T · M · B | Service

IT´s time for Security

Sicherheitsbewusstsein in der IT

www.tmb-service.de/it-sicherheit

T·M·B

IT´s Time for Awareness

Vorwort

Wir sind Ihr IT-Security Provider

PEN-Test

Forensik

Health-Check

audIT

Stand der Technik

Kontinuierliche Verbesserung

Vorwort

Wichtig für eine zielführende IT-Security-Strategie ist das Know-How und die Ressource dahinter. Das Thema IT-Security ist nicht nur ein Arbeitsplatz mit einem verantwortlichen Mitarbeiter dahinter, sondern eine Berufung. Da es ausnahmslos wichtig ist, die aktuellen Normen, Leitlinien und gesetzlichen Bestimmungen zu kennen und diese zielführend umgesetzt zu bekommen.
Aufgeführte möchte ich Ihnen gern folgende gesetzliche Vorgaben (**DSGVO**, **BSI**, **ISO**) einmal etwas näher bringen, damit Sie wissen, welchen Maßgaben diese Leitlinien für die IT-Sicherheit haben.

DSGVO: Wenn man sich aus Interesse einmal die DSGVO durchließt, ist mit dem Art. 5 Abs. 1 f) die erste Vorgabe getroffen, die es in sich hat. Da steht: *[…] personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“),*
Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen auch genannt als *„Data protection by design and by default –* bedeutet nichts anderes als: geeignete technische und Organisatorische Maßnahmen unter Berücksichtigung des Stand der Technik umzusetzen sind.
Weiter geht es in Art 32, da werden folgende Skizzierung als bindlich definiert, wie z.B: *Verschlüsselung und Pseudonymisierung, Vertraulichkeit, Integrität, Wiederherstellbarkeit, Belastbarkeit, Verfügbarkeit und die Zweckbindung.*

BSI-Grundschutz:
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Das BSI verlangt die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen. Daher hat der BSI mit seinem IT-Grundschutz-Kompendium eine bewährte Methodik entwickelt, um das Niveau der Informationssicherheit in Behörden und Unternehmen JEDER Größenordnung zu erhöhen.
Der IT-Grundschutz ist in 5 Richtlinien unterteilt: BSI-Kompendium, BSI-Standard 100-4, 200-1, 200-2 und 200-3.

ISO 27000 Familie:
Durch die aufgeführte ISO Familie werden internationale Sicherheitsstandards formuliert und die Einrichtung, Implementierung, Betrieb, Überwachung, Überprüfen (Monitoring), Pflege und Verbesserung als Anforderung beschrieben. Diese sollen helfen eine erträgliche Sicherheit herzustellen und Schwachstellen zu erkennen und die daraus resultierende Härtungsmaßnehmen fortführend umzusetzen. Wichtig für die erfolgreiche Umsetzung sind folgende DIN-Normen: 27001 (Anforderung), 27002 (Leitfaden für Informationssicherheitsmanagement),
27003 (Anleitung zur Implementierung), 27004 (Messung), 27005 (Risikomanagement).

T·M·B

IT´s Time for Awareness

Wir sind Ihr IT-Security-Provider

Sie kennen es auch; es wurde in den letzten drei, vier Jahren viel Werbung zu dem Thema IT-Cloud gemacht, wie z.B. ***„Einfach sicher – Das Zuhause für Ihre Daten“, „Die Zukunft der Cloud beginnt jetzt“*** oder, was ich als Werbung gefunden habe, ist ein Logo mit einem ®. Das schaut erstmals vertrauenswürdig aus, richtig?
Verkaufstechnisch gesehen, eine tolle Überschrift, die sich in der Breitenauswirkung gut lesen lässt. Aber was noch verwirrender ist, ist dass die bekanntesten Cloud Anbieter wie Dropbox, Google Drive und Microsoft OneDrive noch spannender werben. Man liest oft, dass deren Cloud nach ***ISO 27001*** zertifiziert ist; jedoch bedeutet das nicht automatisch, dass die Daten dort sicher sind.
In puncto Datenschutz sind wir aber als Bundesbürger seit dem 25. Januar 2017 in den USA als Internetnutzer „zweiter Klasse“ gesetzt. Denn der aktuelle US-Präsident, Donald Trump, hat per Verordnung im Januar 2017 erklärt, dass Nicht-US-Bürger vom US-amerikanischen Datenschutzrecht ausgeschlossen oder zumindest deren Rechte diesbezüglich eingeschränkt werden.

Unser **S**ecurity **O**peration **C**enter (SOC) bietet eine rechtzeitige und genaue Identifizierung sicherheitsrelevanter Ereignisse, um sicherzustellen, dass wir mit Ihnen auf gültige Bedrohungen reagieren, damit Ihre kritischen (digitalen) Vermögenswerte jederzeit angemessen geschützt sind. Zusätzlich zur Überwachung und Alarmierung reagieren wir auf Cyber Vorfälle in Echtzeit.

In der TMB SOC analysieren erfahrene Mitarbeiter Bedrohungen und Vorfälle mit der eigens von TMB Security entwickelten Global Managed Security Plattform, um Vorfälle zu erfassen, zu analysieren, zu identifizieren und um Maßnahmen zur aktuellen Abwehr weiter zu entwickeln um unseren Managed Security Service weiter auszubauen.

Managed Security Services (MSS) von TMB

Betrieb: Als Reaktion auf fortlaufende technische Änderungen der IT-Systeme auf Grundlage von übergelagerten gesetzlichen bzw. herstellerübergreifenden neuen sicherheitsrelevanten Bekanntmachungen beim Stand der Technik, werden umgehend zielgerichtete systemseitige Veränderungen dokumentierte & transparente Security Prozesse ausgeführt.

Management: Mit erstklassiger künstlicher und menschlicher Intelligenz entwickeln wir Schutzmaßnahmen, um Angriffsmethoden und -taktiken gezielter Bedrohungen und Sicherheitslücken vorzubeugen. Wir bemerken diese im voraus oder sehen dies durch unsere eingesetzte Security-KI frühzeitig und ergreifen rasch die notwendigen Sicherheitsmaßnahmen und setzen diese nach aktuellem Stand der Technik umgehend um. Damit können wir gewährleisten, dass wir mit unserem MSS Ihre IT-Infrastruktur und Systeme immer „**up to date**“ halten.

Optimierung: Durch unsere Erkenntnisse aus weltweiten Aktivitäten und Kundenprojekten, sowie umfassendem Sicherheits-Know-How zur Verbesserung der Sicherheitsabläufe, können wir Ihre IT-Infrastruktur verstehen und sicherheitstechnisch optimieren. Wir stehen an Ihrer Seite als verlängerte Werkbank!

Vorteile:
Auch gängige Serverbetriebssysteme (z.B. Microsoft Windows Server oder Linux Server) besitzen standardmäßig keine sehr restriktive Sicherheitskonfiguration und sind potentiell mit ungenutzten Sicherheits-Komponenten ausgestattet. Gerade diese ungenutzten und nicht konfigurierten Funktionalitäten werden häufig als Einfallstor von Angreifern missbraucht. Deshalb konfigurieren, aktivieren, pflegen und Warten wir fortlaufend diese technischen Einstellungen. Wir nutzen **Machine-Learning bzw. erweiterte Dynamische Bedrohungsabwehr**, um erweiterte Bedrohungsrisiken und Angriffe zu erkennen und diese nach Möglichkeit abzuwehren. Alle Angriffe auf Ihre IT müssen nach den neusten gesetzlichen Vorgaben nach Art.32 DSGVO dokumentiert werden, außerdem dokumentieren wir jede technische Veränderung auf Ihren IT Systemen automatisch.

T · M · B

IT´s Time for Awareness

PEN-Test

Das TMB SOC (Security Operation Center) bietet von dem klassischen PEN-Test bis hin zum beauftragten Blackbox-Test, ein rund-um-sorglos-Paket an, was von der TMB SOC neu definiert wurde.

Es ist ein langer Prozess, Sicherheitslücken in einer Anwendung zu identifizieren, indem das System oder Netzwerk mit verschiedenen bösartigen Techniken und Tools bewertet wird.

Die Schwachstellen eines Systems werden in diesem Prozess durch einen autorisierten simulierten Angriff ausgenutzt. Der Zweck dieses Tests besteht darin, wichtige Daten vor Außenstehenden wie Hackern zu schützen, die unbefugt auf das System zugreifen können. Sobald die Schwachstelle identifiziert ist, wird sie dazu benutzt, das System auszunutzen, um Zugang zu sensiblen Informationen zu erhalten.

Ein Penetrationstest wird auch als Hacking-Szenario bezeichnet, und ein Penetrationstester wird auch als ethischer Hacker beschrieben, der in einer guten Absicht handelt, um Unternehmen Ihre Schwachstellen offen zu legen. Gleichzeitig werden auch die benötigten Härtungsmaßnahmen angeboten.

Typische Ansatzpunkte für einen Penetrationstest sind

- Netzkoppelelemente (Router, Switches, Gateways)
- Sicherheitsgateways (Firewall, Paketfilter, Intrusion-Detection-System, Virenscanner, Loadbalancer etc.)
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme, etc.)
- Telekommunikationsanlagen
- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop)
- Clients
- Drahtlose Netze (WLAN, Bluetooth)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)

Wir unterteilen in Blackbox-Tests und Whitebox-Tests

Bei einem **Blackbox-Test** stehen uns (der TMB (Prüfer)) lediglich die Adressinformationen des Zieles zur Verfügung (Webanwendung, Client, Server, Router, Mailserver, etc.).

Mittels der Vorgehensweise "Blackbox-Test" soll der Angriff eines typischen Außentäters simuliert werden, der nur unvollständige Kenntnisse über das Zielsystem hat.

Bei einem **Whitebox-Test** erhalten wir umfangreiche Informationen über die zu testenden Systeme.
Dazu gehören beispielsweise:

- Informationen über Domain, IP-Adressen des internen Netzes,
- eingesetzte Soft- und Hardware etc.
- Diese Angaben werden uns, der TMB (Prüfer)), zuvor vom Auftraggeber mitgeteilt.

T·M·B

IT´s Time for Awareness

Forensik

Ein weiterer Service, den unser SOC-Team anbietet, ist die Forensische-Untersuchung. Dieser Service enthält folgende Punkte:

Daten Wiederherstellung:

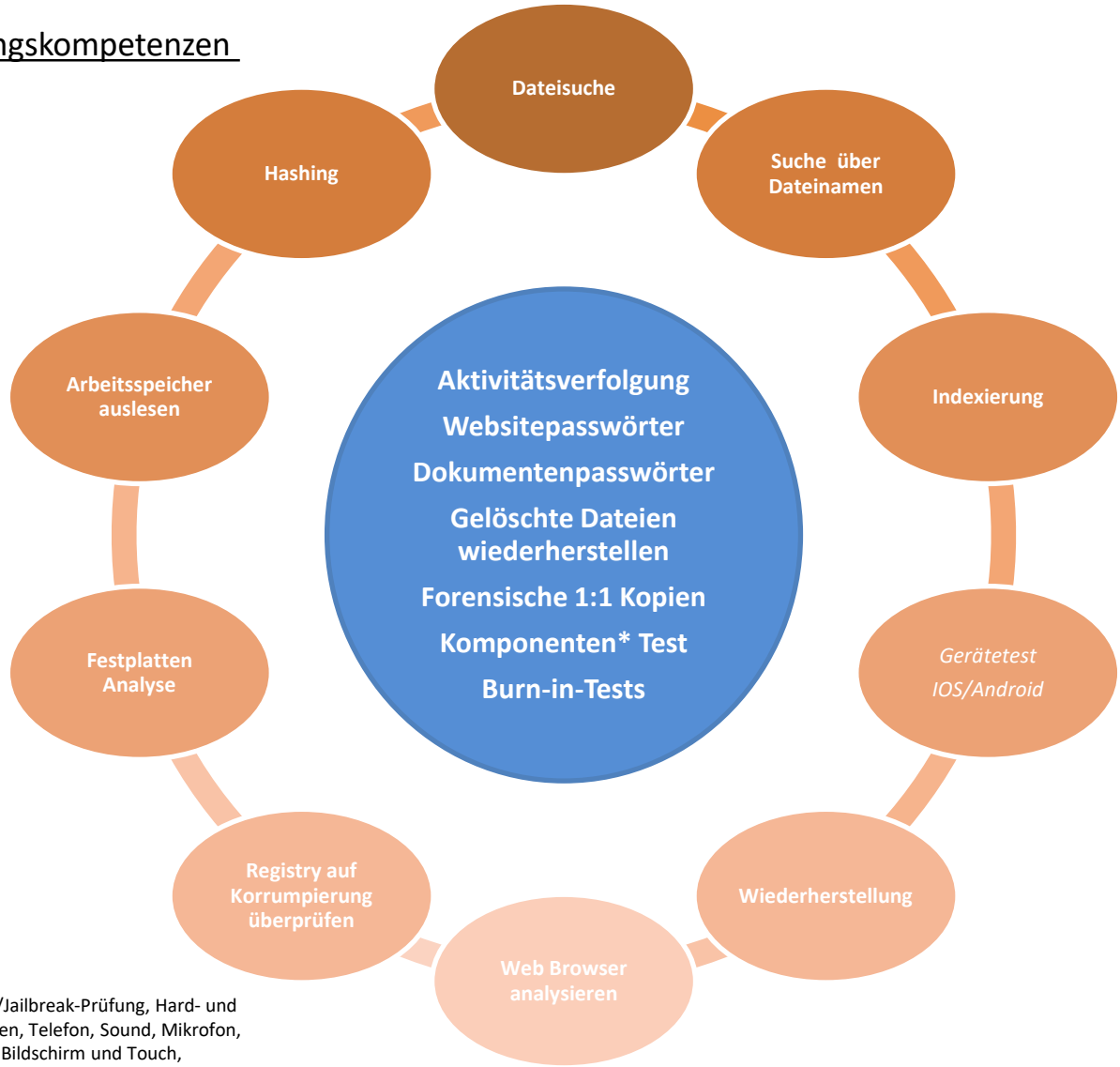
Schnelleres Auffinden relevanter Daten durch hochleistungsfähige Dateisuche und Identifizierung. Auch Extrahieren von Kennwörtern, Entschlüsselung von Dateien, Wechseldatenträgern und Betriebssystemplatten stellen das SOC-Team vor keiner großen Herausforderung. Gelöschte Dateien kann das SOC-Team schnell und automatisch aus Windows, Mac, und Linux-Dateisystem wieder herstellen.

Durch den forensischen Discover-Data Service decken wir alles auf, was in einem PC, Server etc. versteckt ist; ganz egal ob es im TPM Chip oder im Arbeitsspeicher verborgen ist.

Beweise Identifizieren:

Mit Hilfe unserer Hash-Matching und Drive-Signatur-Analysefunktion decken wir ungewünschte und verdächtige Aktivitäten auf. Wir Identifizieren und analysieren für Sie alle Dateien und erstellen sogar automatisch eine Zeitleiste aller Benutzeraktivitäten.

Handlungskompetenzen



*Akku, GSMA/Jailbreak-Prüfung, Hard- und Software-Tasten, Telefon, Sound, Mikrofon, Lautsprecher, Bildschirm und Touch, Fingerabdruck-Scanner, diverse Sensoren, Kamera/Video, usw.

T · M · B

IT´s Time for Awareness

IT Health Check

Ein IT-Healthcheck (ITHC) dient dazu, um zu bestätigen, dass Ihre Informationssysteme und Ihr Netzwerk einem festgelegten Basisstandard entsprechen. Diese Regeln, die auch als Codes of Connection (CoCo) bekannt sind, werden von Konzernen wie KRITS-Betreiber und der Glücksspielkommission verwendet.

Unser Service geht über eine Schwachstellenbewertung hinaus und bietet ihnen eine eingehende Schwachstellen-bewertung an, die regelmäßig - Monatlich, Quartalsweise, Jährlich - Ihre Konformität überprüft, Ihr Unternehmen vor Risiken schützt und Sie in die Lage versetzt, mehr zu erreichen.

Testen Sie die Wirksamkeit der Informationssicherheit Ihrer Organisation mit unseren IT-Healthcheck.

Wir überprüfen alle Ihre User Accounts, Lizenzen und Abonnement. Wir prüfen und Bewerten Ihre Sicherungshistorie. „Wann haben Sie das letzte Mal ein Backup durchgeführt? Funktioniert Ihr System nach dem Widerherstellen des Backups wieder reibungslos? Wie viel Zeit und Aufwand benötigen Sie dafür?“
Ihre Infrastruktur und Inventar wird mit Ihrer Assetdatenbank abgeglichen und überprüft, ob der Bestand vorhanden ist, wie Betriebs-wirtschaftlich festgehalten wurde.

In der Infrastruktur wird die gesamte IT-Verkabelung auf Herz und Nieren getestet. Eine unsaubere Verkabelung kann zu IT-Problemen führen und versehentliches Ausstecken zu unnötigen Ausfallzeiten und Datenverlust beim IT-System führen.

Haben Sie noch Legacy-Anwendungen auf Ihren Workstations installiert sind, die aber nicht mehr verwendet werden?

Alte Legacy-Anwendungen können unnötige Mehr-Kosten verursachen, System-Konflikte produzieren, die Installation von Updates verhindern und sogar zu einem Sicherheitsrisiko werden.

Während unseres Checks werden auch alte Benutzerdaten archiviert um Ressourcen einzusparen.
Dasselbe gilt für alte Ordner und Benutzerdaten auf dem Server, die mit Benutzern verbunden sind, die nicht mehr zum Unternehmen gehören.

Zudem wird auch die sogenannte Schatten-IT geprüft. Hierdurch werden Benutzer im Betrieb analysiert, ob diese Anwendungen wie Dropbox oder Google Drive nutzen, die nicht Teil der Unternehmens-Richtlinien sind.

Historisch gewachsen kommt es häufig vor, dass Unternehmensdaten durch den täglichen Gebrauch und durch menschliche Interaktionen nicht datenschutzrechtlich behandelt werden . Es werden falsche Datenträger, wie private USB-Sticks und Handyspeicher genutzt um Firmen-Daten zu kopieren und diese an weiteren nicht genehmigten Orten zu speichern oder physikalisch abzulegen.
Nutzen Sie ein Benutzer-, Ordner- und Rollenkonzept, um sicherzustellen, dass Ihre sensiblen Daten privilegiert und entsprechend vor unberechtigten Zugriff verschlüsselt sind. Diese und weitere Prozesse werden mit in den Health-Check eingebunden und die Betriebsdokumentation dahingehend überprüft so wie die Sicherheitsrichtlinie nach GPO.

Was natürlich nicht fehlen darf in einem IT-Health Check ist die Gesundheit aller Clients, Komponenten und Mobiledevice-Geräte. Hierzu zählt auch zu prüfen, ob die Updates aktuell sind, da es wichtig ist, das Ihre Geräte alle auf dem neusten Stand sind. Diese Prüfung hilft auch dahingehend, ob das eigene Patch- und Virenmanagement richtig konfiguriert ist oder ob es nachjustiert werden muss.

Es ist eine gute Praxis, alle paar Monate Zeit einzuplanen um den Health Check fortführend durchzuführen, um Ihre IT-Infrastruktur, Prozesse und die zukünftigen Bedürfnisse nach Stand der Technik zu beurteilen.

T·M·B

IT´s Time for Awareness

audIT

IT-Verantwortliche stehen heute vor großen Herausforderungen, um notwendige Standards bei Soft- und Hardware umzusetzen, effiziente Client-Management-Werkzeuge einzuführen und eine optimale Unterstützung der Geschäftsprozesse durch die IT zu gewährleisten. Ein audIT ist eine wichtige Maßnahmen im Rahmen des Qualitätsmanagements. Während eines Audits erfolgt die Überprüfung von Prozessen, Produkten oder Systemen auf Einhaltung von Vorgaben oder Richtlinien.

Das Audit zielt auf eine transparente Berichterstattung über die Informationssicherheit eines Systems ab.
Die TMB führt das audIT nach neusten BSIG-Gesetzlichen Sicherheitsstandards durch, dadurch können angehende (Potenzielle) Neu-Kunden die Ergebnisse aus diesem Report mit in Ihre Berichte und in Ihr Risikomanagement mit einbeziehen und bei der Auswahl, Steuerung und Überwachung Ihrer Systeme, Services, Infrastruktur Härtung mit berücksichtigen. Um die Transparenz für Ihre eigene IT-Sicherheitsstrategie zu erhöhen und geforderte Anforderungen und Maßnahmen stehen somit fest. Dazu gehören insbesondere Informationen über die allgemeinen Bedingungen, wie z.B. Einzelheiten zur Verfügbarkeit und Vorfallbehandlung, zu Subunternehmern, zum Standort der Rechenzentren und zur Behandlung von Ermittlungsanfragen von Regierungsbehörden, Hardware, Software, Netzwerk, IT-Organisation, Personal, Datenschutzprävention, Nutzer im Monitoring.

Zur Erreichung und Optimierung eines geforderten Verfügbarkeitsniveaus erhält das Audit dann eine besondere Bedeutung, wenn z.B. Infrastrukturveränderungen anstehen oder neue Beschaffungen angedacht sind, oder einfach nur der Bedarf ist einmal seine komplette außerhalb von der bekannten Historischen Betreuung kennen zu lernen um zu schauen, wo steht man nach Stand der Technik aktuell. Es Außerdem bildet dies einerseits eine wesentliche Maßnahme zur Sicherstellung eines dauerhaften und zuverlässigen Betriebs, andererseits bietet es die Grundlage für die Steuerung und Kontrolle spezifizierter Serviceparameter und für ein professionelles IT-Service Management sowie die notwendigen Informationen im Hinblick auf die Optimierung der Verfügbarkeit und zur Unterstützung organisatorischer Prozesse und spezifischer Services im Umfeld der Verfügbarkeit.

Die Ziele des audIT

Ein audIT verfolgt mehrere Ziele. Wichtige Ziele sind unter anderem diese:

- Optimierung der Effizienz und Qualität von Unternehmensprozessen, Systemen, Produkten oder Dienstleistungen
- Sicherstellung der Einhaltung wichtiger Qualitätsanforderungen
- Verbesserung der Kundenzufriedenheit
- Verbesserung der Mitarbeiterzufriedenheit
- Qualitätskontrolle von Lieferanten
- Wettbewerbsvorteile durch die Dokumentation und Zertifizierung der erfolgreichen Durchführung von Audits. Der Kunde kann sich auf eine hohe Effizienz des Unternehmens verlasen

GEMEINSAM FÜR MORGEN- ERFOLG IST PLANBAR!

Stand der Technik

Wenn man sich den Methodischen Ansatz zur Bestimmung des Technologie - stands von technischen und organisatorischen Maßnahmen einmal betrachtet, wird man schnell feststellen, dass dies ein unbestimmter Rechtsbegriff ist. Schaut man sich dann die gesetzlichen Bestimmungen dahingehend an, fragen Sie sich sicherlich: warum ist der "Stand der Technik" so wichtig und was ist "Stand der Technik" eigentlich. Fortführend entstehen dann immer schnell die weiteren Fragen, wie lässt sich der "Stand der Technik" bestimmen bzw. wie lässt sich der "Stand der Technik" von anderen Technologieständen abgrenzen?

Aufgeführt erhalten Sie einen Auszug aus folgenden gesetzlichen Bestimmungen mit der Note Richtung IT-Sicherheit.

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik **(BSI-Gesetz - BSIG)** beschreibt diesen Rechtsbegriff wie folgt: *§8a, Abs. 1 : "Betreiber kritischer Infrastrukturen sind verpflichtet […] organisatorische und technische Vorkehrungen […] zu treffen […]Dabei soll der Stand der Technik eingehalten werden.*"

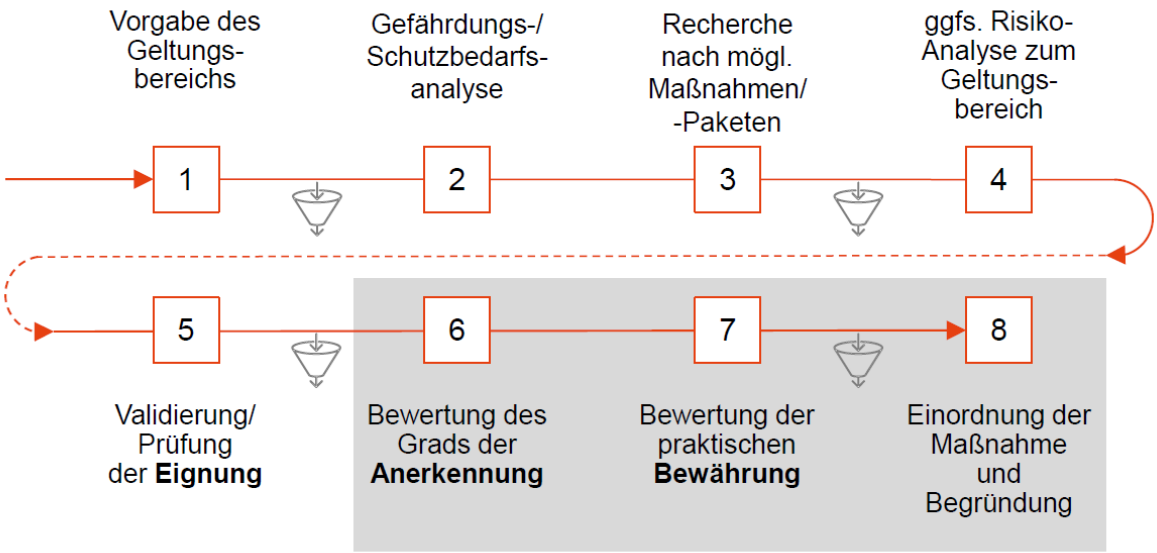
Das Telemediengesetz **(TMG)** definiert es in §13, Abs. 7 wie folgt: *"Diensteanbieter haben […] sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist[…] Vorkehrungen […] müssen den Stand der Technikberücksichtigen".*

Die Netzwerk- und Informationssicherheit Richtlinie **(NIS-RL)** legt die Beschilderung wie folgt aus: Art 15: „[…] Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheits-Niveau der Netz- und Informationssysteme gewährleisten."

Kommen wir zu guter Letzt zum letzten Vorgabenkatalog der am jüngsten und Europaweit greift, in der aktuellen **DSGVO** wird der Stand der Technik wie folgt aufgeführt: Art. 32, Sicherheit der Verarbeitung: *"Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]"*

Zusammengefasst kann man sagen, dass der "Stand der Technik" von den TOMs anhand einer Methode bestimmt sein muss, die die Vergleichbarkeit der Ergebnisse ermöglicht.

Aufgeführt erhalten Sie eine Abbildung allgemeiner Vorgehensweise:



TMB Service GmbH
Am Brambusch 24
44536 Lünen
Tel.:0231/98 60 570

info@tmb-service.de
www.tmb-servie.de

IT-Consulting **IT Security** **Outsourcing** **Infrastruktur** **IMAC** **Rollout** **EU-DSGVO**

Hier finden Sie uns: