Transferstelle
IT-Sicherheit im Mittelstand
Einfach. Sicher. Machen.

Ihr Aktionsplan

Der Weg zu mehr IT-Sicherheit

Partner der Initiative:

IT-Sicherheit
IN DER WIRTSCHAFT

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Ihr Aktionsplan

Mit dem TISiM-Aktionsplan unterstützen wir Sie – Schritt für Schritt – auf Ihrem Weg zu mehr Schutz und Sicherheit in Ihrem Unternehmen.

Sie erhalten auf Grundlage Ihrer Unternehmensbefragung passende Aktionen mit konkreten Umsetzungsvorschlägen und erfahren, wie Sie Ihre IT-Sicherheit erhöhen können. Die Aktionen sind in drei Fokusbereiche gruppiert. In den Fokusbereichen sind Ihre Aktionen nach der Relevanz geordnet. Die für Sie wichtigste Aktion steht an erster Stelle, gefolgt von der zweitwichtigsten, usw.

Sie entscheiden, mit welchen Aktionen Sie den Weg zu mehr IT-Sicherheit beginnen möchten.

Viel Spaß!

Ihre Transferstelle IT-Sicherheit im Mittelstand

Haben Sie Fragen oder benötigen Sie Hilfe?

+49 30 76 75 81 575

sec-o-mat@sicher-im-netz.de

Organisatorische Aktionen

Organisatorische Aktionen bilden die Grundlage für Daten- und Informationssicherheit in Ihrem Betrieb. Nur mit ihnen können Sie personelle und technische Aktionen dauerhaft in den betrieblichen Alltag integrieren, und dabei gesetzliche Vorgaben einhalten.

Mobile Endgeräte sicher einsetzen

Klären Sie den sicheren Umgang mit mobilen Endgeräten in Ihrem Unternehmen. Welche Informationen dürfen auf den mobilen IT-Systemen erhoben, verarbeitet, gespeichert und z. B. per E-Mail übertragen werden? Dürfen mobile Endgeräte sich (z. B. über Bluetooth) mit anderen Geräten verbinden, und wenn ja, mit welchen? Formulieren Sie hierzu leicht verständliche Regeln.

Unsere Umsetzungsvorschläge:

- Checkliste für Mitarbeiter IT-Sicherheit im Home-Office [Broschüre/Flyer (Digital)] (Link)
- Checkliste zur Sicherheit im Home-Office (Link)
- Mobile Device Management [Broschüre/Flyer (Digital)] (Link)
- Mobile Endgeräte sicher nutzen [Broschüre/Flyer (Print), Broschüre/Flyer (Digital)] (Link)
- Sicherheitslücke Homeoffice – wie Sie sich vor Datenklau schützen [Präsentation] (Link)
- Vortrag von der CeBIT 2013 zu rechtlichen Aspekten von BYOD (Bring Your Own Device) [Video] (Link)
- „Human Factor“ in der Krise - Wie uns Cyberkriminelle jetzt angreifen [Webinar] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Passwortregeln festlegen

Passwörter sind ein Übel - dennoch kommen wir ohne sie nicht aus. Formulieren Sie einfache, aber gute Regeln zum sicheren Umgang mit Passwörtern in Ihrem Unternehmen wie z.B. die Nutzung unterschiedlicher Passwörter für die einzelnen IT-Systeme, Mindestlängen für Passwörter sowie die Verwendung von Passwort-Management-Systemen.

Unsere Umsetzungsvorschläge:

- 25 Passwort-Manager für PC und Smartphone [Artikel] (Link)

KOSTENPFLICHTIG

- E-Mail-Sicherheits-Check: have I been pwned? [Website] (Link)
- Empfehlungen für Passwörter [Artikel] (Link)
- HPI Identity Leak Checker: Wurden Ihre Identitätsdaten ausspioniert? [Website] (Link)
- KeePass Passwort Safe (Link)
- Kurz erklärt – 3 Tipps für mehr IT-Sicherheit [Video] (Link)
- Password Depot (Link)

KOSTENPFLICHTIG

- Sicherer Umgang mit Passwörtern Schritt-für-Schritt erklärt [Artikel] (Link)
- Zwei-Faktor-Authentisierung [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Verbindung mit externen Netzwerken regeln

Sind Sie oder Ihre Mitarbeitenden oft unterwegs und arbeiten dann mit Firmen-IT? Formulieren Sie klar verständliche Regeln zur sicheren Verbindung mit WLAN und anderen Netzwerken außerhalb Ihres Unternehmens. So sollte z. B. eine verschlüsselte VPN-Verbindung bei der Nutzung von WLANs an öffentlichen Plätzen wie Cafés, Flughäfen und Bahnhöfen eingesetzt werden.

Unsere Umsetzungsvorschläge:

- Checkliste für Mitarbeiter IT-Sicherheit im Home-Office [Broschüre/Flyer (Digital)] (Link)
- Checkliste zur Sicherheit im Home-Office (Link)
- Datenschutz: Plötzlich im Homeoffice – und nun? [Broschüre/Flyer (Digital)] (Link)
- Mobile Device Management [Broschüre/Flyer (Digital)] (Link)
- Mobile Endgeräte sicher nutzen [Broschüre/Flyer (Print), Broschüre/Flyer (Digital)] (Link)
- Sicherheitslücke Homeoffice – wie Sie sich vor Datenklau schützen [Präsentation] (Link)
- Telearbeit und Mobiles Arbeiten: Ein Datenschutz-Wegweiser [Broschüre/Flyer (Digital)] (Link)
- Top Tips for Cybersecurity when Working Remotely [Artikel] (Link)
- Vortrag von der CeBIT 2013 zu rechtlichen Aspekten von BYOD (Bring Your Own Device) [Video] (Link)
- „Human Factor“ in der Krise - Wie uns Cyberkriminelle jetzt angreifen [Webinar] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Über Sicherheitslage informiert bleiben

Gut und aktuell informiert zu sein ist ein wichtiger Vorteil in der Informationssicherheit. Wählen Sie daher eine für Ihr Unternehmen angemessene Informationsquelle für Neuigkeiten zur aktuellen Cybersicherheitslage und Empfehlungen. So sind Sie auf mögliche Angriffe vorbereitet und können ggf. noch reagieren, bevor Ihr Unternehmen betroffen ist.

Unsere Umsetzungsvorschläge:

- CAk report [Newsletter] (Link)
- Der IT-Sicherheitsblog für den Mittelstand [Blog] (Link)
- Heise Security Pro [Website, Forum] (Link)

KOSTENPFLICHTIG

- Heise Security [Website, Forum] (Link)
- Ransomware-Hilfe-Seite "No more Ransom" [Website] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Meldepflichten beachten

Kommt es zu einem IT-Sicherheits- oder Datenschutzvorfall, muss dieser je nach Branche und Art des Vorfalls bei einer Behörde gemeldet werden. Informieren Sie sich daher im Vorfeld über die für Ihr Unternehmen relevanten Kriterien für eine Meldung, Meldestellen und -fristen. Dokumentieren Sie diese an zentral, leicht zugänglicher Stelle und nehmen Sie bei einem Vorfall innerhalb der gesetzlichen Meldefrist Kontakt zu Ihrer Meldestelle auf.

Unsere Umsetzungsvorschläge:

- Bericht der Artikel-29-Datenschutzgruppe über die Pflicht zur Meldung bei den nationalen Kontrollstellen [Broschüre/Flyer (Digital)] (Link)
- Infoblatt „Meldung von Datenschutzverstößen“ [Broschüre/Flyer (Digital)] (Link)
- Kurzübersicht und Checkliste zu IT-Compliance [Broschüre/Flyer (Digital)] (Link)
- Leitfaden – Was ist IT-Compliance? [Broschüre/Flyer (Digital)] (Link)
- Standard-Datenschutzmodell [Broschüre/Flyer (Digital)] (Link)
- Suchportal DSGVO-Gesetz [Website] (Link)
- Themenheft IT-Sicherheit und Recht (Link)
- Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel] (Link)
- Wissenschaft trifft Praxis - Digitales Recht & Sicherheit (Ausgabe 10) (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM” nach Registrierung.

Kriterien für Dienstleister zusammenstellen

Lassen Sie Ihre IT durch Dienstleister betreuen / warten? Welcher IT-Dienstleistungsbetrieb ist vertrauenswürdig, welcher passt zu Ihnen? Formulieren Sie Kriterien (wie z. B. Mindestverfügbarkeit der IT-Systeme, Umgang mit IT-Angriffen), die Ihnen bei der Bewertung und Auswahl helfen. Lassen Sie sich die Umsetzung Ihrer Anforderungen durch den Dienstleistungsbetrieb vertraglich zusichern.

Unsere Umsetzungsvorschläge:

- DsiN-Cloud-Scout [Webbasierte IT-Sicherheitsanalyse] (Link)

- Kriterienkatalog für die Auswahl eines IT-Dienstleisters [Broschüre/Flyer (Digital)] (Link)

- brand eins/thema IT-Dienstleister 2021 [Fachzeitschrift] (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Überblick über die größten Risiken gewinnen

Gewinnen Sie einen Überblick über die größen Risiken in Ihrem Unternehmen -die Risikomatrix kann Ihnen dabei helfen. Nachdem Sie alle Risiken erfasst haben, bewerten Sie diese nach ihrer jeweiligen Eintrittswahrscheinlichkeit sowie potenziellen Schadenshöhe. Beschließen Sie für Ihre kritischen Risiken (hohe Wahrscheinlichkeit und großer Schaden) geeignete risikosenkende Maßnahmen und geben Sie diese in Auftrag. Überprüfen Sie sowohl die Risiken als auch Ihre Gegenmaßnahmen einmal jährlich.

Unsere Umsetzungsvorschläge:

- Checkliste IT-Sicherheitsrisiko Mensch [Broschüre/Flyer (Digital)] (Link)

- Checkliste für Informationssicherheit (Link)

- DsiN-Sicherheitscheck [Webbasierte IT-Sicherheitsanalyse] (Link)

- E-Mail-Sicherheits-Check: have I been pwned? [Website] (Link)

- Fa. Cyberdyne: IT-Sicherheitsberatung (Link)

KOSTENPFLICHTIG

- HPI Identity Leak Checker: Wurden Ihre Identitätsdaten ausspioniert? [Website] (Link)

- IT-Notfallplan - Im Ernstfall richtig reagieren [Broschüre/Flyer (Digital)] (Link)

- IT-Security Check-Up für kleine und mittelständische Unternehmen (Link)

KOSTENPFLICHTIG

- IT-Sicherheitsaudit (Link)

KOSTENPFLICHTIG

- IT-Sicherheitscheck (Link)

- Maßnahmenvorschläge zur Reduktion von IT-Risiken (Link)

- Online-Kurs zum IT-Grundschutz - Strukturanalyse [Selbststudium] (Link)

- Paket KMU-Sicherheit (Link)

KOSTENPFLICHTIG

- Penetrationstest (Link)

KOSTENPFLICHTIG

- Risikoanalyse einfach erklärt [Video] (Link)

- RiskRex Business (Link)

KOSTENPFLICHTIG

- RiskRex lite (Link)

- SIWECOS - Schnell-Check für sichere Websites [Webbasierte IT-Sicherheitsanalyse] (Link)

- Selbstcheck IT-Sicherheit [Website, Webbasierte IT-Sicherheitsanalyse] (Link)

- SiToM [Website] (Link)

- SoSafe Awareness-Plattform [Website] (Link)

KOSTENPFLICHTIG

- Umsetzungsrahmenwerk zum Notfallmanagement: Risikoanalyse [Selbststudium] (Link)

- Wissenschaft trifft Praxis - Digitales Recht & Sicherheit (Ausgabe 10) (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Gesetzliche und vertragliche Anforderungen erfüllen

Welche Gesetze sind für Ihr Unternehmen relevant? Sind Sie in einer KRITIS-Branche tätig? Verarbeiten Sie personenbezogene Daten? Informieren Sie sich regelmäßig und erfassen Sie die regulatorischen Vorgaben neben vertraglichen Anforderungen Ihrer Kunden und Partner. Integrieren Sie die Aspekte in Bezug auf Informationssicherheit sowie Datenschutz in Ihre IT-Sicherheits-Aktivitäten.

Unsere Umsetzungsvorschläge:

- Basic Security Audit (Link)

KOSTENPFLICHTIG

- Beratung Informationssicherheit und Compliance (Link)

KOSTENPFLICHTIG

- Bericht der Artikel-29-Datenschutzgruppe über die Pflicht zur Meldung bei den nationalen Kontrollstellen [Broschüre/Flyer (Digital)] (Link)

- Best Speakers Datenschutz (Link)

KOSTENPFLICHTIG

- Checkliste für Informationssicherheit (Link)

- CyberSecurity Reifegrad-Analyse (Link)

KOSTENPFLICHTIG

- Datenschutz Quick Check (Selbstauskunft) [Webbasierte IT-Sicherheitsanalyse] (Link)

- Datenschutz-Beratung (Link)

KOSTENPFLICHTIG

- Datenschutz-Navigator (Link)

- Externer Datenschutzbeauftragter (Link)

KOSTENPFLICHTIG

- Fa. Cyberdyne: IT-Sicherheitsberatung (Link)

KOSTENPFLICHTIG

- Infoblatt „Meldung von Datenschutzverstößen“ [Broschüre/Flyer (Digital)] (Link)

- Interimsmanagement IT-Security (Link)

KOSTENPFLICHTIG

- Kurzübersicht und Checkliste zu IT-Compliance [Broschüre/Flyer (Digital)] (Link)

- Leitfaden – Was ist IT-Compliance? [Broschüre/Flyer (Digital)] (Link)

- Paket KMU-Sicherheit (Link)

KOSTENPFLICHTIG

- Standard-Datenschutzmodell [Broschüre/Flyer (Digital)] (Link)

- Suchportal DSGVO-Gesetz [Website] (Link)

- Themenheft IT-Sicherheit und Recht (Link)

- Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel] (Link)

- Wissenschaft trifft Praxis - Digitales Recht & Sicherheit (Ausgabe 10) (Link)

- ds-be Datenschutz (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM” nach Registrierung.

Auf IT-Notfälle vorbereiten

Ein IT-Notfall kann verschiedene Ausprägungen haben, von einem Stromausfall bis zum erfolgreichen Angriff auf Ihre IT-Systeme. Bereiten Sie sich entsprechend vor,

indem Sie erste Maßnahmen in einem Notfallplan festlegen. Bestimmen Sie dabei, wann Systeme abzuschalten sind oder wann nur das Netzwerk oder ein Stromkabel zu trennen ist. Nehmen Sie wichtige Telefonnummern für den Notfall auf und verteilen Sie Notfallkarten an die Arbeitsplätze, da im Notfall auf digitale Dokumente nicht zugegriffen werden kann.

Unsere Umsetzungsvorschläge:

- Cyber-Sicherheitsnetzwerk - Anlaufstelle und Notfallnummer für Betroffene von IT-Sicherheitsvorfällen (Link)

- DSGVO-Rechtsschutz (Link)

KOSTENPFLICHTIG

- Datensicherheit - kurz und knapp - Ein Leitfaden für die Praxis [Buch] (Link)

KOSTENPFLICHTIG

- Gothaer-Cyber-Versicherung (Link)

KOSTENPFLICHTIG

- Hinweisschild Verhalten bei IT-Notfällen (Link)

- IT-Notfallplan - Im Ernstfall richtig reagieren [Broschüre/Flyer (Digital)] (Link)

- IT-Notfallübungen – Krisenstabsübungen [Präsenzschulung] (Link)

KOSTENPFLICHTIG

- Maßnahmenkatalog Notfallmanagement (Link)

- Online-Kurs Notfallmanagement (Link)

- Professioneller Service im Bereich IT-Forensik (Link)

KOSTENPFLICHTIG

- Ransomware-Hilfe-Seite "No more Ransom" [Website] (Link)

- Talent Connection (Link)

KOSTENPFLICHTIG

- Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel] (Link)

- Workshop - Vorbereitung auf Cyber-Notfälle und Cyber-Angriffe (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Leitlinie erstellen und veröffentlichen

Wie adressiert Ihr Unternehmen die Anforderungen an IT-Sicherheit und wie sollten sich Ihre Beschäftigten verhalten? Erstellen Sie ein kompaktes Dokument (ca. 1-2 Seiten), aus dem die Ziele, die wichtigsten Tätigkeiten und entsprechende Verhaltensvorgaben für alle Beschäftigten und ggf. Externe hervorgehen. Machen Sie die Bedeutung der Informationssicherheit durch die Veröffentlichung des Dokuments für alle Betroffenen deutlich und aktualisieren Sie das Dokument regelmäßig.

Unsere Umsetzungsvorschläge:

- Basic Security Audit (Link)

KOSTENPFLICHTIG

- Beratung Informationssicherheit und Compliance (Link)

KOSTENPFLICHTIG

- Business Continuity Management System (BCMS) (Link)

KOSTENPFLICHTIG

- Checkliste IT-Sicherheitsrisiko Mensch [Broschüre/Flyer (Digital)] (Link)

- CyberSecurity Reifegrad-Analyse (Link)

KOSTENPFLICHTIG

- Cybersecurity Navigator [Website, Wissenschaftliches Informationsangebot] (Link)

- Datensicherheit - kurz und knapp - Ein Leitfaden für die Praxis [Buch] (Link)

KOSTENPFLICHTIG

- Fa. Cyberdyne: IT-Sicherheitsberatung (Link)

KOSTENPFLICHTIG

- IT-Notfallplan - Im Ernstfall richtig reagieren [Broschüre/Flyer (Digital)] (Link)

- Interimsmanagement IT-Security (Link)

KOSTENPFLICHTIG

- Leitfaden zur Basis-Absicherung nach IT-Grundschutz [Broschüre/Flyer (Print)] (Link)

- Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung [Broschüre/Flyer (Digital)] (Link)

- Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg [Website] (Link)

- Musterleitlinie Informationssicherheit (Link)

- Musterleitlinie zur IT-Sicherheit im Rahmen des WhitePapers "Sicherheitskonzept (Mustervorlage) für Betreiber Öffentlicher Kommunikationsnetze und -dienste" [Broschüre/Flyer (Digital)] (Link)

- Online-Kurs zum IT-Grundschutz - Die Sicherheitsleitlinie [Selbststudium] (Link)

- Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel] (Link)

- Unternehmensrichtlinie für Informationssicherheit (Link)

- Wissenschaft trifft Praxis - Digitales Recht & Sicherheit (Ausgabe 10) (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

- Privatnutzung klären

Erlauben Sie die Nutzung der Firmen-IT für private Zwecke? Dürfen Mitarbeitende auch mit ihrem privaten Endgerät arbeiten? Legen Sie fest, ob und in welchem Rahmen die private Nutzung der Unternehmens-IT wie auch die Nutzung von privaten Endgeräten für dienstliche Zwecke erlaubt ist. Wenn Sie vertrauliche Daten besser schützen möchten, sollten Sie Privates und Dienstliches strikt trennen.

Unsere Umsetzungsvorschläge:

- Leitfaden – Was ist IT-Compliance? [Broschüre/Flyer (Digital)] (Link)
- Orientierungshilfe der Bayerischen Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz [Broschüre/Flyer (Digital)] (Link)
- Private Nutzung von E-Mail und Internet am Arbeitsplatz [Video] (Link)
- Vortrag von der CeBIT 2013 zu rechtlichen Aspekten von BYOD (Bring Your Own Device) [Video] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Personelle Aktionen

Der Mensch ist die größte Schwachstelle und zugleich die beste Schutzmaßnahme, wenn es um Daten- und Informationssicherheit geht. Die personellen Aktionen helfen Ihnen dabei, Ansprechpartner zu etablieren und die Belegschaft regelmäßig vorzubereiten und zu begleiten.

• Schulungen durchführen

Gut geschulte Mitarbeitende handeln bewusster. Schulen Sie daher Ihre Mitarbeitenden und ggf. Externe regelmäßig zu IT- und Informationssicherheitsthemen. Achten Sie dabei auf kurze, gut verdauliche Lerneinheiten, die sich an der jeweiligen Zielgruppe orientieren.

Unsere Umsetzungsvorschläge:

- Firewall und Netzwerksicherheit (Link)

KOSTENPFLICHTIG

- Webinare zu IT-Sicherheit [Webinar] (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Vorbildfunktion als Geschäftsführung leben

Die Geschäftsführung prägt in Ihrer Vorbildfunktion den Umgang mit Daten- und Informationssicherheit in ihrer Organisation. Informieren Sie sich daher selbst regelmäßig über die aktuelle Risikolage, passen Sie Ihre Gegenmaßnahmen der Risikolage an und lassen Sie sich den Umsetzungsstand sowie die Wirksamkeit Ihrer Maßnahmen berichten. Halten Sie sich gerade als Geschäftsführung an die selbst aufgestellten Regeln!

Unsere Umsetzungsvorschläge:

- CAk report [Newsletter] (Link)

- Der IT-Sicherheitsblog für den Mittelstand [Blog] (Link)

- Heise Security Pro [Website, Forum] (Link)

KOSTENPFLICHTIG

- Heise Security [Website, Forum] (Link)

- Initiative Wirtschaftsschutz - Das Informationsportal [Website] (Link)

- Interimsmanagement IT-Security (Link)

KOSTENPFLICHTIG

- Ransomware-Hilfe-Seite "No more Ransom" [Website] (Link)

- Sicherheitsbarometer [App] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

IT-Sicherheitsbeauftragten benennen

Nur mit einer festen Ansprechperson können Sie die IT-Sicherheit in Ihrem Unternehmen vorantreiben. Bestimmen Sie eine:n IT-Sicherheitsbeauftragte:n - aus Ihrem Betrieb oder von Außen - als Ansprechpartner:in für IT-Sicherheitsfragen und informieren Sie alle relevanten Gruppen darüber. Wählen Sie für diese Funktion weder IT-Leitende noch IT-Ansprechpersonen, das kann zu Konflikten führen.

Unsere Umsetzungsvorschläge:

- ISMS & DSGVO: Rollen und Aufgaben [Artikel] (Link)

- Intro to Information Security [MOOC, Fernstudium] (Link)

- Leitfaden – Was ist IT-Compliance? [Broschüre/Flyer (Digital)] (Link)

- Rollen und Aufgaben in der IT-Sicherheit: CISO, Security Manager oder IT-Sicherheitsbeauftragter? [Artikel] (Link)

- Talent Connection (Link)

KOSTENPFLICHTIG

- Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Sicherheitsbewusstsein steigern

Nur wenn Mitarbeitende die Risiken auch wahrnehmen, können sie sich sicher verhalten. Steigern Sie das Bewusstsein für Informationssicherheit bereits beim Einstieg neuer Mitarbeitender. Sensibilisieren Sie zudem in regelmäßigen Abständen für einen sicheren Umgang mit IT-Systemen und Informationen. Dabei unterstützen Sie etwa Aushänge, Flyer oder Info-Mails.

Unsere Umsetzungsvorschläge:

- 25 Passwort-Manager für PC und Smartphone [Artikel] (Link)

KOSTENPFLICHTIG

- Awareness-Blog [Blog] (Link)
- Awareness-Schulung (Link)

KOSTENPFLICHTIG

- Best Practices für Phishing-Simulationen (Link)
- Black Belt IT-Security Training [Educational Game] (Link)
- Bleib wachsam, Darmstadt! (Link)
- CAk report [Newsletter] (Link)
- Checkliste für Informationssicherheit (Link)

- Cybersecurity Awareness Blog [Blog] (Link)
- Der IT-Sicherheitsblog für den Mittelstand [Blog] (Link)
- E-Mail-Sicherheits-Check: have I been pwned? [Website] (Link)
- HPI Identity Leak Checker: Wurden Ihre Identitätsdaten ausspioniert? [Website] (Link)
- Heise Security Pro [Website, Forum] (Link)

KOSTENPFLICHTIG

- Heise Security [Website, Forum] (Link)
- IT 4 KMU: Warum IT-Sicherheit? [Video] (Link)
- IT-Notfallübungen – Krisenstabsübungen [Präsenzschulung] (Link)

KOSTENPFLICHTIG

- IT-SICHERHEIT - Magazin für Informationssicherheit und Compliance [Fachzeitschrift] (Link)

KOSTENPFLICHTIG

- IT-Sicherheit am Arbeitsplatz [Artikel] (Link)
- IT-Sicherheit für KMU [Video] (Link)
- IT-Sicherheitscheck (Link)
- Initiative Wirtschaftsschutz - Das Informationsportal [Website] (Link)
- KMU. Einfach sicher. [Blog] (Link)
- KMU. Einfach sicher: Das Anwendernetzwerk [Arbeitskreis] (Link)

- KeePass Passwort Safe (Link)
- KeePassXC (Link)
- Leitfaden zur Basis-Absicherung nach IT-Grundschutz [Broschüre/Flyer (Print)] (Link)
- Live Hacking und Awareness Show (Link)

KOSTENPFLICHTIG

- Mission IT-sicher [App] (Link)
- Mitgliedschaft bei Allianz für Cybersicherheit [Website, Forum] (Link)
- Muster-Passwortkarte (Link)
- Paket KMU-Sicherheit (Link)

KOSTENPFLICHTIG

- Poster Bildschirmsperre (Link)
- Poster USB-Stick-Alarm (Link)
- Security Awareness Standortbestimmung (Link)

KOSTENPFLICHTIG

- Security Awareness messbar steigern – Dos and Don'ts bei Phishing-Simulationen [Webinar] (Link)
- Sevencast [Podcast] (Link)
- Sichere Digitalisierung im Mittelstand [Broschüre/Flyer (Digital)] (Link)
- SoSafe Awareness-Plattform [Website] (Link)

KOSTENPFLICHTIG

- brand eins/thema IT-Dienstleister 2021 [Fachzeitschrift] (Link)

KOSTENPFLICHTIG

- usd Security-Awareness-Plattform (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Technische Aktionen

Um Ihre Informationen und IT-Systeme vor Angriffen aus dem Cyberraum zu schützen, müssen Sie es Angreifenden schwer machen. Die technischen Aktionen erhöhen dabei den Schutz von IT-Anwendungen, Netzwerken und – sofern vorhanden – vernetzten Maschinen.

• Netzwerke trennen

Verbundene interne Netzwerke können es dem Angreifer leicht machen, sich im Unternehmen auszubreiten. Trennen Sie daher interne Netzwerke je nach Anwendungsbereich. Stellen Sie etwa ein Gäste-WLAN zur Verfügung, das von Ihrem Büronetzwerk getrennt ist. Wenn Sie im verarbeitenden Gewerbe tätig sind, trennen Sie insbesondere Ihr Büronetzwerk vom Produktionsnetzwerk.

Unsere Umsetzungsvorschläge:

- Firewall und Netzwerksicherheit (Link)

KOSTENPFLICHTIG

- Funktionsweise eines Advanced Persistent Threat (APT) [Video] (Link)
- Grundregeln zur Absicherung von Fernwartungszugängen [Broschüre/Flyer (Digital)] (Link)
- IT-Sicherheit für KMU [Webinar] (Link)
- Regelbasiertes Firewallsystem für KMU (Link)

KOSTENPFLICHTIG

- Sicheres Datennetzwerk für meinen Handwerksbetrieb [Präsenzschulung] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Übersicht über Benutzerkonten erstellen

Angreifer nutzen zunehmend die Konten von Mitarbeitenden, z.B. über Phishing. Das Risiko kann beschränkt werden, wenn nicht "jeder alles kann". Wer nutzt welches Benutzerkonto? Welche Rollen und Berechtigungen gehören zu diesem Benutzerkonto? Dokumentieren Sie dies regelmäßig in einer übersichtlichen Liste so, dass Sie jederzeit auch die Vergabe, Änderung und Löschung nachvollziehen können.

Unsere Umsetzungsvorschläge:

- Was ist Benutzerverwaltung? [Artikel] (Link)
- tenfold Berechtigungsmanagement-Software (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Eigenes Netzwerk absichern

Ohne Schutzmaßnahmen können Unbefugte recht einfach auf Ihr Netzwerk zugreifen. Sichern Sie daher Ihr Netzwerk ab, z. B. indem Sie fremde Geräte im WLAN abweisen. Nutzen Sie zudem VPN-Lösungen, wenn Sie mit anderen Standorten bzw. mobilen Mitarbeitenden kommunizieren.

Unsere Umsetzungsvorschläge:

- Cloudflare DDoS-Schutz (Link)

KOSTENPFLICHTIG

- Firewall und Netzwerksicherheit (Link)

KOSTENPFLICHTIG

- Funktionsweise eines Advanced Persistent Threat (APT) [Video] (Link)
- Grundregeln zur Absicherung von Fernwartungszugängen [Broschüre/Flyer (Digital)] (Link)
- IT-Sicherheit für KMU [Webinar] (Link)

- Kaspersky DDoS Protection [Anwendungsprogramm] (Link)

KOSTENPFLICHTIG

- Sicheres Datennetzwerk für meinen Handwerksbetrieb [Präsenzschulung] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Ehemalige Benutzerkonten sperren

Angreifer nutzen gerne "verlassene" Anmeldedaten, um unbemerkt auf IT-Systeme zuzugreifen. Wird ein Benutzerkonto nicht mehr benötigt, sperren oder löschen Sie es. Vermerken Sie die Änderung auch in Ihrer Übersicht.

Unsere Umsetzungsvorschläge:

- Was ist Benutzerverwaltung? [Artikel] (Link)

- tenfold Berechtigungsmanagement-Software (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Schadsoftware verhindern

In der Regel hilft es dem Angreifer am meisten, wenn er es schafft, Schadsoftware auf ein IT-System aufzuspielen. Schützen Sie Ihre IT-Systeme vor Schadprogrammen. Installieren Sie dafür bei Bedarf Antivirus-Software oder nutzen Sie die betriebseigenen Abwehrmechanismen.

Unsere Umsetzungsvorschläge:

- Firewall und Netzwerksicherheit (Link)

KOSTENPFLICHTIG

- Funktionsweise eines Advanced Persistent Threat (APT) [Video] (Link)

- Grundregeln zur Absicherung von Fernwartungszugängen [Broschüre/Flyer (Digital)] (Link)

- IT-Sicherheit für KMU [Webinar] (Link)

- Kaspersky Small Office Security (Link)

KOSTENPFLICHTIG

- NoSpamProxy Protection (Link)

KOSTENPFLICHTIG

- SecuMail (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

IT-Administration dokumentieren

IT-Adminstratoren sind besonders interessante Ziele für Hacker. Eine Kontrolle der Befugnisse sowie der technischen Umsetzung hilft im Angriffsfall den Schaden zu begrenzen. Welche Rollen und Berechtigungen haben Ihre IT-Administratoren? Dokumentieren Sie diese ebenso detailliert wie die Befugnisse, Aufgaben und Pflichten dieser Personen.

Unsere Umsetzungsvorschläge:

- ISMS & DSGVO: Rollen und Aufgaben [Artikel] (Link)

- Rollen und Aufgaben in der IT-Sicherheit: CISO, Security Manager oder IT-Sicherheitsbeauftragter? [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Starke Authentifizierung verwenden

Verarbeiten Sie geschäftskritische Informationen auf Ihren IT-Systemen? Dann nutzen Sie besonders sichere Lösungen zur Identitätsprüfung wie eine Mehr-

Faktor-Authentifizierung. Dabei wird Ihre Identität anhand zweier physisch getrennter Merkmale geprüft, beispielsweise als Code per SMS und Passwort im Browser.

Unsere Umsetzungsvorschläge:

- 25 Passwort-Manager für PC und Smartphone [Artikel] (Link)

KOSTENPFLICHTIG

- E-Mail-Sicherheits-Check: have I been pwned? [Website] (Link)
- Empfehlungen für Passwörter [Artikel] (Link)
- HPI Identity Leak Checker: Wurden Ihre Identitätsdaten ausspioniert? [Website] (Link)
- KeePass Passwort Safe (Link)
- KeePassXC (Link)
- Kurz erklärt – 3 Tipps für mehr IT-Sicherheit [Video] (Link)
- Password Depot (Link)

KOSTENPFLICHTIG

- Sicherer Umgang mit Passwörtern Schritt-für-Schritt erklärt [Artikel] (Link)
- Zwei-Faktor-Authentisierung [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Verschlüsselung einsetzen

Vertrauliche Informationen benötigen einen besonderen Schutz: Verschlüsseln Sie geschäftskritische Dokumente sowohl bei der digitalen Ablage als auch bei der Übertragung, etwa per E-Mail.

Unsere Umsetzungsvorschläge:

- Gpg4win [Anwendungsprogramm] (Link)
- Key2B (Link)
- Qualifizierte Transportverschlüsselung (qTLS) für datenschutzkonforme E-Mails (Link)

KOSTENPFLICHTIG

- Reddoxx Reddcrypt Business (Link)

KOSTENPFLICHTIG

- Z1 SecureMail Gateway (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Datensicherung durchführen und testen

IT-Systeme können ausfallen, oder angegriffen werden - in beiden Fällen sind Ihre Daten möglicher Weise weg. Schützen Sie sich vor ungewolltem Datenverlust. Führen Sie daher regelmäßige Datensicherungen durch und üben Sie regelmäßig, die Datensicherungen von wichtigen Systemen wiederherzustellen.

Unsere Umsetzungsvorschläge:

- Datensicherung: Grundsätzliches zum Sichern von Daten [Broschüre/Flyer (Digital)] (Link)
- Erklärvideo zum Thema Datensicherung [Video] (Link)
- ReBack (Link)

KOSTENPFLICHTIG

- ReFile (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Sichere Einstellungen wählen

Viele IT-Systeme sind im Auslieferungszustand auf maximale Flexibilität ausgelegt - nicht auf höchste Sicherheit. Sorgen Sie für sichere Einstellungen in von Ihnen verwendeten IT-Systemen und Software-Anwendungen. Hierzu gehören z. B. das Entfernen von nicht benötigten Anwendungen, das Vermeiden von Tracking-Cookies, das Sperren vom Bildschirm oder die Nutzung integrierter Sicherheitsmechanismen wie Malware-Erkennung und Code-Signatur-Prüfung.

Unsere Umsetzungsvorschläge:

- Kurz erklärt – 3 Tipps für mehr IT-Sicherheit [Video] (Link)
- Sichere Konfiguration von Microsoft Office 2013/2016/2019 [Broschüre/Flyer (Digital)] (Link)
- Sicherheits-Checkliste: Web-Browser [Artikel] (Link)
- Softwareupdates – ein Grundpfeiler der IT-Sicherheit [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

• Software und IT-Systeme aktuell halten

Die aktuell größte Bedrohung ergibt sich durch veraltete Software und IT-Systeme. Stellen Sie sicher, dass alle IT-Systeme und Software-Anwendungen stets auf aktuellem Stand sind. Konfigurieren Sie Ihre Geräte, automatische Updates bevorzugt nachts einzuspielen. Nicht alle Anbieter informieren aktiv über die Verfügbarkeit von Updates, daher müssen Sie ggf. selbst regelmäßig prüfen, ob es für Ihre IT-Systeme und Software Updates gibt.

Unsere Umsetzungsvorschläge:

- Kurz erklärt – 3 Tipps für mehr IT-Sicherheit [Video] (Link)

- Letec Patch-Management (Link)

KOSTENPFLICHTIG

- Patchmanagement Praxisleitfaden [Broschüre/Flyer (Digital)] (Link)

- Sichere Konfiguration von Microsoft Office 2013/2016/2019 [Broschüre/Flyer (Digital)] (Link)

- Softwareupdates – ein Grundpfeiler der IT-Sicherheit [Artikel] (Link)

- Warum sind Softwareupdates so wichtig? [Artikel] (Link)

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.

Schwachstellen finden und schließen

IT-Systeme werden mit der Zeit immer angreifbarer, da Hacker bisher noch nicht bekannte Schwachstellen finden und diese publik machen. Durch regelmäßige Überprüfungen Ihrer IT-Systeme und Software-Anwendungen können Sie bekannte Schwachstellen aufspüren. Automatisierte Verfahren unterstützen Sie dabei. Schließen Sie die gefundenen Schwachstellen dann schnellstmöglich.

Unsere Umsetzungsvorschläge:

- Basic Security Audit (Link)

KOSTENPFLICHTIG

- Checkliste für Informationssicherheit (Link)

- CyberSecurity Reifegrad-Analyse (Link)

KOSTENPFLICHTIG

- Fa. Cyberdyne: IT-Sicherheitsberatung (Link)

KOSTENPFLICHTIG

- IT-Sicherheitscheck (Link)

- Paket KMU-Sicherheit (Link)

KOSTENPFLICHTIG

HINWEIS: Detailliertere Umsetzungsvorschläge finden Sie in Ihrer persönlichen TISiM-Übersicht „Meine TISiM" nach Registrierung.