Leitfaden/Handlungsempfehlungen zum Schutz (unternehmens-) kritischer Informationen.

Für Klein- und Mittelständische Unternehmen (KMU)

IT- und Informationssicherheit

Stand 07.2020

KKI

KOMPETENZZENTRUM
KRITISCHE
INFRASTRUKTUREN E. V.

Leitfaden/Handlungsempfehlungen

Einleitung

Wir erhalten oder hören täglich neue Meldungen zu IT-Sicherheitsvorfällen, die mal mehr mal weniger schlimm sind oder vielleicht nur so klingen. Manch ein KMU erwartet dabei aber nicht, dass es ihn betrifft, sondern immer nur die anderen.

Zudem wird meist nur über IT-Sicherheit berichtet oder gesprochen. Vorfälle oder Versuche, die nicht so spektakulär, also berichtenswert sind, wie das Verschwinden von Akten, Unterlagen oder Datenträgern, unberechtigte Weitergabe von Informationen usw., werden meist nicht oder nur nebenbei erwähnt. Diese einzubeziehen ist allerdings im Gesamtkontext wichtig.

Denn: Tatsächlich ist der **Bereich KMU** (kleinere und mittlere Unternehmen) teilweise nicht bis schlecht auf solche Angriffe oder solche -versuche vorbereitet und deshalb häufig ein „lohnendes“ Ziel.

KMUs verfügen zunächst häufig nicht selbst über die erforderliche Fachexpertise. Wenn der beteiligte/hinzugezogene IT-Dienstleister seinen Fokus auch nicht darauf hat, ist das/ihr Unternehmen für sogenannten Informationssicherheits-Vorfälle leicht verletz- und ggf. erpressbar.

Leitfaden/Handlungsempfehlungen

Einleitung II

Informations-Sicherheit wird im allgemeinen Sprachgebrauch immer synonym mit IT-Sicherheit verwendet. Das ist genau genommen jedoch nicht richtig. Informationssicherheit umfasst weitere Bereiche jenseits von Datenflüssen und Firewalls. IT-Sicherheit ist so gesehen nur eine Teildisziplin der Informationssicherheit.

Mit diesen Handlungsempfehlungen möchte der Verein Kompetenzzentrum Kritische Infrastrukturen e. V. (KKI e. V.) gerade KMU-Unternehmen Hinweise und Bedenkenswertes an die Hand geben, mit der sich Informationssicherheit ohne großen Aufwand steigern lässt.

Deshalb werden neben Themen wie der „Absicherung technischer Systeme“ weitere Aspekte erörtert, die dem Schutz von (unternehmens-) kritischen Informationen dienen sollen. Einen 100%igen Schutz erreicht man dennoch praktisch nie. Das Gesamtpaket der Handlungsempfehlung kann bei konsequenter Beachtung aber erheblich dazu beitragen, das ggf. vorhandene Sicherheits-niveau anzuheben.

Grundsätzliche oder weitergehende Fragen setzen freilich einen entsprechenden (kostenpflichtigen) Beratungstermin voraus. Dieser sollte bspw. den IST-Zustand bestimmen, Schwachstellen erheben, geeignete und individuelle Maßnahmen sowie damit verbundene Kosten und Zeiten benennen usw.

Clusterung der Themen

- Organisatorische Fragen und Maßnahmen
- Gebäudetechnische (physische) Fragen und Maßnahmen
- Mitarbeiter*bezogene Fragen und Hinweise
- Datenträger-/sicherheitstechnische Fragen und Hinweise
- Mobile Endgeräte; Fragen und Maßnahmen
- Fragen rund um den IT-Dienstleister
- IT-technisch/systemische Fragen und Hinweise

Organisatorische Fragen und Maßnahmen I

- Ist das Management ihres Unternehmens in die Informationssicherheitsbelange involviert, kennt die Abläufe, Verfahren und Risiken?
- Ist dem Management die Wichtigkeit der Informationssicherheit bewusst und ist es bereit für zu ergreifende Maßnahmen ausreichende finanzielle Mittel bereitzustellen?
- Fragen Sie sich (und das Management), welche Informationen zu schützen sind. Das können neben den elektronischen Daten auch gedruckte Dokumente oder Handskizzen, aber auch Notizen sein.
- Welche der Informationen sind (unternehmens-)kritisch und warum?

Organisatorische Fragen und Maßnahmen I

Hinweise:

→ Unternehmenskritisch können bspw. Preiskalkulationen, eigene Angebote oder Waren Bezugsquellen sein.

→ Ablagestellen von Patenten oder Entwicklungsunterlagen, Bauprojekte, Planungsunterlagen (eigene und Dritter) beachten

→ Auch Personal- und Versicherungsdaten oder Bankinformationen sowie Zugangsdaten aller Art sind zu berücksichtigen, ebenso Kunden- oder Mandantendaten.

→ Auf welchen Systemen sind welche Informationen wie abgelegt?

Gebäudetechnische Fragen und Maßnahmen I

- Ist die physische Absicherung der kritischen/relevanten Systeme gegeben? Bedeutet: Gibt es einen abgeschlossenen Raum, in dem diese/solche Systeme betrieben werden?
- Wer hat (noch immer) Schlüssel oder Schlüsselkarten für den Zutritt und wird dies in festgelegten Zeitabständen überprüft?
- Ist diese Schlüsselübergabe (und die Rückgabe) notiert/dokumentiert?
- Ist eine Absicherung hinsichtlich der Energieversorgung erforderlich und wenn ja, ist diese gegeben?

Hinweis: Je nach Sicherheitsbedarf ist entweder eine redundante Anbindung oder/und sogar zwei separate Kabelwege nötig.

Tipp: Alternativ bzw. zusätzlich sind ggf. kleinere USV-Anlagen sinnvoll, die einen kurzzeitigen (max. 15 Minuten) Stromausfall kompensieren

- Ist eine netzwerkseitige Absicherung erforderlich und wenn ja, ist diese gegeben? Gemeint ist entweder eine providerredundante Anbindung oder/und sogar zwei separate Kabelwege, je nach Sicherheitsbedarf.
- Tipp: Achten Sie darauf, dass die/***alle*** aktiven Netzwerkkomponenten auch an die Strom-Redundanz angebunden sind. Nicht angeschlossene sind sonst bei Stromausfall stromlos…

Gebäudetechnische Fragen und Maßnahmen II

- Sind Standorte, an denen die kritischen Systeme stehen und betrieben werden, ausreichend vor äußeren Einflüssen gesichert? Auch Hochwasser, Sturm, Einbruch, Unfall usw. ist zu bedenken.

Hinweis: Zu den äußeren Einflüssen zählen auch Temperaturen, deshalb:

→ Ist eine Klimatisierung/Heizung für die Systembetriebsräume vorhanden?

→ Gibt es Wartungspläne für diese technischen Komponenten (Klima/Heizung)?

- Sind die relevanten Standorte mit einer Einbruchmeldeanlage versehen? Wohin meldet diese in welchen Zeiten? Und was passiert dann?
- Prüfen Sie ob Rauchwarndetektoren eine sinnvolle Ergänzung sind
- Ist eine Videoüberwachung und/oder Aufzeichnung eventgesteuert erforderlich? Wenn ja, wo?
- Schon vorhanden? Wer speichert die Aufzeichnungen wo (Ort und Gerät) und wie lange?

Mitarbeiterbezogene Fragen und Maßnahmen I

Vorbemerkung:

Von Mitarbeitern* (auch bei den Dienstleistern) können Bedrohungen ausgehen. 80% der Angriffe kommen „von innen“. Es kann entweder ein ehemaliger Kollege sein, der noch Zugang zu den Systemen hat, aber auch der aktive, interne Kollege der täglich mit den Systemen und Informationen arbeitet.

Manche der unternehmenskritischen Daten werden durch Mitarbeiter* „mal schnell“ ungesichert per Mail übertragen oder auf einem transportablen Datenträger mitgeführt. Ist dieser Datenträger nicht gesichert oder die Daten darauf nicht separat verschlüsselt, könnten so unternehmens-kritische Informationen bei Verlust des Datenträgers in die Hand unberechtigter Dritter gelangen.

Die Sensibilisierung der/aller Mitarbeiter* (in- und extern) ist deshalb wichtig und bleibt nötig.

- Führen Sie hierzu regelmäßig Schulungen mit Ihren Mitarbeiter*n durch?
- Kennen die/Ihre Mitarbeiter* den Umgang mit (allen Arten von) Datenträgern?
- Wissen die Mitarbeiter* um den (sicheren) Umgang mit mobilen Endgeräten?
- Existieren Meldeprozesse zur Meldung von (IT)-Sicherheitsvorfällen? Wie werden diese behandelt?

Mitarbeiterbezogene Fragen und Maßnahmen II

- Sind Unterlagen und Dokumente bspw. gemäß der Kritikalität klassifiziert oder bezeichnet?
- Wissen die Mitarbeiter*, welche Stufe welche Auswirkung im täglichen Umgang damit hat?
- Haben Sie den Umgang mit kritischen Informationen mit Dienstleistern und Auftragnehmern geregelt und verabredet?
- Sind die genannten Ansprechpartner/aktuell Berechtigten noch aktuell/wer kann entfallen und werden diese in festgelegten Zeitabständen überprüft und dokumentiert?
- Wird das Passwort regelmäßig (durch den Anwender) gewechselt und wenn ja, gibt es einen automatischen Wechsel-Zyklus?
- Wie hoch ist die Passwort-Komplexität (Anzahl und Art der Zeichen)?
- Haben und verwenden sie unternehmensweit (einen) Passwort-Manager?

Datenträger-/sicherheitstechnische Fragen und Maßnahmen I

Vorwort

Der Begriff „Datenträger“ ist nicht nur elektronisch zu verstehen. Im Sinne der Informationssicherheit ist Papier auch ein Daten-/Informationsträger. Täglich werden in Besprechungen, Strategie-Meetings, Workshops usw. Skizzen angefertigt, Ideen entwickelt, Konzepte erarbeitet, die auf Papier festgehalten werden. Diese können also durchaus (unternehmens-)kritisch sein oder werden.

Fragen Sie sich:

- Wie gehen wir mit diesen „Datenträgern“ um? Einfach mal schnell nach Abschluss des Termins in einen der Mülleimer? Hoffentlich nicht.
- Bleibt das Flip-Chart mit bspw. den letzten Strategie-Ergebnissen am Board oder der Wand hängen, damit die nächsten Raumnutzer die Informationen sehen oder gar abfotografieren können?
- Bedenken Sie, dass auch Putzkräfte oder Wartungspersonal diese Informationen sehen könnten. Aber auch am Besprechungsraum vorbeiflanierende Passanten könnten Informationen und Details aufschnappen.

Datenträger-/sicherheitstechnische Fragen und Maßnahmen II

- Die Entsorgung von -im weiteren Sinne- Datenträgern ist demnach ein elementarer Bestandteil der Informationssicherheit. Wichtige und aktuelle Papiere/Unterlagen sollten deshalb immer gut verschlossen = unzugänglich und uneinsehbar für unbefugte Dritte aufbewahrt werden.

- Nicht mehr benötigte Unterlagen sollten auf abgesichertem Weg entsorgt werden. Ein Akten-schredder ist eine mögliche, aber unsichere Idee.

- Für veraltete Unterlagen, Kalkulationen, Flip-Charst und dglm. werden von Dienstleistern sichere Datentonnen angeboten. Deren Verwendung stellt bei entsprechender Regelung organisatorisch sicher, dass (unternehmens-) kritische Unterlagen nicht doch im Papierkorb landen.

- Besser ist die gesicherte Entsorgung via qualifiziertem Dienstleister. Das gilt auch für defekte, elektronische Datenträger jeder Art (CDs, Bänder, Festplatten/SSDs (intern und externe), USB-Sticks usw. Diese sollten und dürfen nicht einfach im Haus-/Industriemüll entsorgt werden.

Mobile Endgeräte Fragen und Maßnahmen I

Vorwort:

Fast jeder Mitarbeiter* verfügt heute über ein mobiles Endgerät, quasi ein mobiles Büro. Unterschieden werden muss hier nach Art des Endgeräts: Notebooks und Handys. Damit lassen sich -und werden oft- u. a. Termine, Mails und Dateien synchronisiert.

Fragen Sie sich deshalb:

- Was, wenn das oder ein solches Gerät verloren geht/verschwindet?
- Welche Daten sind nun in den Händen von Dritten und wie kritisch ist das für Ihr Unternehmen?
- Sind Nutzerkonten mit begrenzten Berechtigungen auf dem Endgerät eingerichtet?
- Wer und wie vielen kennen die Administrator-Zugangsdaten und muss das in dem Umfang sein?
- Wurden diese administrativen Zugänge individuell mind. mit einem neuen Passwort versehen (anstelle des Standard-Passworts)?

Mobile Endgeräte Fragen und Maßnahmen II

- Sind die Daten auf der internen Festplatte des Notebooks verschlüsselt?
- Wurde des Endgerät „gehärtet“ und wenn ja, von wem wie und in welchem Umfang?
- Ist auf dem Handy eine Passwortsperre oder eine sonstige ggf. individuelle Zugriffssteuerung eingerichtet?
- Welche Datenkommunikations-Funktion ist bspw. auf dem Handy ständig aktiv?

Frage hier lautet: Was ist wirklich nötig? Muss immer alles eingeschaltet sein? Weniger ist manchmal mehr.

- Ist ein (aktueller) VPN-Client installiert, mit dem bspw. die Nutzung eines öffentlichen WLAN-Spots gesicherte Kommunikation ermöglicht? Gilt auch bei der Verwendung von mobilen Datennetzen.
- Verwenden Sie (unternehmensweit) eine zwei-Faktor-Authentisierung?

IT-Dienstleister Fragen und Maßnahmen I

Vorwort:

Einen geeigneten IT-Dienstleister zu finden ist schwierig genug. Dessen Personal soll eine ausreichende Qualifikation nachweisen und aktuell halten. Das Personal soll über Informationssicherheit geschult sein um den Datenabfluss ihrer unternehmenskritischen Informationen bestmöglich zu verhindern und gegen An- und Zugriffe von außen verteidigen.
Dabei sollen die Kosten im Rahmen bleiben. Auch auf der Dienstleisterseite bestehen entsprechende Zwänge.

- Ist der aktuell beauftragte IT-Dienstleister (noch) zuverlässig?
- Haben Sie mit Ihren Dienstleistern über durchzuführende IT-Sicherheitsmaßnahmen gesprochen?
- Bestehen **aktuelle** Vereinbarungen bzgl. Geheimhaltung und Vertraulichkeit mit dem Dienstleister?
- Ist dessen Umfeld (insbesondere der Bereich Wartungszugang) gut gesichert? Bedeutet: Ist der Zugangsweg gegen (versehentlich) unbefugte Nutzung abgesichert?
- Sind dessen Mitarbeiter* geschult und sensibilisiert im Bezug auf die Informationssicherheit?

IT-Dienstleister Fragen und Maßnahmen II

Werden Systeme und wenn ja, welche durch einen Dienstleister aus der Ferne gewartet?

- Welcher Zugangsweg wird dafür verwendet?
- Ist der Fernzugang abschaltbar (Einschalten nur bei Bedarf durch Ihre Mitarbeiter)
- Verwendet der Wartungsdienstleiter dafür einen verschlüsselten Zugangsweg? Welchen?

Hinweis: Zu beachten ist hier eine ausreichende Verschlüsselungstiefe (aktuell 128 Bit)

- Wird ein eigener Wartungs-User-Zugang mit eigenem Passwort verwendet → Also kein Standard-Passwort oder ein einfach zu erratendes?
- Wird 2-Faktor-Authentisierung angewendet?
- Wer verwaltet die Zugangsdaten? Und wie werden die Informationen gespeichert und gegen unberechtigten Zugriff geschützt? Stichwort ist hier: Passwort-Manager-Tool
- Wie oft werden Passwörter beim IT-Dienstleister aktualisiert?

Systemtechnische Fragen und Maßnahmen I

Einleitung:

Täglich werden neue Schwachstellen entdeckt, die es schnellstmöglich zu schließen gilt. Wartungsverträge sind deshalb elementarer Bestandteil des IT-sicherheitstechnischen Gesamtpakets.

- Wann und wie oft erfahren SIE wie davon, dass ein System oder eine Komponente aktualisiert werden muss?
- Bestehen Meldeprozesse für Meldungen von Sicherheitsvorfällen? Sind Ansprechpartner benannt?
- Welche Systeme haben einen direkten oder indirekten Zugang zum Internet?
- Wer benötigt überhaupt und wirklich einen Fernzugriff (bspw. von unterwegs) auf welche Systeme?
- Gibt es Wartungspläne für die identifizierten, kritischen Systeme und Komponenten?
- Regelmäßige Wartung bezieht sich auch auf Patches, Hotfixes, Updates insbesondere der Betriebssysteme, Firmware, aber auch auf Schadsoftware-Schutz (Viren- oder auch Malware) oder von Browsern usw.

Systemtechnische Fragen und Maßnahmen II

- Ist ein Schadsoftware-Schutz vorhanden, installiert und aktuell?
- Haben Sie kritische Geschäftsbereiche in Netzwerksegmenten separiert?
- Sind diese auf den relevanten Servern und allen Arbeitsplatzsystemen (fest oder/und mobil) aktuell?
- Werden regelmäßig Datensicherungen durchgeführt?
- Wann werden welche Daten wie oft gesichert und wo werden diese wie gelagert?
- Wurde im Wartungsvertrag auch die Systemwiederherstellung nach Datenverlust geregelt und mit Wiederherstellungszeiten hinterlegt?
- Sind die genutzten/eingesetzten Server-Systeme professionell ausgestattet (bspw. doppelte Netzteile und Netzwerkkarten, namhafter Hersteller, Einsatz von RAID-Systemen usw.)
- Sind die genutzten/eingesetzten aktiven Netzwerkkomponenten professioneller Herkunft?

Gemeint ist: Endanwender-Geräte haben meist eine geringe Lebensdauer/Zuverlässigkeit.
Gerade diese nicht für einen Dauerbetrieb ausgelegt und deshalb störanfälliger.

Leitfaden/Handlungsempfehlungen

Zum Schluss:

Wie man aus dem vorliegenden Fragen-Katalog erkennen kann, ist Informations- und IT-Sicherheit mehr als die Begriffe auf den ersten Blick verraten und deshalb auch häufig missverstanden/fehl-interpretiert werden.

Die vorliegenden Fragen und Handlungsempfehlungen können nur unterstützend wirken, erheben jedoch nicht den Anspruch, alles zum Thema 100%ig abzudecken. Das Vorliegende ersetzt den (kostenpflichtigen) Beratungstermin mit geeigneten Experten nicht.

Weiterhin sind gesetzliche Vorgaben stets einzuhalten. Dies sind z.B. TKG, Telemediengesetz, IT-Sicherheitsgesetz, usw.

In diesem Leitfaden/Handlungsempfehlungen fehlen auch die verschiedenen Aspekte des Daten-schutzes und dem Umgang mit personenbezogenen Daten (pbD). Da die meisten Unternehmen seit Mai 2018 die Regeln der DSGVO einhalten und geregelt haben (müssen), wurde hier darauf verzichtet, den Fragenkatalog dahingehend zu ergänzen.

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Juli 2020

KKI

KOMPETENZZENTRUM
KRITISCHE
INFRASTRUKTUREN E. V.

KONTAKT

KKI Kompetenzzentrum Kritische Infrastrukturen e. V.

M. Zimmer
ISB, DSK

An der Spandauer Brücke 10

10178 Berlin

E-Mail: isb@nbb-netzgesellschaft.de

Internet: www.kki-verein.de