichend, um über existenzgefährdende Cyber-Bedrohungen Auskunft zu geben.

Klassische Bewertungsinstrumente lassen außeracht, dass eine Cyber-Bedrohung sich von anderen Risiken in Ausgestaltung und Auswirkungen signifikant unterscheidet. Bereits eine kleine Schwachstelle kann sich bei einem Cyber-Angriff zu einer existenziellen Bedrohung für das Unternehmen und damit auch auf seine Partner auswachsen. Denn durch die komplexen wirtschaftlichen

Interaktionen und die verknüpften Kommunikationswege kann sich die Schwachstelle eines Gliedes der Wertschöpfungskette als Einfallstor zu allen weiteren beteiligten Unternehmen erweisen.

Wie aber kann ein Unternehmen selbst erkennen, welche Qualität sein Sicherheitsniveau besitzt? Und – vielleicht noch wichtiger: Welcher Sicherheitsstandard wird bei seinem Partner gelebt?

Bislang fehlten Methodik und Erfahrungswerte, um das Niveau der Unternehmenssicherheit durch eine geeignete Kenngröße auszudrücken und vergleichbar zu machen. Das Cyber-Rating schließt diese Lücke.

Cyber-Rating, ein standardisiertes Verfahren

Das Cyber-Rating ermöglicht es, das aktuelle Sicherheitsniveau eines Unternehmens zu erkennen, zu vergleichen und seine IT-Sicherheit zu verbessern.

Damit erfüllt das Cyber-Rating die seit langem geforderte Existenz eines Bewertungsverfahrens zur Beurteilung der Cyber-Sicherheit von Unternehmen und anderen Organisationen. Es ergänzt die Aussage eines Bonitätsindex über die wirtschaftliche Stabilität eines Unternehmens um den Aspekt seiner Unternehmenssicherheit.

Der durch das Cyber-Rating erstellte Cyber-Index bezieht sich auf die operationellen Risiken in der Informationstechnologie. Er trifft durch einen Score zwischen 1 und 9 eine individuelle Qualitätsaussage für jedes Unternehmen. Auf diesem Ergebnis kann aufgebaut werden: Durch gezielte Beratung und Unterstützung werden Fortbestand und das wirtschaftliche Wachstum von Unternehmen gesichert, indem Cyber-Angriffe entweder verhindert oder frühzeitig erkannt und erfolgreich abgewehrt werden können.

Aufbau des Cyber-Index

Der Cyber-Index besteht aus Bewertungen der internen und externen Risiken des Unternehmens. Er setzt sich aus gewichteten Faktoren zusammen, die in die nachfolgend beschriebenen drei Komponenten einfließen. Aus diesen Risikofaktoren und den daraus generierten Kennzahlen ergibt sich ein genormter, vergleichbarer und einschätzbarer Cyber-Index, der es erlaubt, den Ausfall der Kernprozesse eines Unternehmens statistisch vorherzusagen.

Außendarstellung

Zur Bestimmung externer Risiken werden die wirtschaftlichen Rahmenbedingungen untersucht, unter denen das Unternehmen tätig ist und die von außen auf das Unternehmen einwirken. Sie ermöglichen die Risikoeinordnung des Unternehmens aufgrund von Makro-Faktoren wie Branche, Größe, Geschäftsfeld und Geschäftsmodell. Zur Bestimmung werden statistische Korrelationen zwischen den Makro-Faktoren und der Exposition für Cyber-Angriffe sowie deren Art und Ausmaß zugrunde gelegt. Ebenfalls fließt ein Transparenz-Faktor ein. Er bezeichnet die Außendarstellung des Unternehmens und weist aus, in welchem Ausmaß Informationen von und über das Unternehmen öffentlich zugänglich sind und von unternehmensfremden Personen verwendet werden können (z.B. für Social Engineering). Diese Kennzahl kann durch das Unternehmen nicht oder nur unter größten Anstrengungen (Veränderung des Geschäftsmodells, Wechsel der Branche etc.) verändert werden.

Schutzerfüllungsgrad

Die internen Sicherheitsrisiken bestimmen sich aus dem Schutzerfüllungsgrad des Unternehmens. In welchem Umfang und in welchen Formen ist IT-Sicherheit aktuell implementiert? Die Bestimmung dieser Kennzahl erfordert eine Mitwirkung des Unternehmens, da hier unternehmensinterne Mikro-Faktoren in organisatorischer, personeller und technischer Hinsicht einfließen (z.B. Existenz von Richtlinien, Bestellung Beauftragte/r, Einstellungen in den Firewalls, Netzwerksicherheit, Reifegrad Datenschutz etc.). Die erforderlichen Informationen werden über standardisierte Fragebögen (Selbsteinschätzung) oder zusätzlich über Validierung der Angaben durch spezielle Audits erhoben. Auf die internen Faktoren kann das Unternehmen durch Maßnahmen aktiv einwirken und durch sein individuelles Sicherheitsverhalten eine Verbesserung oder Verschlechterung des Wertes generieren.

Schwachstellen-Scan

Neben dem organisatorischen Audit können technische Schwachstellen-Scans durchgeführt werden. Durch den Einsatz von Scan-Tools werden beispielsweise IP-Adressen und Hosts überprüft und offene Ports bzw. Schwachstellen, durch welche Angreifer eindringen können, kenntlich gemacht.

Verfahrensbeschreibung

Das Cyber-Rating soll Unternehmenssicherheit sowohl untereinander als auch gegenüber einer definierten Gesamtmenge als ausgewiesene Norm vergleichbar machen. Die Gesamtmenge ist durch die freundliche Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) / die Allianz für Cybersicherheit erhalten worden. Nachdem die Fragen für die Cyber-Sicherheit-Umfrage 2017 durch uns entwickelt wurden, hat das BSI zur Teilnahme an der Umfrage aufgerufen.

Durch diese sowie unsere eigene Bewerbung sind dem Aufruf 879 Organisationen gefolgt. Damit konnten wesentlich mehr Unternehmen als in den Vorjahren angesprochen werden. Die Teilnahme der Unternehmen an dieser Umfrage war vollkommen anonym. Daher kann davon ausgegangen werden, dass die Antworten keiner Verfälschung (Falschangaben aus Imagegründen) unterliegen.

Nach der Validierung dieses Gesamtbestandes wurden 875 Datensätze für die weitere Untersuchung zugelassen. Die Umfrage selbst teilt sich in 3 Blöcke ein

- Einschätzung (subjektive Gefährdungslage) und Betroffenheit durch Cyber-Angriffe
- Umsetzungsgrad entsprechender Schutzmaßnahmen (Stand der Informationssicherheit im Unternehmen)
- Statistische Angaben zum Unternehmen

Die Bewertung der Cyber-Sicherheit erfolgt vorwiegend aus den Fragen des mittleren Blocks, also den Fragen, die die innere Sicherheit des Unternehmens erkennen lassen und somit auch die Wirksamkeit der dort getroffenen Maßnahmen, was auch als Reifegrad des Unternehmens bezeichnet wird.

Die Fragen und deren Antworten sind unterschiedlichen Auswertung unterzogen worden. Das generelle Ziel ist der Erhalt eines kumulierten Wertes, der eine

konkrete Aussage über die Gefährdungslage einer Organisation geben soll. Dieser Wert wird als der Cyber-Index bezeichnet.

Dafür wurde das gesamte Spektrum der Cyber-Sicherheit zur besseren Übersichtlichkeit in mehrere Kategorien eingeteilt (ähnlich dem BSI-Grundschutz). Die unterschiedlichen Gefährdungen wurden diesen Kategorien passend zugeordnet. Demgegenüber steht ein zu ermittelnder Reifegrad der jeweiligen Organisation.

Kategorieklassifizierung

Folgende Kategorien sind erstellt worden:

IT-Infrastruktur	*Eine optimal funktionierende IT-Infrastruktur ist die Basis für eine effektive und sichere Nutzung der IT. So werden dieser Kategorie der IT-Betrieb, die Server-Anwendungen und die Management-Services zugeordnet*
IT-Systeme	*Diese Kategorie umfasst die einzelnen IT-Systeme, wie Server, Desktops, Mobile Devices und Drucker. Darüber hinaus gehören in diese Kategorie die Client-Anwendungen und die Verzeichnis- und Netzdienste*
Netzwerke	*Diese Kategorie behandelt die Sicherheitsaspekte von Netzen, Netzverbindungen und Kommunikation zwischen den IT-Systemen.*
Organisation	*In diese Kategorie fallen alle betrieblichen Organisationsprozesse als auch alle personalbezogenen Aspekte.*
Prävention	*Vorzeitiges Erkennen und Reagieren dienen der Prävention zur Minimierung von Sicherheitsvorfällen. In dieser Kategorie werden auch diejenigen Gefährdungen behandelt, die dann entstehen, wenn bereits ein Schaden eingetreten ist.*
Datenschutz	*Im Zuge der verschärften Anforderungen zur Erreichung der Compliance durch die EU-Datenschutzgrundverordnung (DSGVO) in Übereinstimmung mit dem neuen Bundesdatenschutzgesetz (BDSG neu) sind nicht nur bei Nichterfüllung wesentliche höhere Sanktionen zu erwarten, sondern durch die Verletzungen von Persönlichkeitsrechten können materielle und auch immaterielle Schadensersatzansprüche geltend gemacht werden. Eine Beachtung der Datenschutzauflagen ist nicht nur aus wirtschaftlichen Gesichtspunkten sinnvoll, sondern*

	personenbezogene Regelungen und Verfahrensweisen führen auch zu einer Erhöhung des Sicherheitsniveaus.
Unternehmen	*Gebäude, Räume, IT-Verkabelung, somit die gesamte Unternehmens-Infrastruktur sind in dieser Kategorie enthalten. Darüber hinaus findet sich hierin auch die Auswertung der Cyber-Sicherheits-Exposition des Unternehmens, also die Darstellung nach außen, welche schützenswerte Informationen sind öffentlich verfügbar (Webseiten, Foren, …). Wegen der notwendigerweise vorzunehmenden Personalisierung der Organisation gehört diese Kategorie nicht zu den vergleichbaren Standardbetrachtungen.*
Schwachstellen Scan	*In dieser Kategorie werden einmalige, als auch kontinuierliche Scans beschrieben. Wegen der notwendigerweise vorzunehmenden Personalisierung der Organisation gehört diese Kategorie nicht zu den vergleichbaren Standardbetrachtungen.*

Der Reifegrad der Organisation ergibt sich aus den Antworten der hierfür relevanten Fragen. Diese Antworten werden aufgrund ihrer aktuellen Gefährdung bewertet.

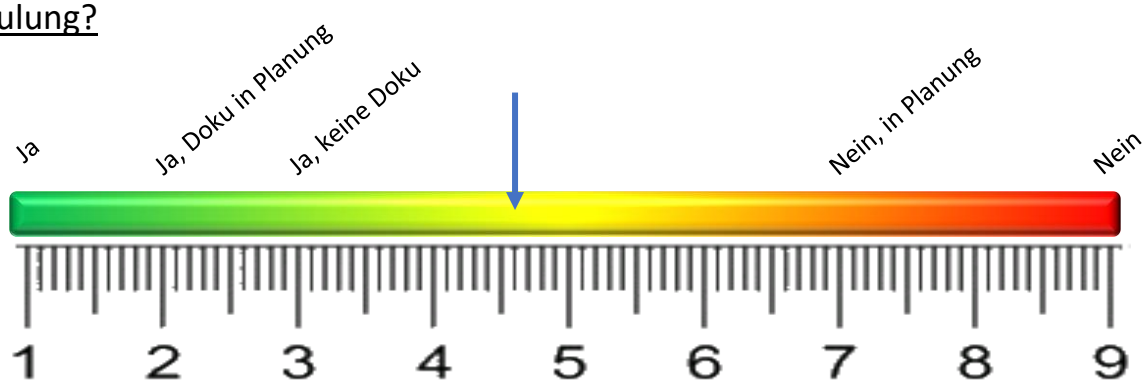
Beispiel

Die Behandlung der Frage zu *Sensibilisierung und Schulung* ist der Kategorie *Organisation* zugewiesen. Die Bewertung dieser und analoger Antworten sind nach einer Risikoskala von 1 bis 9 bewertet (geringes Risiko = 1, hohes Risiko = 9). Die Frage und deren Antwortmöglichkeiten haben folgenden Wortlaut:

Frage	*Wird das Personal in regelmäßigen Abständen in Bezug auf die IT-Sicherheit geschult und die Durchführung dieser Schulungen dokumentiert?*	*Anzahl* *875*
01	keine Angabe	26
02	ja, es wird geschult und dokumentiert	268
03	ja, es wird geschult und nicht dokumentiert	162
04	ja, es wird geschult, die Dokumentation ist in Planung	67
05	Nein	252
06	In Planung	100

Die Verteilung der Anzahl der abgegebenen Antworten ist in der letzten Spalte (Anzahl) berücksichtigt. Mittels eines auf die Fragen zugeschnittenen Bewertungsverfahrens erhält man die nachfolgend dargestellte Graphik. Die Antwort *keine Angabe* bleibt unberücksichtigt.

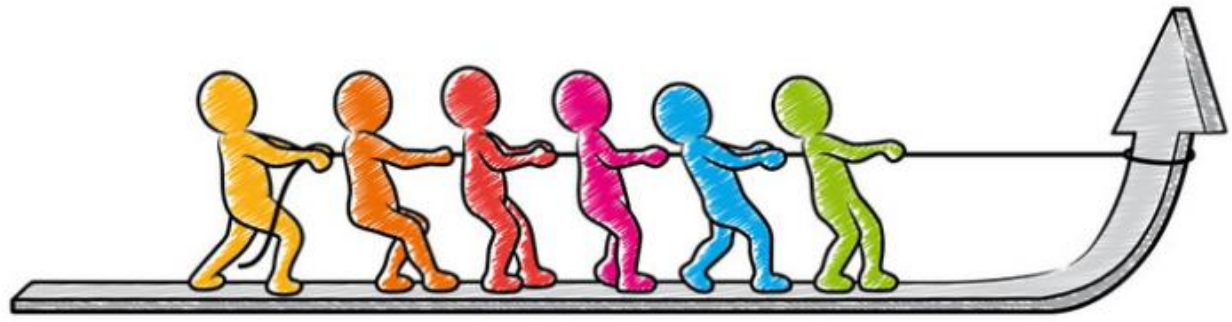
<u>Schulung?</u>



Die Gesamtheit der jeweils abgegeben Antworten wird als der Schutzerfüllungsgrad bezeichnet. Die Bestimmung des Risikoindex dieser Frage ergibt sich somit aus:

$$\text{Risikoindex} = \frac{\sum_{i=1}^{n}(Schutzerf\ddot{u}llungsgrad(i) * Bewertungsfaktor(i))}{n}$$

zu einem Wert von 4,6



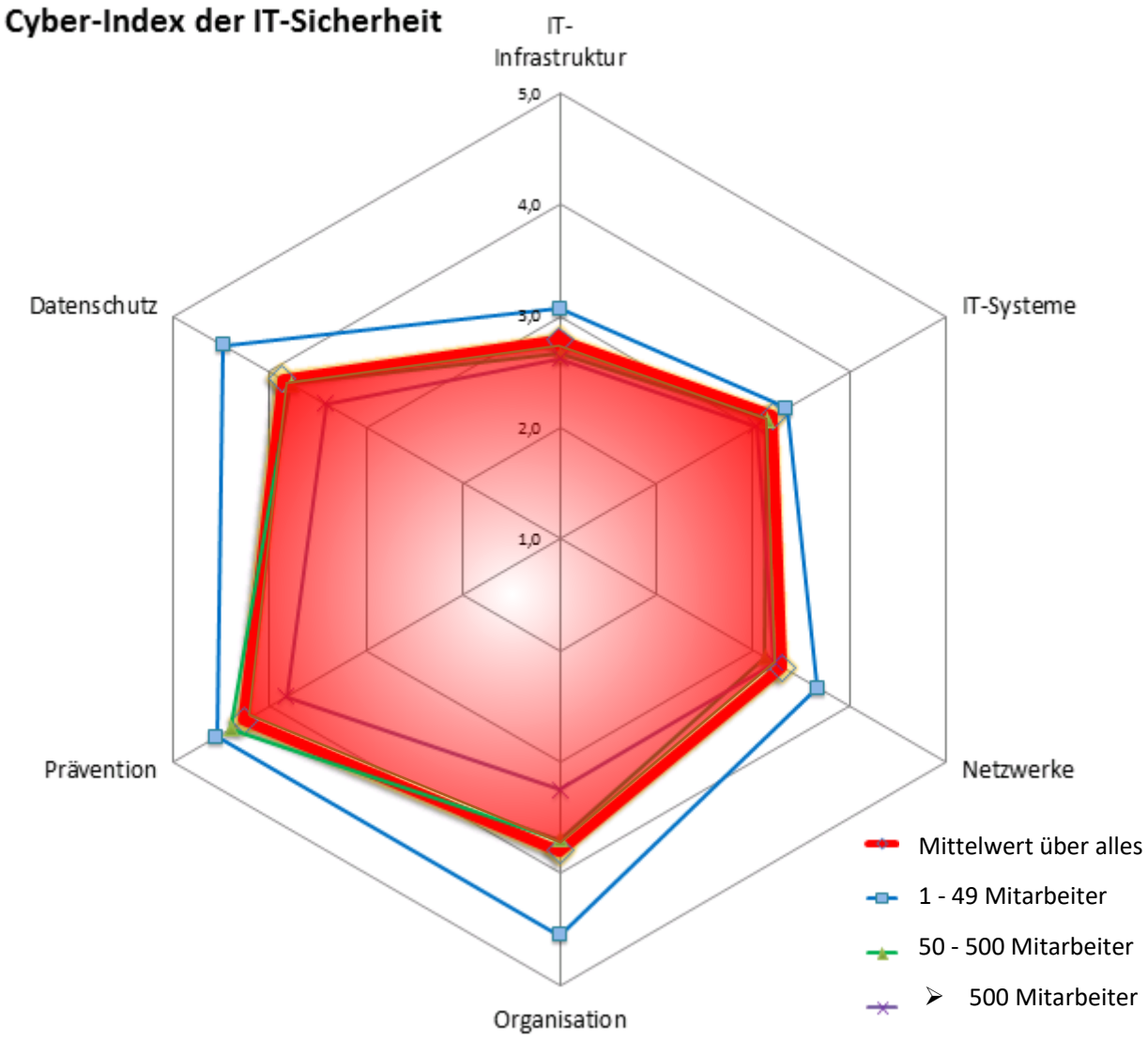
Gesamtbewertung

Die Einordnung der Antworten in die vorgestellten Kategorien und die Berechnung der je nach Inhaltsbezug bestimmten Risikoindizes kann nun in einem Spinnendiagramm am deutlichsten dargestellt werden.

Das nachfolgende Diagramm stellt den Bezug zu der Größe einer Organisation dar, welche über die Anzahl der Mitarbeiter definiert wird. Der über die Gesamtheit der teilgenommenen Organisationen ermittelte arithmetische Mittelwert ist in dieser Darstellung rot gekennzeichnet und steht für den eigentlichen Vergleich weiterer zu untersuchenden Unternehmen zur Verfügung.

Die Unternehmensgröße von 50-500 Mitarbeiter stellt dabei einen repräsentativen Mittelwert dar, wohingegen kleine Unternehmen ein in allen Kategorien schlechteres Ergebnis abgeben, die größeren Unternehmen sind vergleichsweise besser aufgestellt.

Dieses Ergebnis ist nicht überraschend, denn kleine Unternehmen können aufgrund ihrer Masse die IT-Sicherheits-Anforderungen in der geforderten Form nicht erfüllen, größere jedoch schon eher.


Cyber-Index der IT-Sicherheit
IT-Infrastruktur
IT-Systeme
Netzwerke
Organisation
Prävention
Datenschutz
5,0
4,0
3,0
2,0
1,0
Mittelwert über alles
1 - 49 Mitarbeiter
50 - 500 Mitarbeiter
500 Mitarbeiter

Der Vergleich

Ein Vergleich mit der eingeschlossenen Fläche ist allein nicht repräsentativ. Sinnvoller erscheint ein zusätzlich gewichteter Vergleich mit der direkten Kategorie-Differenz. Genauere Untersuchungen an der Gesamtheit eingangs erwähnter Umfrage zeigen, dass die vorgenommene Kategorie-Zusammenstellung eine erkennbare Trennschärfe besitzt, was die Einteilung auf diese Art und Weise bestätigt.

Es wird auch erkennbar, dass der Großteil (genauere Zahlen können in der BSI-Studie *Cyber-Sicherheits-Umfrage 2017* nachgelesen werden) der teilnehmenden Organisationen sich den wesentlichen Herausforderungen der IT gestellt haben. So kann auch erkannt werden, dass die Absicherung der IT-Infrastruktur und der IT-Systeme einen hohen Stellenwert besitzen, wohingegen organisatorische Maßnahmen, Prävention und Datenschutz weiteres Potential für eine sinnvolle Steigerung des Sicherheitsniveaus bieten.

Die Veränderung des Sicherheitsniveaus in den Unternehmen und die Verschiebung der Angriffsvektoren wird das vorgestellte Cyber-Risiko-Verfahren durchaus dynamisch gestalten, indem das arithmetische Mittel sich verschieben wird. Dieser Zustand führt jedoch dazu, Anpassungen vorzunehmen, die sich wiederum in einem geänderten Risiko-Wert niederschlagen werden. Eine Maßgabe, die der Veränderung in der Cyber-Sicherheit Rechnung tragen kann.

Das Marketing

Für das unternehmenseigene Marketing bietet sich das Cyber-Rating als Gütesiegel zur Außendarstellung an, welches je nach Interessenslage der Organisation eine entsprechende Ausprägung verleiht.

Foundation

Das Angebot zeichnet sich durch eine vorzunehmende Selbsteinschätzung der eigenen Sicherheit aus. Hierfür wurde ein Fragebogen-Komplex erstellt, der weite Teile der Unternehmens-Sicherheit beleuchtet, wobei der Ergebnisprozess praktisch automatisch abläuft. Das Unternehmen erhält nach Beantwortung aller Fragen den ermittelten Cyber-Index, eine Beurteilung und einen angedeuteten Maßnahmenplan.

Die Fragen sind so ausgelegt, dass sie auch die Ermittlung eines Expositons-Koeffizienten gestatten, der angibt, wie sich das Unternehmen nach außen darstellt und wie stark sich Hacker an der angebotenen Informationenfülle orientieren können.

Das Unternehmen kann hieraus einen enormen Nutzen erzielen, denn es besteht die Möglichkeit der Kostenermittlung bezüglich der vorgeschlagenen Maßnahmen.

Dieses Angebot kann über einen Testzugang kostenfrei durchgeführt werden.

Standard

Der gleiche Fragebogen-Komplex steht auch dem Standard-Angebot zur Verfügung, jedoch wird die Selbsteinschätzung durch ein Security-Audit im Unternehmen erweitert, wodurch qualitativ hochwertige validierte Aussagen erhalten werden.

Darüber hinaus können zusätzlich vorhandene Schwachstellen im Unternehmen mittels automatisierten Scans untersucht und dokumentiert werden. Dieser Schwachstellen-Scan geht genauso wie der Expositions-Koeffizient in das Cyber-Rating mit ein und kann dadurch auch den Cyber-Index beeinflussen.

Firmendarstellung

Die Cyber-Rating Analyse, als eigene Marke der GSG GmbH, ist ein spezifisches Produkt der IT-Security Suite.

GSG Global Service Group GmbH

Die Global Service Group GmbH (GSG) trägt die Verantwortung für die ordnungsgemäße Durchführung der Management- und Organisations-Aufgaben. Bei ihr sind alle Verfahren, Fragen, Datenbanken und Auswertungen verortet, da auch bei ihr das Hosting des Systems erfolgt.

Das Unternehmen bietet Schulungen, Workshops und Seminare an und wählt sorgfältig Partner und Experten für beratende und ausführende Tätigkeiten bei den Kunden aus.

Für die Durchführung der Aufgaben und für die korrekte Ausführung des Verfahrens sind Prinzipien auferlegt worden, die verpflichtend einzuhalten sind. Diese sind im Folgenden dargelegt.

Prinzipien

Sicherheitsbewertungen basieren auf genauen und relevanten Informationen, nützlichen Werkzeugen zur Bewertung von Cyberrisiken und zur Ermöglichung kollaborativer, risikobasierter Gespräche zwischen Organisationen.

Alle Bereiche der Cyber-Rating Organisation haben sich die folgenden Grundsätze zur fairen und genauen Sicherheitsbewertung auferlegt:

1. wir fördern die Qualität und die Genauigkeit bei der Erstellung von Sicherheitsbewertungen
2. wir unterstützen und fördern die Fairness in der Berichterstattung
3. zur Korrektur von Fehlern und Ungenauigkeiten existiert ein entsprechend koordinierter Prozess
4. für eine angemessene Verwendung und Offenlegung von Score und Rating existieren angepasste Richtlinien.

Darüber hinaus gibt es Verfahren zur Absicherung der Kommunikationswege:

> Wir setzen SSL-Zertifikate ein, so dass eine Punkt-zu-Punkt Verschlüsselung gewährleistet ist. Das SSL-Protokoll ermöglicht eine gesicherte HTTPS-Verbindung zwischen unseren Webservern und den eingesetzten Browsern. Mit einer solchen SSL-Verschlüsselung kann dieser Website absolut vertraut werden. Dieses Verschlüsselungsverfahren wird zumindest auch teilweise bei der Übertragung der Emails eingesetzt, auf jeden Fall ist die Kommunikation mit PDF-Dateien über ein selbst vergebenes Passwort geschützt.

Weiterhin besteht das Unternehmen aus zertifizierten Datenschutzbeauftragten, die per se der Verschwiegenheit verpflichtet sind.

Impressum

Hausgeber

Die GSG Global Service Group GmbH, Darmstädter Straße 53, 64354 Reinheim, ist der Herausgeber dieser vorliegenden Dokumentation.

Die Erstellung dieser Abhandlung erfolgte durch Dr. Frank H. Thiele unter Mitwirkung von

Kanya Pawlewicz-Rupp	Marketing und Vertrieb
Gregor Oelze	Technik und Gestaltung

Email: f.thiele@gsg-edv.de

Telefon: 06162 1051

Telefax: 06162 1055

Stand:

Februar 2021

Fotolia-Bilder:

- 106800360	Cyber-Logo
- 187019321	Glossar
- 165391630	Inhaltsverzeichnis
- 163979617	Situationsbeschreibung
- 175763088	Cyber-Rating ein standardisier …
- 174282950	Aufbau des Cyber-Index
- 188934440	Verfahrensbeschreibung
- 143668936	Kategorieklassifizierung
- 151554586	Gesamtbewertung
- 104667374	Der Vergleich
- 163262135	Das Marketing
- 141678996	Firmendarstellung
- 127839156	Impressum

Dokument-Einstellungen:

Design:	Kondensstreifen
Farbenauswahl:	Dactylos / Rotviolett
Textfont / Größe:	Century-Gothic / 14