Mittelstand 4.0
Kompetenzzentrum
Kiel

CHECKLISTEN

IT-SICHERHEIT
Mit Checklisten zum Erfolg

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Checklisten

Leitfaden für Unternehmenssicherheit

Unsere Checklisten helfen kleinen und mittleren Unternehmen bei der Einrichtung wichtiger IT-Sicherheitsmaßnahmen. Sie vermitteln einen schnellen Überblick der wichtigsten Punkte, die bei einer Bestandsaufnahme oder Neueinrichtung der beschriebenen Komponenten beachtet werden sollten. Dabei liegt der Fokus darauf, dass sich die angegebenen Maßnahmen ohne erweiterte IT Kenntnisse konkret durchführen lassen.

Der anerkannte Stand der Technik ist der Basisschutz IT-Sicherheit vom BSI. Die Checklisten versuchen nicht, die vorgeschlagenen Sicherheitsrichtlinien und Prozesse des BSI zu ersetzen, sondern bieten vielmehr einen niederschwelligen Einstieg. Hiervon können insbesondere Unternehmen ohne eigenes IT-Fachpersonal profitieren.

Durch einen Vergleich des Ist-Zustandes mit den Listen kann eine schnelle Einschätzung des Unternehmensstands hinsichtlich IT-Sicherheit vorgenommen werden.

Inhalt

Ihre Ansprechpartner für Nachfragen, Projekte und Feedback:

Prof. Dr. Sören Werth

soeren.werth@th-luebeck.de

Lars Vosteen

lars.vosteen@th-luebeck.de

Felix Lohse

felix.lohse@th-luebeck.de

Checkliste Management

◯ **Teilen Sie Verantwortlichkeiten zu**

Verteilen Sie Verantwortlichkeiten im Sinne von Rollen in Ihrem Unternehmen. Dadurch kann in Notfallsituationen flexibler und schneller reagiert werden. Wir empfehlen folgende Rollen mit entsprechenden Aufgabenbereichen:

- Admin – hat Zugriff auf kritische technische Infrastruktur und ist auch ohne tiefgreifende IT-Kenntnis dafür verantwortlich
- Informationsschutz (IS)-Beauftragter - hat die Kompetenz im Notfall Entscheidungen zu treffen und weiteres Vorgehen zu bestimmen.

Je nach Größe Ihres Unternehmens bietet es sich an, die Rollen mehrfach zu vergeben, um einerseits eine Teilung der Arbeitslast zu erreichen und andererseits Risiken beim Ausfall von Personal zu entschärfen.
Dokumentieren Sie die Zuweisung anhand zu beantwortender Fragen:

- Wer hat Zugriff auf welche Komponente?
- Was soll im Rahmen der Rolle getan und erreicht werden?
- Wie/wer wird die Wahrnehmung der Rolle geprüft?

◯ **Passen Sie die Arbeitszeitplanung an**

Die vergebenen Rollen und Verantwortlichkeiten erfordern regelmäßig Arbeitszeit. Die Mitarbeitenden, die diese Rollen ausfüllen, müssen dazu in der Arbeitszeitplanung gesondert berücksichtigt werden. So müssen sie ggf. von anderen Tätigkeiten freigestellt werden, um ihren Aufgaben nachzukommen. Die Rollen sollten somit integriert werden und nicht als zusätzliche Belastung verstanden werden.

◯ **Informationsschutzrichtlinie erstellen**

Füllen Sie die nachfolgende Vorlage für Ihr Unternehmen aus und veröffentlichen Sie sie geeignet. Im Folgenden werden die einzelnen Angaben erläutert.

1. Unternehmensziele

Um ein zielgerichtetes Handeln zu ermöglichen, müssen Ziele bestimmt werden.

- Bewusstsein für Informationssicherheit

Alle Beschäftigten müssen über die möglichen Gefahren im Umgang mit modernen Technologien vertraut sein und dementsprechend handeln können. Regelmäßige Fortbildungen sind wichtig, um das Bewusstsein zu stärken.

- Einhaltung von Gesetzen oder Vorschriften:

Es sollen die relevanten Gesetze und Vorschriften eingehalten werden. Die folgende Liste bietet Anhaltspunkte, die für Ihr Unternehmen ergänzt und angepasst werden sollten:

  - §§ 238-239, 257-261 Handelsgesetzbuch (HGB)
  - § 91 Abs. 2 Aktiengesetz (AktG) ODER GmbHG §41 Abs 1 GmbH-Gesetz (GmbHG)
  - Datenschutz-Grundverordnung (DSGVO)
  - Bundesdatenschutzgesetz (BDSG)
  - Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)
  - Betriebsverfassungsgesetz (BVerfG)
  - ergänzende Kundenanforderungen

- Funktionale Aufgabenerledigung:

Die gesamte Informationstechnik eines Unternehmens muss so betrieben werden, dass Terminüberschreitung bei Geschäftsabschlüssen vermieden werden. Grundsätzlich sollte die Informationstechnik Ausfälle tolerieren können.

- Vermeidung materieller Schäden:

Schutzbedürftige vertrauliche Daten stellen einen zunehmenden Wert da. Der Verlust dieser Daten bzw. der Verlust der Vertraulichkeit führt zu unmittelbaren bzw. mittelbaren finanziellen und somit materiellen Schäden.

- Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen:

Persönlichkeitsrechte und Betriebsgeheimnisse sollen unbedingt gewahrt werden. Das Vorliegen von Betriebsgeheimnissen in digitaler Form erzeugt Angriffsflächen auf diese. Diese Angriffsflächen sind zu minimieren.

- Vermeidung von Ansehensverlust bzw. Imageschaden:

Digitale Kommunikation erlaubt es, dass Informationen sich mit hoher Geschwindigkeit verbreiten. Auch negative Informationen über Unternehmen verbreiten sich wie Lauffeuer. Durch ein negatives Image können Umsatzeinbußen und Marketingkosten entstehen. Das nicht Einhalten von Informationssicherheit kann zu einem schlechten Image führen.

- Kontinuierliche Verbesserung:

Informationssicherheit ist ein Prozess. Somit ist eine ständige Weiterentwicklung und Reflektion über aktuelle Vorgehensweisen notwendig.

2. kritische Prozesse und kritische Infrastruktur

Bestimmen Sie kritische Infrastruktursysteme. Hier soll jedes System (Auftragsgewinnung, Angebotserstellung, E-Mailserver, Datenfreigabe, ...) aufgezählt werden, dessen Ausfall dem Unternehmen großen Schaden bewirkt. Insbesondere muss geklärt werden, wer die Systeme bedienen kann, welche Vertretungsabsprachen existieren und eine Dokumentation für grundlegende Funktionen vorliegen.

3. kritische Informationen

Bestimmen Sie kritische Informationen. Es gibt Daten, ohne die das Geschäftsleben deutlich erschwert wird (Passworte, Kundenkontaktinformationen, Patientendaten, ...). Diese zu identifizieren ermöglich einen angemessenen Umgang bspw. in Bezug auf die Datensicherung (siehe Seite 12). Alle Passworte des Unternehmens müssen zentral (mit Zugang für Administratoren) gesammelt werden.

4. Checklisten

Nutzen Sie unsere Checklisten. Alle nachfolgenden auf Ihr Unternehmen passende Checklisten müssen durchgearbeitet werden.

◯ **Notfallvorsorge**

Hängen Sie den Notfallplan aus. Um allen Mitarbeitenden eine schnellstmögliche Reaktion auf eventuell auftretende Notfälle zu ermöglichen, sollten die IT-Notfallkarten an günstigen Stellen positioniert sein. Als Ansprechpartner sollte in der Notfallkarte entweder der den zugewiesenen Rollen entsprechende Verantwortliche oder eine allgemeine externe Notfallnummer, z.B. die der DiWiSH.

Vorlage: Informationsschutzrichtlinie

◯ **Unternehmensziele**

Diese Richtlinie unterstützt die folgenden Ziele des Unternehmens:

- Bewusstsein für Informationssicherheit
- Funktionale Aufgabenerledigung
- Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen
- Einhaltung von Gesetzen oder Vorschriften
- Vermeidung materieller Schäden
- Vermeidung von Ansehensverlust bzw. Imageschaden

Weitere individuelle Ziele sind:

- _____
- _____

◯ **Schützenswerte Prozesse:**

Bspw. Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung oder Abrechnung

Prozess	zuständige Person	Vertretung	Dokumentation liegt vor
			[ ]
			[ ]

◯ **Schützenswerte Infrastruktur:**

Bspw. Netzwerkspeicher, Telefone, Arbeitsstationen oder Server

Infrastruktur	zuständige Person	Vertretung	Dokumentation liegt vor
			[ ]
			[ ]

◯ **Schützenswerte Daten/Informationen**

Bspw. Passworte oder Kundendaten

Daten	Person mit Vollzugriff	Vertretung	Backup erfolgt	Backup ist getestet
			[ ]	[ ]
			[ ]	[ ]

◯ **Checkliste abgearbeitet**

[ ] WLAN
[ ] Arbeitsplatz – allg.
[ ] Arbeitsplatz – Browser
[ ] Passwörter
[ ] Kommunikation – E-Mail
[ ] Kommunikation – VPN
[ ] Datensicherung
[ ] Home-Office

Checkliste WLAN

◯ **Mit Konfiguration vertraut machen**
Setzen Sie sich mit den Konfigurationsmöglichkeiten Ihres WLAN-Routers auseinander. Alle heutzutage vertriebenen WLAN-Router lassen sich über ein Webinterface konfigurieren. Finden Sie heraus, wie Sie sich in diesem Interface anmelden können und erforschen Sie die Konfigurationsmöglichkeiten. Aufgerufen wird dieses Interface, indem man nach dem physischen Anschluss ein Gerät über ein Kabel oder WLAN verbindet und im Browser eine spezielle Adresse eingibt. Diese Adresse hat bei den weitverbreiteten FRITZ!Boxen z.B. die Form http://fritz.box oder auch http://192.168.178.1. Die Zugangsdaten zu dieser „Website“ finden Sie entweder auf einem Aufkleber auf dem Router oder in der Bedienungsanleitung. Keine Angst vor technischer Tiefe. Insbesondere bekannte Hersteller von WLAN-Routern setzen sehr viel Wert darauf, dass die Konfiguration möglichst einfach und für jeden verständlich gestaltet ist.

◯ **Gästenetzwerk einrichten**
Erstellen Sie für Gäste über das Webinterface Ihres Routers ein eigenes Gäste-WLAN. Dies sorgt dafür, dass neugierige Gäste keinen Zugriff auf Ihr Firmennetzwerk haben. Ebenso verhindert diese Maßnahme, dass sich Schadsoftware von Gastgeräten in Ihrem Netzwerk ausbreitet. Nur weil Sie Ihrem Gast vertrauen, sollten Sie seinen Geräten noch lange nicht vertrauen. Ermitteln Sie, ob sich die nutzbaren Dienste einschränken lassen. So existiert häufig die ratsame Möglichkeit, Gästen nur das Browsen im Internet zu erlauben.

◯ **Aktivierte Verschlüsselung**
Aktivieren Sie die Verschlüsselung Ihres kabellosen Netzwerkes. Heutzutage werden die meisten Router bereits mit aktivierter Verschlüsselung ausgeliefert. Dennoch kann es vorkommen, dass besonders günstige Geräte eine unzureichende Verschlüsselung als Standardeinstellung verwenden. Setzen Sie den Verschlüsselungsmodus mindestens auf WPA2, besser WPA3 (nicht jedes Altgerät unterstützt diesen Standard).

◯ **Ändern der Standardpasswörter**
Ändern Sie die Standardpasswörter für Verschlüsselung und Webinterface. Häufig sind die Passwörter vom Hersteller bereits sinnvoll gewählt, was Länge und Komplexität angeht. Allerdings befinden sich die Passwörter häufig auf an den Geräten angebrachten Aufklebern. Sichere WLAN Passwörter haben in der Regel 20 bis 30 Zeichen. Ein Passwort für das Webinterface sollte den Anforderungen aus der Checkliste Passwörter genügen.

◯ **Firmware aktuell halten**
Die Firmware von Routern lässt sich meist über das Webinterface komfortable aktualisieren oder es lassen sich sogar automatische Updates einstellen. Prüfen Sie bei Inbetriebnahme und regelmäßig auf Firmware-Updates, um potentielle Sicherheitslücken zu stopfen.

◯ **Gästenetzwerk regelmäßig bereinigen**
Ändern Sie das Passwort für das Gästenetzwerk regelmäßig, um die Anzahl an Gastnutzern zu beschränken. So halten Sie unerwünschte Dauergäste fern und verhindern, dass diese Gäste Einfluss auf die Qualität der Internetverbindung für Ihre Kunden haben.

◯ **Deaktivieren von WPS**
Deaktivieren Sie in Ihrem Router WPS über das Webinterface. Durch WPS lassen sich Geräte einfacher in einem WLAN anmelden. Dabei muss ein Knopf auf Ihrem Router und auf einem Client gedrückt werden. Dritte könnten so, in einem unbeobachteten Moment, den WPS-Knopf Ihres Routers drücken und Teil Ihres Firmennetzwerkes werden, um Daten auszuspionieren oder Schadsoftware zu installieren. Außerdem existieren weitere professionelle Angriffsmöglichkeiten auf WPS, sodass die Deaktivierung dringend empfohlen wird.

◯ **Meiden von besonders günstigen Geräten**
Vermeiden Sie den Kauf von vermeintlich kostengünstigen Geräten. Diese Geräte werden häufig mit unzureichenden Sicherheitseinstellungen ausgeliefert. So kann es sein, dass keinerlei Verschlüsselung aktiviert ist oder das Webinterface zur Konfiguration des Routers aus dem Internet erreichbar ist. Diese Konfigurationen lassen sich nachträglich treffen, erfordern aber Kenntnisse und insbesondere zeitlichen Aufwand. Außerdem bieten die Hersteller dieser günstigen Geräte selten Sicherheitsupdates oder Kundensupport.

Checkliste Arbeitsplatz

◯ **Aktuell bleiben**

Sorgen Sie dafür, dass sowohl das Betriebssystem als auch verwendete Software regelmäßig Updates erhält. Für Betriebssysteme sind meist automatische Aktualisierungen voreingestellt, prüfen Sie dies und aktivieren Sie diese gegebenenfalls. Updates kommen häufig und können stören, sind aber essenziell für ein sicheres Arbeiten. Auch Software bietet heutzutage häufig automatische Updates an. Wenn Sie eine Update Benachrichtigung erhalten, führen Sie das Update sofort oder zeitnah aus.

◯ **Virenschutz**

Aktivieren Sie einen Virenschutz. Häufig vermittelt ein Virenschutz ein Gefühl von absoluter Sicherheit, dies ist aber nicht der Fall. Immunisierung gegen alle Schadprogramme existiert nicht, dennoch unterstützt ein regelmäßig aktualisierter Virenschutz das Sicherheitskonzept für PC-Arbeitsplätze. Bei Nutzung von Windowssystemen (neuer als Windows 8.1) ist übrigens bereits ein Virenschutz vorinstalliert. Der Windows Defender kann sehr gut mit seinen Mitbewerbern mithalten und bietet sogar Vorteile. Sorgen Sie dafür, dass automatische Aktualisierungen Ihres Virenschutzes eingestellt sind, um neue Bedrohungen frühzeitig erkennen zu können.

◯ **Backup**

Machen Sie sich mit Backups vertraut. Unsere Checkliste Backup ist dafür ein guter Einstiegspunkt.

◯ **Angriffe vor Ort erschweren**

Schützen Sie Ihren Arbeitsrechner vor Zugriff Dritter, indem Sie Ihrem Benutzerkonto ein Passwort zuweisen. Sperren Sie den PC, sobald Sie sich aus der unmittelbaren Nähe entfernen. Bei Windows geht dies über die Tastenkombination Windows+L. Stellen Sie ggf. auch ein, dass sich das System nach einer gewissen inaktiven Zeit selbst sperrt. Unterschätzen Sie diesen Punkt nicht, Gelegenheit und Neugier macht den Angreifer.

◯ **Verschlüsseln**

Verschlüsseln Sie betrieblich genutzte Datenträger. Diese Datenträger beinhalten sensible Daten. Wird Ihr Computer entwendet, hilft das Windows-Passwort nur noch eingeschränkt, da direkt auf die Daten auf dem PC zugegriffen werden kann. Nutzen Sie zur Verschlüsselung von sensiblen Daten deswegen BitLocker oder VeraCrypt. Einmal eingerichtet, erhöht diese Software die Sicherheit beträchtlich.

Microsofts Verschlüsselungsprogramm BitLocker wird bei den Windows 10 Versionen „Pro“, „Education“ und „Enterprise“ bereits mitgeliefert. Wie Sie diese Software schnell und einfach einrichten, erfahren Sie hier: Bitlocker - Microsoft

Falls Sie eine Version von Windows ohne Bitlocker nutzen, bietet sich als Alternative das kostenlose und quelloffene VeraCrypt an. Informationen zum Download, Installation und Ersteinrichtung finden sich auf der Homepage des Projektes. Veracrypt

◯ **Dateierweiterungen einblenden**

Blenden Sie sich die Dateierweiterungen ein. Als Standardkonfiguration von Windows ist vorgesehen, dass bekannte Dateierweiterungen, wie „.jpg“ oder „.pdf“ ausgeblendet werden. Leider wird die Erweiterung „.exe“ ebenso ausgeblendet. Anhand dieser lassen sich allerdings Dateien von Programmen unterscheiden. Setzen Sie im Explorer einen Haken unter „Ansicht -> Dateinamenerweiterungen“, um voreilig Klicks auf Dateien, wie „kätzchen.jpg.exe“, zu vermeiden.

◯ **Deaktivieren von Office Makros**

Deaktivieren Sie Makros in Office Dokumenten. Diese Makros können als Einfallstor in Ihr System genutzt werden. Viele Spam oder Phishing E-Mails enthalten mit Makros bestückte Office Dokumente, deren Ausführung ein Sicherheitsrisiko darstellt. Weitere Informationen finden Sie hier: Makros in Office - Microsoft

Checkliste Browser

◯ **Welcher Browser?**
Entscheiden Sie sich für einen im Betrieb einheitlich genutzten Browser. Grundsätzlich sollten Sie bei der Wahl des Browsers an Arbeitsplätzen auf etablierte Browser, wie Firefox oder Chrome zurückgreifen. Für diese Browser werden regelmäßig Updates erstellt und so Sicherheitslücken geschlossen. Außerdem bieten sie durch ihre Beliebtheit große Unterstützung in Form von Dokumentation und Erweiterungen (auch hinsichtlich Sicherheit). Das Bundesamt für Sicherheit in der Informationstechnik hat 2019 Firefox ESR Firefox Enterprise empfohlen.

◯ **Ad-Blocker**
Installieren Sie einen sogenannten Ad-Blocker als Browsererweiterung. Diese Erweiterung versucht möglichst viel Werbung auf Webseiten zu blockieren. Es existieren allerdings Möglichkeiten durch Werbung Schadsoftware zu verteilen oder nutzende Personen durch spezielle Techniken zum Anklicken zu bewegen. Ein einfacher Klick kann Sie dann auf schadhafte Webseiten leiten.

◯ **Verhaltensregeln**
Legen Sie interne Verhaltensregeln im Umgang mit dem Surfen im Internet fest. Machen Sie sich selbst und Mitarbeiter über mögliche Konsequenzen im Umgang mit dem Internet bewusst. Bleiben Sie in seriösen Bereichen und meiden Sie zu gut klingende Angebote. Auch der „anonyme“ oder Inkognito-Modus ist kein Freifahrtsschein. Sie sind dabei keinesfalls gegenüber Webseiten oder Ihrem Internetanbieter anonym.

Weitere Verhaltensregeln:

1. Achten Sie auf momentan angeforderte Berechtigungen durch den Browser, wie Mikrofon oder Webcam

2. Stellen Sie sicher, dass Sie verschlüsselt surfen. (Geschlossenes Schloss in Adressleiste)

3. Beim Aufruf von Links die Schreibweise prüfen

Checkliste Passwörter

◯ **Passwortmanager**

Nutzen Sie zur Verwaltung Ihrer Passwörter einen Passwortmanager, wie „KeePass“ oder „LastPass“. So können Sie sich Ihre Passwörter auf all Ihre Geräte synchronisieren lassen, müssen sich nur noch ein Master-Passwort merken und müssen bei der Erstellung von Passwörtern oder einem Passwortschema nicht mehr kreativ werden. Passwortmanager erlauben es auch, vollständige Zugangsdaten, Kreditkarteninformationen, PINs usw. sicher zu speichern. Ein Umstieg und eine nachfolgende Eingewöhnungsphase lohnen sich.
Am Beispiel von „LastPass“ lässt sich ein Passwortmanager einrichten, indem Sie unter https://www.lastpass.com ein Angebot wahrnehmen. Anschließend laden Sie eine Browsererweiterung herunter und installieren diese. Zur Erstellung eines „Vault“ genannten Passwortspeichers erstellen Sie ein sicheres Master-Passwort, welches fortan das einzige Passwort darstellt, welches Sie sich merken müssen. Auf Geräten wie Smartphones oder Tablets lässt sich eine App installieren, über die Sie Zugriff auf Ihre Passwörter haben. Einzelne Zugangsdaten zu Diensten können dann über die Browsererweiterung oder die App erzeugt und verwaltet werden.

◯ **Passwortrichtlinien**

Stellen Sie ähnlich zu dem Umgang mit dem Browser Sicherheitsrichtlinien zur Erstellung und Verwaltung von Passwörtern für Sie und Ihre Mitarbeiter auf. Nutzen Sie Erzeugung sicherer Passwörter die Möglichkeiten Ihres Passwortmanagers, falls Sie beispielsweise aus technischen Gründe keinen Passwortmanager nutzen können, schlagen wir folgende Vorgehensweise vor:

Denken Sie sich einen langen Satz mit mehreren Satzbestandteilen aus und verwenden ihn als Passwort.

z.B. „I gehe Montagsmorgens to the Bank and frühstücke Semmeln s'il vous plaît.“

Nutzern Sie keine Passwortspeicher von Browsern. Diese Speicher bieten unter Standardeinstellungen meist nur geringen Schutz und Passwörter lassen sich bei physischem Zugriff auf Ihr System einfach auslesen.

◯ **Backup ihrer Passwörter**

Erstellen Sie ein Backup Ihrer Passwörter, denn der Verlust von Zugangsdaten ist ärgerlich, lässt sich aber durch ein Backup verhindern. Das einfachste Backup ist, sich Passwörter auf einen Zettel zu schreiben und sicher zu verwahren (bspw. eine abgeschlossene Schublade oder ein unübersichtliches Bücherregal). Beachten Sie, dass das Masterpasswort Ihres Passwortmanagers gesondert gesichert werden sollte.

◯ **Zwei-Faktor-Authentifizierung verwenden**

Aktivieren Sie Zwei-Faktor-Authentifizierung bei jedem Dienst, der dies erlaubt. Im Bereich des Online-Banking ist üblicherweise ein solcher zweiter Faktor (TAN-Verfahren) vorgesehen.

Checkliste Kommunikation

◯ **Verschiedene Kanäle nutzen**
Nutzen Sie zur Kommunikation mit Kollegen stets andere Kanäle als privat. Das hilft zu vermeiden, Firmeninterna aus Versehen an Dritte weiterzugeben. Versenden Sie auch keine Mails von privaten E-Mail-Adressen, nur weil es gerade bequem ist. Halten Sie mehrere Kanäle bereit, falls die Situation eine Nachfrage bei Kollegen erfordert. Es ist insbesondere sinnvoll, einmal die Kommunikationswege festzulegen und welche Art der Kommunikation und Daten über welchen Kanal versendet werden sollen.

◯ **Wahl der firmeninternen Kommunikation**
Wählen sie einen datenschutzfreundlichen Messenger für Ihre Unternehmenskommunikation. Mitunter ist es zur Trennung des beruflichen vom privaten Umfeld sinnvoll, unterschiedliche Messenger zu verwenden. Ein häufig unter Betrachtung des Datenschutzes empfohlener Messenger ist „Signal“. Für diesen Messenger existieren sowohl Apps für alle gängigen Smartphones, aber auch ein Desktopprogramm.

E-Mail

◯ **E-Mail-Programm**
Konfigurieren Sie Ihr E-Mail-Programm so, dass keine externen Inhalte geladen werden und die E-Mails als Text statt als HTML geladen werden. Diese Einstellung ist auch für den Versand von E-Mails zu empfehlen.

◯ **Transportverschlüsselung**
Aktivieren Sie Transportverschlüsselung für E-Mails. Bei der Einrichtung Ihrer E-Mail-Konten in entsprechenden Programmen sollten Sie darauf achten, dass Transportverschlüsselung via STARTTLS bzw. TLS/SSL aktiviert ist. Alle heutigen E-Mailanbieter bieten diese Optionen an.

◯ **Sicheren Umgang festlegen**
Legen Sie Verhaltensregeln für den Umgang mit E-Mails fest. Insbesondere im Zusammenhang mit Phishing lassen sich so Gefahren vermeiden. Phishing ist heutzutage weitverbreitet und stellt ein Problem dar, da gefälschte E-Mails von legitimen E-Mails oft schwer unterscheidbar sind. Die Umgangsregeln sollten folgende Punkte enthalten:

1. E-Mail-Adresse der absendenden Person genau prüfen
2. keinesfalls die Anhänge unerwarteter Mails öffnen, prüfen Sie die Echtheit der E-Mail bspw. durch Anrufen des Absenders vor dem Öffnen
3. auf Dateinamenerweiterungen achten, Ausführen von „.exe“ Dateien vermeiden („kätzchen.jpg.exe“)
4. Makros von Office Dateien im Anhang nicht ausführen

VPN

◯ **VPN - Relevanz abschätzen**

Ermitteln Sie, ob ein passender Anwendungsfall für VPN-Verbindungen vorliegt:

1. VPN als Fernzugang

   In der heutigen agilen Gesellschaft ist es oft notwendig, dass einzelne Mitarbeiter*innen der Zugang zum internen Firmennetzwerk ermöglicht wird. So können unterwegs Dokumente betrachtet und bearbeitet werden, die sicher firmenintern gespeichert werden. Eine solche VPN Lösung kann auch dafür genutzt werden, Angriffe in öffentlichen WLANs zu entgehen, indem Datenverkehr über einen verschlüsselten Tunnel durch das öffentliche Netz „hindurch“ stattfindet.

2. VPN zur Verbindung von Standorten

   Die Verbindung mehrerer Standorte über das Internet zu einem großen Firmennetzwerk ist ebenfalls ein typischer Anwendungsfall.

Ein Verbindungspunkt durch ein VPN stellt eine offene Schnittstelle nach außen dar, die mitunter angegriffen werden kann. Deshalb ist es wichtig, genau zu prüfen, ob die Notwendigkeit für einen solchen Zugang gegeben ist.

◯ **VPN - Einrichtung**

Bei der Verwendung eines modernen Routers im Firmennetzwerk, ist es inzwischen auch Laien möglich, VPN-Verbindungen zu konfigurieren. Die Einrichtung über die Weboberfläche des Routers ist oft benutzerfreundlich gestaltet. Hersteller von Routern stellen oft eine eingängige Dokumentation für verschiedenste Anwendungsfälle zur Verfügung. So findet man unter Einrichtung einer VPN Verbindung unter Android z.B. die Einrichtung eines Fernzugangs für Android Geräte.

Checkliste Backup

◯ **Entwickeln einer Strategie**

Entwickeln Sie eine für Sie passende Backup-Strategie:

1. Auswahl der Software und Verschlüsselungsmethode
   Die Wahl der Backupsoftware und der Verschlüsselungsmethode der Backups ist Kern einer guten Strategie. Mögliche Lösungen finden Sie unter dem Punkt „automatische Sicherungen“ bzw. „Backups verschlüsseln“.

2. Auswahl der Häufigkeit
   Nutzen Sie tägliche inkrementelle Sicherungen, dadurch ist bei einem Totalausfall die Menge an verlorenen Daten minimiert.

3. Auswahl des/der Datenträger
   Im Groben ist zwischen drei Kategorien zu unterscheiden – mobil (USB-Stick, externe Festplatte), stationär (Netzwerkspeicher) und fremdverwaltet (Cloud).

4. Auswahl verschiedener Ort
   Planen Sie zur Lagerung/Speicherung Ihrer Backups verschiedene Orte, um im Fall von Bränden, Diebstählen, Meteoriteneinschlägen oder anderen ortsgebundenen Zwischenfällen weiterhin Zugriff auf die eigenen Daten zu haben. Dies kann beinhalten, Backups auf mobilen Datenträgern in Bankschließfächern aufzubewahren, Netzwerkspeicher an anderen Orten synchron zu halten oder Cloudlösungen zu nutzen.

◯ **automatische Sicherungen anlegen**

Verwenden Sie bei Möglichkeit automatisierte Datensicherungen. Im Alltag ist es angenehm, ein Datensicherungssystem zu nutzen, das im Hintergrund agiert und keine wiederholte manuelle Ausführung erfordert. Hierfür ist bspw. das Programm Aomei in der Version „Professional“ (kostenpflichtig – Link) oder das freie Programm Duplicati (beta, funktionsreicher – Link) geeignet. Beide beherrschen die Sicherung auf mobile Datenträger (bspw. USB-Festplatten im täglichen Wechsel) sowie auf Netzwerkspeicher.

◯ **Backups verschlüsseln**

Verschlüsseln Sie Datensicherungen – gerade, wenn diese das Betriebsgelände verlassen, dazu zählen auch Cloudumgebungen.

AOEMI bietet die Verschlüsselung in der Version „Professional“ an, Duplicati in der Grundversion. Das Passwort sollte in eine Datensicherung (nicht die verschlüsselte) aufgenommen oder sicher abgelegt werden, da keine Wiederherstellung ohne es möglich ist. Schreiben Sie es mit dem Masterpasswort ihrer Passwortdatenbank gemeinsam bspw. auf einem Blatt Papier und legen Sie es in ein Bankschließfach, einen zufälligen von vielen Klemmordnern oder unter Ihre Kaffeemaschine – diese beiden Informationen sind sorgfältig zu bewahren.

◯ **Testläufe durchführen**

Testen Sie die geschaffenen Datensicherungssysteme auf Funktionsfähigkeit und Vollständigkeit. Führen Sie dazu neben einer inhaltlichen Prüfung (Sind alle notwendigen Daten dabei?) mindestens stichprobenartig eine Wiederherstellung der gesicherten Daten aus. Ebenso lohnt es in regelmäßigen Abständen (bspw. halbjährlich) zu überprüfen, ob der Speicherplatz noch reicht oder zu den gesicherten Verzeichnissen weitere dazukamen, die in die Sicherung aufgenommen werden sollten.

Spezielle Herausforderungen im Home-Office

◯ **Arbeitsplatz sichern**
Schützen Sie auch zu Hause Ihren Arbeitsplatz vor dem Einfluss Dritter. Sorgen Sie dafür, dass Kinder oder Haustiere sich nicht an Ihren Geräten zu schaffen machen können, auch neugierige Partner und Gäste sind auszusperren. Ein Passwortschutz und das Abmelden bei Verlassen des Arbeitsplatzes ist unbedingt anzuwenden. Aktualisieren Sie auch
hier Ihre Geräte regelmäßig und verwenden Sie einen Virenschutz. Siehe Checkliste – Arbeitsplatz allgemein

◯ **Daten trennen**
Trennen Sie möglichst Privates von Beruflichem. Nutzen Sie idealerweise separate Geräte. Ist dies nicht möglich, können Sie bei allen Geräten separate Benutzerkonten anlegen. Das verhindert zum einen, dass Sie die letzten Urlaubsfotos für alle Kollegen freigeben, aber zum anderen auch, dass Firmendaten in Umlauf gelangen. Zur einfacheren Trennung empfiehlt es sich sogar, andere ggf. zusätzlich beschaffte Geräte zu verwenden.

◯ **Daten sichern**
Arbeiten Sie nach Möglichkeit direkt auf dem Firmenserver, dadurch greifen die üblichen Sicherungsmaßnahmen in der Firma und Sie müssen keine Daten von zu Hause mit ins Unternehmen bringen. Falls diese Möglichkeit nicht besteht, sollten Sie regelmäßig für verschlüsselte Backups auf externen Geräten sorgen. Sollte sich ein Datenträger auf dem Firmendaten vorhanden sind/waren, als defekt herausstellen, werfen Sie diesen auf keinen Fall in den Hausmüll, sondern informieren sich über eine datensichere Entsorgung. Sie verhindern so, dass Sie wegen Verstoßes gegen den Datenschutz haftbar gemacht werden oder Betriebsgeheimnisse an Dritte gelangen. Siehe Checkliste - Backup

◯ **VPN-Verbindungen bereitstellen**
Stellen Sie eine VPN-Verbindung für Mitarbeiter*innen bereit. Als Mitarbeiter*in stellen Sie ausschließlich Verbindungen zum Firmennetzwerk über VPN her. Das hat den großen Vorteil, dass sich Ihr Heimarbeitsplatz logisch in das Firmennetzwerk integrieren lässt und Sie somit auf alle Funktionen und Dienste wie vor Ort zugreifen können. Aber Achtung, hierbei ist es besonders wichtig, dass Sie Ihr Gerät schützen, da vorhandene Schadsoftware ebenso Zugriff aufs Firmennetzwerk erhält.

IHRE EXPERTEN IM BEREICH IT-SICHERHEIT

Technische Hochschule Lübeck

Prof. Dr. Sören Werth
E-Mail: soeren.werth@th-luebeck.de
Prof. Dr. Dorina Gumm
E-Mail: dorina.gumm@th-luebeck.de
Lars Vosteen
E-Mail: lars.vosteen@th-luebeck.de
Felix Lohse
E-Mail: felix.lohse@th-luebeck.de

www.digitales-kompetenzzentrum-kiel.de

Über die Förderinitiative Mittelstand 4.0

Das Mittelstand 4.0-Kompetenzzentrum Kiel gehört zu Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.
Der DLR Projektträger begleitet im Auftrag des BMWi die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.
Weitere Informationen finden Sie unter:
www.mittelstand-digital.de

Impressum
Regine Schlicht, Leiterin Kompetenzzentrum, E-Mail: schlicht@m4kk.de, Tel: +49 431 218-4482
Herausgeber: Mittelstand 4.0-Kompetenzzentrum Kiel, c/o Technische Hochschule Lübeck, Mönkhofer Weg 239, 23562 Lübeck
Redaktion, Gestaltung und Produktion: Lars Vosteen, Felix Lohse, Prof. Dr. Sören Werth, Regine Schlicht
Bildnachweise: freepik.com