complimant

Member of FOX Group

Wirkungsvoller Schutz für kleine und Kleinstunternehmen mit dem CyberRisikoCheck

DIN SPEC 27076

Donnerstag, 10. Oktober 2024 von 17:30 - 20:30 Uhr
Rosenheim

09.10.2024 – Franz Obermayer

Vorstellung Franz Obermayer

Franz Obermayer
Geschäftsführer bei FOXGroup

Beratungsleistungen: Informationssicherheit, Nachhaltigkeit

Expertenwissen:	IT-Sicherheit, Informationssicherheit, Nachhaltigkeit
Zertifizierungen:	Lizenzierter ISO 27001 Auditteamleiter nach BSI (seit 2006) Leadauditor ISO27001, ISO27019 ISO27001, ISO22301, RDC, EN50600, ISO22237 Leadauditor SmartMeterGatewayAdministration (BSI)
Kernkompetenzen:	Normen um die Informationssicherheit, Nachhaltigkeit, Energie

Die aktuelle Bedrohungslage

Es ist nicht die Frage ob man angegriffen wird.

Es ist die Frage, wann man angegriffen wird.

Wer wurde schon angegriffen ?

Noch ne Norm ?


NIS2
DIRECTIVE


EU DATENSCHUTZ-GRUNDVERORDNUNG
EU-DSGVO


CyberRisiko
Check
DIN SPEC
27076:2023


ISO
27001


CISIS12

Alle Punkte die über das betriebliche Erfordernis hinausgehen

01

02

03

04

05

DIN SPEC 27076

Das Thema

Die Norm sieht eine klare Struktur im Ablauf vor. Es beginnt bei der Anbahnung der Beratung und endet mit der Präsentation des Ergebnisberichts bzw. einer möglichen Wiederholung des Gesamtprozesses nach Umsetzung der Handlungsempfehlungen. Dieser Abschnitt erläutert den beratenden IT-Dienstleistern den Gesamtprozess und geht auf die zu beachtenden Details zur korrekten Durchführung ein.

Die Ziele

- **Ermittlung des IST-Zustandes der Informationssicherheit des Unternehmens und Sichtbarmachung der wichtigsten Sicherheitsrisiken**. Damit verbunden ist die Generierung eines Risiko-Status, der mit der Aufnahme des IST-Zustandes ermittelt wird. Werden Anforderungen nicht erfüllt, erscheinen diese im Ergebnisbericht deutlich markiert und weisen das Unternehmen auf Handlungsbedarf hin.

- **Unterbreitung von Handlungsempfehlungen**. Das Unternehmen erhält in Form von Handlungsempfehlungen konkrete Vorschläge, wie es seine IT- und Informationssicherheit erhöhen kann. Mögliche staatliche Fördermaßnahmen (Bund, Land, und Kommune), die für das Unternehmen in Frage kommen, um diese Maßnahmen umzusetzen, sollten durch den IT-Dienstleister in den Ergebnisbericht aufgenommen werden.

- **Sensibilisierung**. Der IT-Dienstleister sensibilisiert das Unternehmen bei der Überreichung von Ergebnisbericht und Handlungsempfehlungen für gängige Gefahren.

Die Vorgehensweise

6.3.2 Anforderungskatalog

Das Erhebungsgespräch basiert auf einem Anforderungskatalog (Tabelle A.1).

Dieser Anforderungskatalog mit den 27 Anforderungen, welche sich in sechs Themenbereiche aufteilen, muss nach der vorgegebenen Reihenfolge gemeinsam mit dem zu beratenden Unternehmen durchgegangen werden.

Der Anforderungskatalog enthält die folgenden Komponenten:

— **Themenbereiche**: Jede Anforderung ist einem von sechs Themenbereichen zugeordnet. Diese sind Organisation & Sensibilisierung, Identitäts- und Berechtigungsmanagement, Datensicherung, Patch- und Änderungsmanagement, Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerke.

— **Anforderung**: Jede Anforderung beschreibt einen Zustand, der im Unternehmen hergestellt sein muss, um die volle Punktzahl für die jeweilige Anforderung zu erreichen. Manche Anforderungen sind in mehrere Komponenten unterteilt (bspw. „01-1“, „01-2“ und „01-3“). Neben den regulären Anforderungen gibt es zudem TOP-Anforderungen, die stärker gewichtet sind.

— **Leitfragen**: Die Leitfragen dienen dazu das zu befragende Unternehmen „ins Erzählen“ zu bringen und den Dienstleister in die Lage zu versetzen, einzuschätzen, ob die Anforderung erfüllt ist.

— **Statuspunkte**: Jede reguläre Anforderung bringt bei Erfüllung 1 Punkt bzw. bei Nicht-Erfüllung 0 Punkte. Besonders wichtige Anforderungen (TOP-Anforderungen) bringen bei Erfüllung 3 Punkte. Bei Nicht-Erfüllung werden 3 Punkte abgezogen. Eine Anforderung kann nur als erfüllt gelten und Punkte erhalten, wenn alle Teilkomponenten (bspw. „01-1“, „01-2“ und „01-3“) erfüllt sind. Detaillierte Ausführungen zum Risiko-Status sind 6.4.1 „Die Errechnung des Risiko-Status“ zu entnehmen.

— **Handlungsempfehlungen**: Die Handlungsempfehlungen sind als kompakte und verständlich formulierte Handlungshilfen für die zu beratenden Klein- und Kleinstunternehmen zu verstehen. Diese werden mit dem Ergebnisbericht ausgehändigt und sollen den Unternehmen konkrete Anhaltspunkte dazu geben, wie eine nicht erfüllte Anforderung zukünftig als „erfüllt“ bewertet werden kann. Die Handlungsempfehlungen müssen bewusst kurz, kompakt und verständlich gehalten, um Klein- bzw. Kleinstunternehmen ohne IT-Fachkenntnis nicht zu überfordern. Erfolgt die Beauftragung eines externen Dienstleisters zur Umsetzung und Verbesserung der Informationssicherheit, wird empfohlen, sich an dieser Handlungsempfehlung zu orientieren.

4.4 Angemessenheit der Informationssicherheit

Unternehmen, die bei der Anwendung dieses Dokuments einen guten Risiko-Status erreichen und denen daher keine Handlungsempfehlungen unterbreitet werden, sollten sich darauf nicht ausruhen, sondern sich bemühen, zusätzliche Informationssicherheitsanforderungen wie beispielsweise die des IT-Grundschutzes zu erfüllen. Gleiches gilt für Unternehmen, die über deutlich größere personelle und finanzielle Ressourcen verfügen, als sie ein Unternehmen mit weniger als 50 Beschäftigten für die Erhöhung der Informationssicherheit in der Regel aufbringen kann.

Dieses Dokument trägt dem Gedanken Rechnung, dass es sich bei Informationssicherheit nicht um einen Zustand, sondern um einen Prozess handelt.

6.3 Durchführung des Gespräches zur Erhebung des IST-Zustandes

Das zu befragende Unternehmen muss sich auf das Gespräch zur Erhebung des IST-Zustandes vorbereiten. Folgende Dokumente sollten, falls vorhanden, beim Gespräch zur eigenen Information zur Verfügung stehen:

— Back-Up-Konzepte;

— Sicherheitsrichtlinien;

— Vertraulichkeitserklärungen;

— Betriebsanweisungen für die IT;

— Notfallpläne;

— Rollenkonzepte;

— Zugriffs- und Zutrittsrechte;

— Übersicht über die hauptsächlich genutzte Hard- und Software.

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
01	TOP	Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss die Gesamtverantwortung für die Informationssicherheit im Unternehmen tragen.	Wer trägt die Gesamtverantwortung für IT- und Informationssicherheit in Ihrem Unternehmen?	3/–3	Die Geschäftsführung muss die Gesamtverantwortung für die Informationssicherheit im Unternehmen übernehmen. Das Thema IT- und Informationssicherheit muss als relevantes und immer aktuelles Alltagsthema von der Geschäftsleitung in alle Abteilungen des Unternehmens hineingetragen werden. Wenn die Geschäftsführung das Thema Informationssicherheit nicht vorlebt, wird sich das Bewusstsein auch nicht auf die Belegschaft übertragen und führt so zu Sicherheitslücken in allen Abteilungen.
02–1		Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss – sofern sie sich nicht alleine um die IT kümmert – eine verantwortliche Person benennen können.	Haben Sie jemanden, der für die IT- und Informationssicherheit zuständig ist? Wenn ja, wer ist das?	1/0	Ernennen Sie eine für die Informationssicherheit zuständige Person oder beauftragen Sie formell einen Dienstleister. Die Geschäftsführung ist häufig überlastet. Es hat sich in der Praxis gezeigt, dass bei einem Fehlen von verantwortlichen Personen das Informationssicherheitsrisiko erhöht ist.

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
02–2		Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss dafür sorgen, dass die für IT- und Informationssicherheit beauftragte Person für die Wahrnehmung ihrer Aufgaben über die notwendigen Kapazitäten verfügt.	Wieviel Kapazitäten stehen Ihnen oder der von Ihnen benannten Person für diese Tätigkeit zur Verfügung?		Die zuständige Person muss über genug freie Kapazitäten verfügen und sich regelmäßig zur IT- und Informationssicherheit weiterbilden können. Eine gewissenhafte Aufgabenwahrnehmung als beauftragte Person ist nur mit entsprechenden Ressourcen sicherzustellen. Die Halbwertszeit von IT-Wissen und Kenntnisse über neue Risikofaktoren (Angriffsszenarien) beschränkt sich auf etwa 1,5 Jahre. Jährliche Schulungen sind daher notwendig.
02–3		Organisa-tion & Sensibilisie-rung	Die Geschäftsführung muss dafür Sorge tragen, dass die beauftragte Person über relevante Kenntnisse im Bereich der Informationssicherheit verfügt.	Über welche Kenntnisse zur IT- und Informationssicherheit verfügen Sie bzw. die zuständige Person?		Die beauftragte Person muss über relevante Kenntnisse im Bereich der Informationssicherheit verfügen. Diese Kenntnisse beziehen sich auf die internen und externen Risiken, die das Unternehmen betreffen. Schwachstellen und Risiken können nur dann realistisch erkannt und bewertet werden, wenn die zuständige Person über das notwendige Know-How verfügt.

Nr.	TOP	Themen-bereich	Anforderung	Leitfrage	Status-punkte	Handlungsempfehlung
03		Organisa-tion & Sensibilisie-rung	Es muss ein Notfallkontakt für unregelmäßige oder ungewöhnliche Vorkommnisse (im IT-System, Telefonanrufe, verdächtige E-Mail-Nachrichten usw.) zur Verfügung stehen. Dies gilt auch für den Verlust von IT-Arbeitsgeräten und Datenträgern.	An wen wenden sich Beschäftigte, wenn ein unregelmäßiges oder ungewöhnliches Vorkommnis erkannt wird oder IT-Arbeitsgeräte verloren gehen? (Beispielsweise eine merkwürdige E-Mail, ungewöhnliches Vorkommnis im System bzw. der Firma)	1/0	Beschäftigte müssen jederzeit eine Ansprechperson (Notfallkontakt) erreichen können, um ungewöhnliche Vorkommnisse oder Verluste unverzüglich zu melden. Bei kritischen Vorkommnissen muss schnell gehandelt werden, um das Ausmaß des Schadens zu begrenzen.
04–1		Organisa-tion & Sensibilisie-rung	Im Falle eines Sicherheitsvorfalles muss jedem Beschäftigten klar sein, wie er sich zu verhalten hat und wem er was und wann melden muss (Notfallplan)	Angenommen, Sie hätten einen IT-Sicherheitsvorfall in Ihrem Unternehmen. Haben Sie klar geregelt, wie sich Beschäftigte verhalten und wem sie was und wann in welcher Form mitteilen müssen, damit der Vorfall zügig und fachgerecht bearbeitet werden kann? Falls ja, bitte erläutern Sie das näher.	1/0	Es muss ein Notfallplan entwickelt und allen Beschäftigten zur Verfügung gestellt werden. Bei kritischen Vorkommnissen muss schnell und zielgerichtet gehandelt werden. Dies kann nur sichergestellt werden, wenn es einen Notfallplan gibt. Hier erfahren Beschäftigte, wie sie sich verhalten und wem sie was, wann und in welcher Form mitteilen müssen.

6.4.2 Erstellung des Ergebnisberichts

6.4.2.1 Struktur des Ergebnisberichts

Nach dem Gespräch zur Erhebung des IST-Zustandes muss der Dienstleister mit den erhobenen Informationen den Ergebnisbericht vorbereiten. Dieser muss aus folgenden Teilen bestehen:

— **Bericht**

Der Bericht sollte eine Länge von maximal 2 DIN-A4-Seiten, welche die wichtigsten Erkenntnisse für das Klein- bzw. Kleinstunternehmen zusammenfassen, haben (siehe 6.4.2.2).

— **Anhang A**

Zusätzlich zu diesen zwei Seiten muss die tabellarische Auflistung der 27 Anforderungen und ihrer Komponenten einschließlich jeweiligem erreichten Status-Wert, stichpunktartiger Begründung und Handlungsempfehlung als Anhang angefügt werden (siehe 6.4.2.3).

— **Anhang B**

Zusätzlich muss eine Auflistung von für das Klein- oder Kleinstunternehmen relevanten Förderprogrammen für die weitere Verbesserung der IT- und Informationssicherheit erstellt und angefügt werden. Dies können Förderungen auf Basis von kommunalen, regionalen, Bundes- oder EU-Mitteln sein. Alle aufgelisteten Förderprogramme müssen für das individuelle Unternehmen relevant und grundsätzlich geeignet sein (siehe 6.4.2.4).

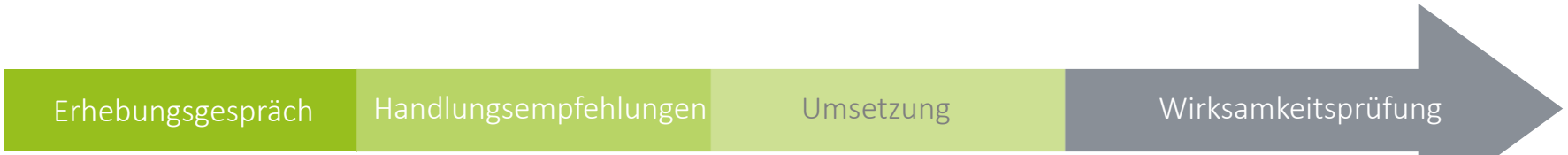
Ablauf

Angemessenheit

Die Handlungsempfehlungen sind immer im Hinblick der Angemessenheit zu sehen. Diese werden mit den Beratern besprochen, um die Klarheit zu schaffen.

Wirksamkeitsprüfung

Wichtig ist die Maßnahmen auf Sinnhaftigkeit zu überprüfen.
Haben die Maßnahmen gegriffen ?
Hat sich die Informationssicherheit verbessert ?
Sind Prozesse gestört ?
Ist das ganze wirtschaftlich ?



Beratung

Im Erstgespräch können Sie mit erfahrenen Beratern / Auditoren Ihren Stand der Informationssicherheit erfahren.

Maßnahmen

Der Maßnahmenplan wird erstellt und dann umgesetzt. Die Jahresplanung sollte erstellt werden –
ES MUSS UND SOLL NICHT ALLES ADHOC ERFOLGEN.

“Es ist besser, Deiche zu bauen,

als darauf zu hoffen,

dass die Flut allmählich Vernunft annimmt.”

Hans Kasper (*1916), dt.
Schriftsteller u. Hörspielautor

Franz Obermayer
Geschäftsführer bei FOXGroup

complimant

Herzlichen Dank für Ihre Aufmerksamkeit.

Member of FOX Group