SKYTALE®
ONLINE ACADEMY FOR IT SECURITY

7 GOLDENE REGELN IT-SICHERHEIT

7 Sofortmaßnahmen für Ihr Unternehmen

7 Goldene Regeln für Ihre IT-Sicherheit

20 Minuten braucht ein Fußgänger bei moderatem Tempo, um 1,5 Kilometer zurückzulegen, ein durchschnittlicher Leser für ungefähr 15 Seiten eines Buches, steht ein Berliner Autofahrer täglich mindestens im Stau – oder benötigen Sie, um mit unseren sieben Goldenen Regeln in Ihrem Unternehmen für entscheidend mehr IT-Sicherheit zu sorgen.

Ziel dieses Leitfadens ist es, dass Sie sich auf der einen Seite einen ersten Überblick zu diesem wichtigen Thema verschaffen, zum anderen aber auch Anregungen zur schnellen Umsetzung von Sofort-Maßnahmen bekommen. Nehmen Sie sich also 20 Minuten Zeit – die sind „mit Sicherheit" - im doppelten Sinn - gut investiert.

Das erwartet Sie:

1. Verschaffen Sie sich einen Überblick

Der erste Schritt ist immer der schwerste – egal, ob Sie den Keller entrümpeln müssen, endlich mal wieder mit dem Sport anfangen wollen oder Ihre IT-Sicherheit auf Vordermann bringen; ist der erste Schritt erst einmal gemacht, läuft es anschließend (fast) wie von selbst.

Sicher haben Sie sich schon oft gefragt **„Wo fange ich das Thema IT-Sicherheit bloß an?“** Nun, das ist eigentlich ist das ganz einfach, wenn Sie sich folgende Frage beantworten: **„Was ist mir in meiner IT wichtig?“**

Das finden Sie heraus, indem Sie in einem ersten Schritt eine Übersicht Ihrer wichtigsten Systeme und Anwendungen erstellen, basierend auf Ihren **Geschäftsprozessen**. Dazu haben wir Ihnen eine kleine Tabelle vorbereitet. Sie müssen sie jetzt nicht perfekt und vollständig ausfüllen; es geht in erster Linie darum, möglichst die wichtigsten Systeme und Geschäftsprozesse zu erfassen.

Schritt 1:

- Beginnen Sie mit den **Geschäftsprozessen** (Spalte 1-3). Die Wichtigkeit bzw. Priorität können Sie in eigenen Worten oder Stufen (z.B. A bis C oder niedrig bis hoch) angeben. Hier geht es nicht um Formalismus, sondern um eine erste subjektive Einschätzung.

Schritt 2:

- Füllen Sie die restlichen 3 Spalten nach bestem Wissen und Gewissen. Wenn Sie nicht alle Details kennen, gehen Sie die Liste mit einem Ansprechpartner aus der IT oder Prozessabteilung durch.

Name des Geschäfts-prozesses	Kurze Beschreibung Geschäfts-prozess	Wichtigkeit bzw. Priorität des Geschäfts-prozesses	Beteiligte Anwendungen, Abteilungen bzw. Personen	Beteiligte IT-Systeme	Liste der Räume
Produktion	Bestückung von Leiterplatten	Hoch **Ausfall kritisch**	• Shopfloor Personal • Prod Planner Tool	• SMD Leiterplatten Bestücker • Prod Planner Server • Fileserver X	• Serverraum neben Linie X

Schritt 3:

- Markieren Sie die Geschäftsprozesse, auf die **besonderes Augenmerk** in puncto Sicherheit gelegt werden sollte.
- Darf beispielsweise ein System nur maximal 5 Minuten ausfallen, damit nachgelagerte Prozesse nicht ins Stocken geraten, vermerken Sie dies in der Tabelle.
- Sind in einem System besonders **vertrauliche Daten** gespeichert (z.B. Entwicklungsdaten, Finanzkennzahlen usw.), markieren Sie auch diesen Prozess. Gleiches gilt für Daten, die sich auf Personen beziehen (z.B. Daten der Personalabteilung), die damit besonderen gesetzlichen Bestimmungen unterliegen.

Schritt 4:

- Gehen Sie diese Liste mit einem **IT-Ansprechpartner** durch und prüfen Sie, ob die aufgeführten Systeme vollständig sind und ob die aktuellen Sicherheitsmaßnahmen Ihrer Priorisierung entsprechen. Dies ist schon der erste Schritt in Richtung Sicherheitskonzept und sollte schnell wirkungsvolle Maßnahmen für Ihre wichtigsten Systeme und Anwendungen ergeben.

Schon gewusst ?

- So genannte „**Härtungsanleitungen**“ für viele Systeme und Anwendungen finden Sie beim „Center for Internet Security“ (https://www.cisecurity.org/cis-benchmarks/). Ganz konkret erfahren Sie hier, mit welchen Einstellungen Sie Systeme und Anwendungen absichern können.

- Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet mit den **BSI Grundschutzkatalogen** ausführliche Hilfestellungen zur technischen Absicherung.

2: Rechnen Sie mit dem Verlust oder Diebstahl von Smartphones oder Tablets

Die immer größere Verbreitung von Homeoffice, aber auch von Außendiensttätigkeiten bringen es mit sich, dass in immer mehr Unternehmen auch Mobilgeräte wie Smartphones, Tablets oder Notebooks in das Unternehmensnetzwerk und in die zentralen Geschäftsprozesse eingebunden sind.

Leider werden Mobilgeräte auch immer wieder gestohlen oder einfach irgendwo liegen gelassen; allein für das Jahr 2015 meldete der IT-Branchenverband Bitkom vier Millionen „verschwundene“ Geräte, inzwischen dürfte die Zahl da – aufgrund der weiter gewachsenen Verbreitung – noch deutlich höher sein. Sie müssen daher davon ausgehen, dass auch Ihre Firma früher oder später zum Opfer wird. **Bereiten Sie sich also frühzeitig vor** und ergreifen Sie (mindestens) folgende Maßnahmen, damit der Dieb/Finder nicht auch noch in den Besitz Ihrer hochsensiblen Unternehmensdaten gelangt oder gar Zugriff auf Ihr Firmennetz bekommt:

- Geben Sie darauf acht, dass alle Ihre Geräte einen **sicheren Passwortschutz** haben. Einfache PIN-Codes oder simple Muster zum Entsperren des Bildschirms bieten keinen ausreichenden Schutz. Außerdem sollte eine Zeitspanne von max. 5 - 10 Minuten eingestellt sein, nach der sich das Gerät automatisch sperrt. Informieren Sie Ihre Mitarbeiter und Kollegen. Sie können aber auch technische Lösungen wie eine MDM-Software (Mobile Device Management) nutzen, um zentral eine sichere Passwortrichtlinie vorzugeben.

- Sorgen Sie für regelmäßige **Backups der Geräte**, indem Sie alle Mitarbeiter dazu anhalten, Ihre Mobilgeräte selbständig zu sichern. Alternativ können Sie auch Enterprise Backup-Lösungen einsetzen, die für eine zentrale automatisierte Sicherung der Daten sorgen. Achten Sie beim Erstellen von Backups darauf, dass Sicherungen vertraulicher Daten verschlüsselt abgelegt werden.

Wird der **Verlust eines Mobilgerätes** Ihres Unternehmens gemeldet, dürfen Sie keine Zeit verlieren und müssen schnell und umgehend reagieren:

- Versuchen Sie, das Gerät über die Remote-Funktionen des Betriebssystems zu **orten und proaktiv zu löschen**. Unter Android heißt die Funktion „Mein Gerät finden“, bei Apple nutzen Sie „Mein iPhone suchen“. Solang das Gerät noch eingeschaltet und mit dem Internet verbunden ist, können Sie so zumindest noch die darauf gespeicherten Daten löschen, sodass sie keinem Dieb in die Hände fallen.

- Nachdem Sie die Löschung angestoßen haben: **Sperren Sie die SIM-Karte** und melden Sie das Gerät als gestohlen. Die Sperre können Sie bei Ihrem Telefonanbieter oder über die bundesweite zentrale **Hotline 116 116** einrichten.

- Für die Meldung bei der Polizei oder der Versicherung benötigen Sie die 15-stellige **IMEI-Nummer**. Diese erhalten, Sie, wenn Sie die Tastenkombination *#06# wie eine Telefonnummer im Gerät eingeben und wählen. Falls Sie keinen Zugriff mehr auf das Gerät haben sollten, finden Sie die Nummer häufig auch auf der Verpackung oder dem Kaufbeleg.

- Als zusätzliche Sicherheitsmaßnahme können Sie das Handy über die IMEI noch bei den großen Providern **sperren lassen**. Dieser Schritt ist aber unumkehrbar und sollte daher gut abgewogen werden. Ist das Gerät einmal auf der Sperrliste, kann es auch mit einer anderen SIM-Karte nicht mehr eingesetzt werden.

- Auch wenn Sie das Gerät haben sperren lassen, sollten Sie zur Sicherheit alle auf dem Gerät gespeicherten **Passwörter** wie Email-Kennwort, ggf. VPN-Zugang, Social Media Konten usw. **ändern**.

- Wollen Sie vorab sämtliche Daten für den Notfall beisammen haben, nutzen Sie unsere SKYTALE Notfallkarte, die Sie unter https://skytale.academy/downloads/Notfall-Karte_Smartphone_-_Skytale.pdf kostenlos herunter laden können:

Tipp: Die ICCID, IMEI und Seriennummer finden Sie bei iPhones in den Einstellungen unter „*Allgemein*“ – „*Info*“, bei Android ebenfalls in den Einstellungen „*Über das Telefon*“. Die IMEI können Sie auch abfragen, indem Sie die „Rufnummer“ ***#06#** eintippen und „anrufen“. Die Nummer der SIM-Karte ist zumeist auch auf der Karte aufgedruckt, dazu muss sie aber aus dem Gerät heraus genommen werden.
Die Telefonnummer zur Sperrung der Karte im Notfall müssen Sie bei Ihrem Provider erfragen bzw. im Internet nachlesen.

Auch bei Notebooks sollten Sie natürlich einige Verhaltensweisen beachten:

- Eine Fernlöschung ist in der Regel nicht möglich. Umso wichtiger ist es, dass die Festplatte **verschlüsselt** und mit einem **guten Passwort** gesichert ist. Bei Windows-Systemen lässt sich dies beispielsweise bequem und sicher über den Windows **Bitlocker** erreichen. Dieser ist auch Enterprise-tauglich und kann zentral von der IT verwaltet werden.
- Die **regelmäßige Sicherung** ist hier ebenso wichtig wie bei Smartphones und Tablets. Unter Windows können Sie bzw. die IT auch hier mit Bordmitteln zentral eine regelmäßige Sicherung z.B. auf einen gesicherten Fileserver vorgeben. Das System wird dann beispielsweise jeden Dienstagmittag um 12:00 Uhr automatisch gesichert.

3: Geben Sie Ihren Mitarbeitern ein Tool zum sicheren Datenaustausch

Der Austausch von Daten innerhalb der Firma, aber auch mit externen Dienstleistern, Geschäftspartnern oder Kunden gehört mittlerweile zum Unternehmensalltag. Wenn Sie diesen Vorgang aber nicht reglementieren oder keine zentralen Lösungen vorgeben, werden die Mitarbeiter „irgendeinen“ Weg nach bestem Wissen und Gewissen nutzen. Das kann gerade bei vertraulichen Daten oder Daten, die dem Datenschutz unterliegen, eine **Bedrohung** darstellen. Beispielsweise werden Daten dann häufig **unverschlüsselt** per Email übertragen oder zu externen Cloud-Anbietern wie Dropbox, OneDrive o.ä. hochgeladen und somit **Dritten** (teilweise sogar außerhalb der EU) zugänglich gemacht.
Das Unternehmen hat in diesem Moment **keinerlei Kontrolle** mehr darüber, wann, wie und wo welche Daten genutzt und übertragen werden. Auch die Zugriffskontrolle lässt sich dann nicht mehr angemessen steuern.

- Geben Sie also Ihren Mitarbeitern einen Weg an die Hand, wie Sie dieses Problem der Datenweitergabe sauber, sicher und kontrolliert lösen können.
  Setzen Sie beispielsweise einen OwnCloud-Server auf, über den Sie Dateien mit Externen über Links - optional auch mit Ablaufdatum - teilen können.

  Wenn Sie keine eigene Lösung betreiben möchten, sehen Sie sich nach einer Cloud-Lösung (nach Möglichkeit wegen der Datenschutzbestimmungen in Deutschland) wie beispielsweise PowerFolder um – das übrigens auch On-Premise auf der eigenen IT betrieben werden kann, so dass die Daten nicht mehr Ihr Haus verlassen müssen.

4: Bereiten Sie sich auf den Notfall vor

Der Mensch hat die Angewohnheit anzunehmen, dass Katastrophen und Notfälle immer nur die anderen treffen. In unseren Gedanken ist es stets das Haus der anderen, das abbrennt oder vom Blitz getroffen wird, immer irgendein anderer, den Krankheit oder Unfall ereilen. Machen Sie es besser, wenn es um Ihr Unternehmen geht. Seien Sie **auf alle denkbaren Eventualitäten vorbereitet**.

Hand aufs Herz: Weiß Ihre IT auf Anhieb, was zu tun ist, wenn die Technik wegen Blitzschlag, Hacker-Angriff, Anbieter-Ausfall oder Feuer lahm gelegt wird? **Wie handeln Sie?** Wen rufen Sie zuerst an? Wo finden Sie die entsprechenden Telefonnummern? Welche Systeme müssen zuerst wieder zum Laufen gebracht werden, welche können noch etwas warten?

All diese Fragen können im Notfall viel Zeit und Geld kosten - und im schlimmsten Fall auch viele unnötige Fehlhandlungen verursachen.

- Machen Sie sich also **vorher Gedanken** und tragen Sie beizeiten alle diese relevanten Informationen zusammen. Ziehen Sie dabei auch die **Strukturanalyse** (siehe Tipp 1) zur Rate. Sie sollten darauf direkt die wichtigsten und kritischen Systeme und Personen ablesen können.

- Berücksichtigen Sie, dass Sie bei einem Strom- oder Netzwerkausfall nicht auf elektronische Dateien auf dem Fileserver zugreifen können. Entweder halten Sie also eine Kopie auf einem (oder mehreren) Laptops oder Sie drucken das **Notfallhandbuch** ganz einfach klassisch auf Papier aus.
  Denken Sie bzw. die IT-Abteilung auch daran, die Einstellungen und nötigen Schritte zur Wiederherstellung der wichtigen Systeme bereitzuhalten.

- Als vorbeugende Maßnahmen helfen auch hier **Backups** der wichtigsten Systeme und Daten. Machen Sie sich vorab Gedanken über Sicherungsintervalle, Aufbewahrungsorte - und vor allem: **prüfen** Sie die Sicherungen **regelmäßig** auf Ihre Funktion. Nichts ist ärgerlicher als eine Sicherung, die im Notfall nicht funktioniert oder die falschen Daten enthält.

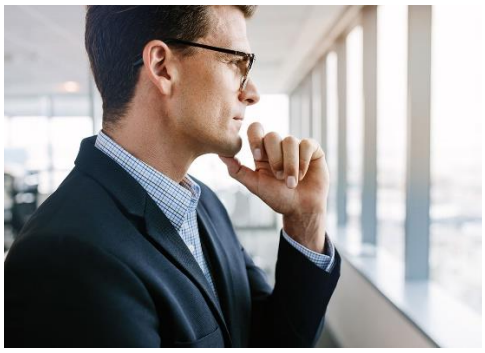
5: Bleiben Sie stets informiert

Wir leben in einer schnelllebigen Welt; besonders im digitalen Umfeld gibt es fast täglich Neuerungen – auch was Viren, Malware und Angriffsmuster betrifft. Was glauben Sie: Wie viele neue schädliche Dateien werden täglich entdeckt? 100? Nun, AV-Test registrierte 2016 vier bis **fünf neue Schadprogramme – pro Sekunde!** Das sind 16.000 pro Stunde oder 390.000 am Tag. Um da den Überblick über die wichtigsten zu behalten, sollten Sie stets auf dem Laufenden sein und die wesentlichen Meldungen im Blick halten. Wenn mal wieder eine neue Phishingwelle rollt oder ein neuer Erpressungstrojaner unterwegs ist, sollten Sie davon wissen, bevor es Ihr Unternehmen trifft.

- Es gibt im Netz **zahlreiche Dienste** wie beispielsweise die Initiative „Deutschland sicher im Netz“ (DSiN), über die sich Nutzer und Unternehmen informieren können. Hier gibt es auch die App „Sicherheitsbarometer“ (SiBa), die Privatanwendern und kleinen Unternehmen aktuelle Warnmeldungen, Hilfestellungen und Infos zum sicheren Shoppen und Surfen bietet. Den Dienst „SiBa“ gibt es auch als RSS-Feed, falls Sie diese Art der Information bevorzugen.

- Werden Sie Mitglied der Allianz für Cyber-Sicherheit, die vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)** betrieben wird. Hier können sich Firmen austauschen und über Angriffe, Sicherheitsmaßnahmen u.v.m. informieren lassen.

6: Prüfen Sie Dateien und Links auf Viren, bevor Sie sie öffnen



Dass man auf keinen Fall Dateianhänge von Mails öffnet, wenn man nicht ganz sicher ist, dass der Absender vertrauenswürdig und der Anhang ok ist, sollte inzwischen bekannt sein; nur allzu groß ist da die Gefahr, das IT-System mit Malware, Viren und Trojanern zu infizieren.

Laut einer Statistik des BSI stieg der Anteil von Schadprogramm-infizierten Mails innerhalb der letzten zwei Jahre auf 1,3 Prozent. Das klingt erst einmal nicht viel; das bedeutet aber, dass von 1.000 E-Mails statistisch gesehen mindestens 13 Malware enthalten.

Wie viele Mails bekommt Ihr Unternehmen täglich? Nachdem wir das geklärt haben, stellt sich aber die Frage: Woran können Sie die gefährlichen Mails erkennen und vermeiden, und wie können Sie dieses auch im täglichen Betrieb noch gewährleisten?

- Wenn Sie die wesentlichen Kennzeichen wie Absender, Korrektheit, Kontext, Sprache und Zeitpunkt einer Email als „sauber“ einstufen, aber trotzdem noch unsicher sind, nutzen Sie doch einen der vielen **kostenlosen Dienste** im Internet, die Sie dabei unterstützen, Schadsoftware zu erkennen:

  Bei virustotal.com können Sie eine Datei hochladen oder Website angeben, die dann von **über 50 Virenscannern** unterschiedlichster Hersteller auf bekannte Viren oder Muster überprüft wird. Ähnlich funktionieren auch die Seiten isitphishing.org oder phishtank.com - probieren Sie es einfach einmal aus!

- Aber bedenken Sie bitte, dass Sie hier **keine wirklich vertraulichen Inhalte** hochladen sollten, da die übermittelten Dateien in der Regel von den Diensten gespeichert werden.

7: Schulen Sie Ihre Mitarbeiter und seien Sie ein Vorbild in Sachen Sicherheit

Die größte Schwachstelle in jedem System ist und bleibt der Mensch. So würde zum Beispiel **jeder sechste Mitarbeiter** ohne Nachfrage auf eine gefälschte E-Mail der Chefetage antworten und sensible Unternehmensinformationen preisgeben, wie eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergeben hat.

Fast die Hälfte der Befragten gab zu, sich selbst nicht aktiv mit dem Thema IT-Sicherheit zu beschäftigen, 18 Prozent vertrauen darauf, dass der Arbeitgeber sich schon um die Sicherheit kümmern wird und immerhin noch 13 Prozent warten darauf, dass sie vom Unternehmen darauf hingewiesen werden, wenn sie Sicherheitsmaßnahmen ergreifen sollen. Und das nutzen Kriminelle aus.

Deshalb:

- **Stärken Sie Ihre Mitarbeiter**, gewinnen Sie sie für das Thema Sicherheit ! Denn was helfen Ihnen die besten technischen Sicherheitsmechanismen, wenn Ihre Mitarbeiter im besten Glauben am Telefon vertrauliche Daten herausgeben oder Türen und Bildschirme nicht gesichert sind?

- Bringen Sie Ihren Mitarbeitern bei, Ihre Systeme sicher zu verwalten, sichere Passwörter zu wählen und sich vor allem sicher im Internet zu bewegen.

- Als **effiziente Schulungsmaßnahme** ohne Reisekosten, ohne hohen Organisationsaufwand und mit hoher Erfolgsquote haben sich **Online-Schulungen** bzw. eLearning bestens bewährt.

- Neben dem Angebot für IT-Experten bietet die **SKYTALE Online-Akademie** Schulungen für Mitarbeiter an, die sich auf **nicht-technischem Niveau** mit den Tücken der IT-Sicherheit befassen, die aufklären, wie mit betrügerischen Emails und Webseiten umzugehen ist, wie sichere Passwörter gewählt und wie man sich im Falle eines Angriffs verhalten sollte.

- Mit **SKYTALE Security Awareness** bieten wir Ihnen die Möglichkeit, den Besuch der Schulungen **zentral zu dokumentieren** und somit für Audits, wie z.B. Datenschutz-Audits, **nachweisbar festzuhalten**.

- Unter https://skytale.academy/kurse/security_awareness.html finden Sie unser **Schulungsprogramm zur Sensibilisierung Ihrer Mitarbeiter**.

- Sprechen Sie uns unverbindlich an, wir unterstützen Sie gern!

SKYTALE Online-Akademie für IT-Sicherheit

Audiocation GmbH
Lippertor 2
59555 Lippstadt

Deutschland

Tel. +49 (0) 2941 66096-90
Fax +49 (0) 2941 66096-99

info@skytale.academy