Industrie- und Handelskammer zu Leipzig

IT-Sicherheit

Die fortschreitende Digitalisierung von Geschäftsprozessen, mit all ihren Vorteilen, bedingt auch eine höhere Sensibilisierung beim Thema Daten- und Informationssicherheit. Entscheidend ist das Wissen über Risiken und konkrete Maßnahmen. Die nachfolgenden Materialien, Angebote und Informationen unterstützen Sie dabei.

Bei einem akuten Sicherheitsvorfall kontaktieren Sie bitte die Zentrale Ansprechstelle Cybercrime des LKA Sachsen (Telefon: 0351 855-3226 / E-Mail: zac.lka@polizei.sachsen.de)

- Selbstchecks
- Präventive Sicherheitsmaßnahmen und Mitarbeitersensibilisierung
- Auswahl IT-Dienstleister
- Sicher in die Cloud
- Anbieter aktueller Sicherheitsmeldungen
- Anlaufstellen und Empfehlungen bei einem IT-Sicherheitsvorfall
- Zusammenfassung Internetangebote
- Fördermittel

Viele Sicherheitsangriffe werden nicht bemerkt. Sie werden ermöglicht durch zum Teil einfach zu behebende Sicherheitslücken. Dabei können größere Schäden bei frühzeitigem Erkennen des Angriffs vermieden werden. Dies betrifft auch das Vermeiden von Wirtschaftsspionage. Die folgenden Tests helfen Ihnen, Ihre Technik zu prüfen.

Sicherheitstool Mittelstand (SiToM)

Das Sicherheitstool-Mittelstand ist ein effektives Werkzeug, um den Status der IT-Sicherheit in Ihrem Unternehmen zu erfassen, zu bewerten und durch die Umsetzung vorgeschlagener Maßnahmen zu verbessern.

Sicherheitscheck zum Stand der IT-Sicherheit

Der DsiN-Sicherheitscheck bietet einen leicht verständlichen Überblick über den Stand der IT-Sicherheit in Ihrem Unternehmen und informiert über Handlungsbedarf zu datenschutz- und datensicherheitsrechtlichen Aspekten.

Sicherheitscheck Unternehmens-Website

Ein Großteil der Angriffe von Cyber-Kriminellen richtet sich gegen Webseiten von kleinen und mittelständischen Unternehmen, die besonders häufig Sicherheitslücken in ihrem Internetauftritt haben. Der Webseiten-Check SIWECOS der Initiative "IT-Sicherheit in der Wirtschaft" hilft Webseitenbetreibern zu überprüfen, ob ihre

Webpräsenzen mit Schadcode infiziert sind und unterstützt bei dessen Beseitigung.

Sicherheitscheck E-Mail auf Schadsoftware
Das Video des Bundesamtes für Sicherheit in der Informationstechnik zeigt, wie E-Mails auf mögliche Schadsoftware geprüft werden können.

Sicherheitscheck E-Mail-Konto
Mit diesem Angebot kann geprüft werden, ob E-Mail-Adressen vom Identitätsdiebstahl betroffen sind.

Sicherheitscheck Netzwerk
Dieser Test überprüft Router auf Sicherheitslücken und ob das System offene Ports aufweist. Über diese sind oft die Administrationsoberflächen oder anderen Dienste erreichbar, die sich für Angriffe missbrauchen lassen könnten.

Sicherheitsangriffe lassen sich nie vollständig vermeiden. Aber präventive Maßnahmen sind entscheidend, um den Schaden zu minimieren, die Wahrscheinlichkeit zu verringern und Vorfälle überhaupt zu erkennen. Dies umfasst z.B. organisatorische Maßnahmen, Mitarbeitersensiblisierung und Datensicherung. Mit dem Wissen über die Möglichkeiten können Sie die richtigen Entscheidungen treffen. Folgende Angebote helfen Ihnen dabei.

Sicherheitsmaßnahmen

Leitfaden Informationssicherheit - IT-Grundschutz kompakt
Der Leitfaden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet einen kompakten und allgemeinverständlichen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen. Im Mittelpunkt stehen organisatorische Maßnahmen und die Veranschaulichung von Gefahren durch Praxisbeispiele. Auf technische Details wurde bewusst verzichtet.

Leitfaden IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen
Die in diesem Leitfaden zusammengestellten Informationen und Handlungsempfehlungen sollen eine Hilfestellung zur Verbesserung der IT-Sicherheit darstellen. Die enthaltenen Checklisten unterstützen Sie dabei, herauszufinden, ob Sie die organisatorischen und rechtlichen Anforderungen bereits erfüllen oder ob noch Handlungspotenziale offen sind.

IT-Notfallmanagement
Die umfassenden Informationen zum Notfallmanagement des BSI thematisiert die Gefährdungslage sowie konkrete Maßnahmenempfehlungen.

Datensicherung
Informationsflyer des Mittelstand 4.0-Kompetenzzentrums Chemnitz mit 10 Regeln die helfen, Ihre Unternehmensdaten zu sichern. Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet.

Sichere E-Mail-Kommunikation
Der Leitfaden für Geschäftsführer und Entscheider erklärt in 19 Schritten die wichtigsten Punkte für den Geschäftsalltag.

E-Mail-Verschlüsselung

Der Leitfaden gibt einen Überblick über die wichtigsten Aspekte der E-Mail-Sicherheit, insbesondere über die Mailverschlüsselung.

Sichere Verwendung von mobilen Endgeräten
Informationsflyer des Mittelstand 4.0-Kompetenzzentrums Chemnitz mit 10 Regeln zu sicheren Verwendung von Tablets und Smartphones im betrieblichen Alltag.

Mitarbeitersensibilisierung

Wichtigste Grundregeln
Eine Übersicht über die sechs wichtigsten Grundregeln für die Informationssicherheit als Basiswissen für Mitarbeiter.

Checkliste "IT-Sicherheitsrisiko Mensch"
Checkliste des Mittelstand 4.0 Kompetenzzentrums Berlin zur Überprüfung, ob Mitarbeiter auf digitale Angriffe vorbereitet und ausreichend zum Thema IT- und Informationssicherheit informiert sind.

Verhaltensregeln für Mitarbeiter
Der Leitfaden mit Verhaltensregeln zur Informationssicherheit für Mitarbeiter kann als Grundlage für die Entwicklung eines eigenen Sicherheits-Gesamtkonzeptes dienen. Zudem kann die Broschüre zur Mitarbeiterschulung oder als Nachschlagewerk zu Sensibilisierungsmaßnahmen im Bereich der Informationssicherheit eingesetzt werden.

Plakatkampagne "IT-Sicherheit ist KEIN Spiel"
Eine Kampagne der Initiative "IT-Sicherheit in der Wirtschaft". Die Plakate können kostenfrei per E-Mail über it-sicherheit-in-der-wirtschaft@bmwi.bund.de bestellt werden.

Projekt "KMU Aware"
Ziel des Projekts der Initiative "IT-Sicherheit in der Wirtschaft" ist es, kleine und mittlere Unternehmen aufzuzeigen, wie sie sich effektiv schützen können. Hierbei stehen drei Themen im Fokus: Das Erkennen von Social Engineering Angriffen, die Verwendung sicherer Passwörter sowie die Verwendung sicherer Privatsphäreneinstellungen. Die Projektergebnisse werden über www.awareness-im-mittelstand.de veröffentlicht. Bereits jetzt steht das Anti-Phishing Training "NoPhish" zur Verfügung.

Muster-Passwortkarte
Erleichtert die regelkonforme Passwortbildung sowie das Merken und Aufbewahren. Die Passwortkarte kann als Datei heruntergeladen oder kostenlos bestellt werden.

10 Regeln für sichere Passwörter
Handlungsanleitung des Mittelstand 4.0-Kompetenzzentrums Chemnitz.

Die große Mehrheit der Unternehmen in Deutschland setzt bei ihrer IT auf externe Dienstleister. Diese sollten vertrauenswürdig sein und die Prozesse mit ihnen müssen klar geregelt werden. Die IHK-Organisation hat für Sie Informationen zusammengestellt, worauf Sie bei der Beauftragung von IT-Dienstleistungen achten sollten.

Informationen für Unternehmen
Mit diesen Kriterien haben Sie alle Sicherheitsrelevanten Fragen zur Hand, um einen vertrauenswürdigen IT-

Dienstleister auswählen zu können.

Informationen für IT-Dienstleister
Wenn Sie IT-Dienstleistungen anbieten, unterstützen Sie diese Kriterien dabei, sich mit ihrem Angebot zu präsentieren und IT-Sicherheit als Qualitätsmerkmal herauszustellen.

Download Kriterienkatalog
In dieser Checkliste für Unternehmen und Dienstleister wurden alle Kriterien zusammengefasst. Damit können Sie alle Punkte vor Beauftragung und zur Prüfung der Dienstleistung besprochen werden.

Hilfestellung für die Auswahl qualifizierter Dienstleister vom BSI
Auch das BSI stellt zu verschiedenen Themengebieten eine Liste von Kriterien bereit, die bei der Auswahl eines qualifizierten Dienstleisters hilfreich sind und zur Unterstützung herangezogen werden können.

Cloud Computing ist gerade für kleinere und mittlere Unternehmen eine oft sinnvolle Lösung. Folgende Angebote liefern Ihnen einen Einblick und Orientierung zu sicherheitsrelevanten Fragen und Möglichkeiten.

Cloud-Scout
Auf dem Weg in die Cloud bietet der DsiN-Cloud-Scout kleinen und mittelständischen Unternehmen einen spielerischen Überblick zu sicherheitsrelevanten Fragen.

Eckpunkte für sicheres Cloud Computing
Der Leitfaden der Bitkom für Entscheider aus kleinen und mittelständischen Unternehmen stellt Eckpunkte für sicheres Cloud Computing dar. Es werden die aus der Cloud-Nutzung entstehenden Chancen verdeutlicht sowie die Auswahl für einen Cloud Service Provider erleichtert.

Trusted Cloud – Orientierung im Cloud Computing
Plattform mit Angeboten zum praxisnahem Grundwissen, Übersicht geprüfter, vertrauenswürdiger Cloud Services und Anbieter cloud-bezogener Dienstleistungen wie Integration, Training und Beratung.

Checkliste zur Auswahl eines Cloud-Services
Übersicht von Kriterien, die Anwender mindestens beachten und vor Vertragsabschluss beim Anbieter einfordern sollten, falls diese nicht klar im Angebot und im Vertrag dargestellt werden.

Folgende Angebote halten Sie über aktuelle Meldungen zu Angriffen und Sicherheitslücken auf dem Laufenden.

Der Warn- und Informationsdienst von CERT-Bund
Das Computer Emergency Response Team (CERT) der Bundesverwaltung publiziert Informationen zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für IT-Systeme.

DsiN-Sicherheitsbarometer
Das DsiN-Sicherheitsbarometer zeigt aktuelle Risiken im Internet für Privatanwender und kleine Unternehmen. Das Barometer differenziert die Gesamtgefahrenlage nach der Ampelkennzeichnung "grün", "gelb" und "rot" und wird auch als App angeboten.

IT-Sicherheitsvorfälle sind in aller Regel Fälle von Cybercrime oder Wirtschaftsspionage und können auch trotz sorgfältiger Sicherheitsvorkehrungen passieren. Wichtig ist, darauf vorbereitet zu sein, z.B. durch eine gute Datensicherung und einen IT-Notfallplan (siehe Prävention). Auch regelmäßige Sicherheitschecks können Unregelmäßigkeiten aufdecken und ggf. vor Schäden schützen (siehe Selbstchecks).

Wenn Sie einen Sicherheitsvorfall entdeckt haben, scheuen Sie nicht davor, diesen zu melden. Wichtige

Ansprechpartner sind die Polizei sowie IT-Forensik-Dienstleister. Diese analsysieren die betroffenen Systeme und sichern gerichtlich verwendbares digitales Beweismaterial.

Ansprechstellen der Polizei

Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft stehen Unternehmen als kompetenter und vertrauensvoller Partner zur Verfügung, sowohl für Informationen zur Vermeidung von Cybercrime-Angriffen als auch im Falle von Cybercrime-Straftaten.
Kontakt des LKA Sachsen bei einem akuten Vorfall:
Tel: 0351 855-3226
E-Mail: zac.lka@polizei.sachsen.de

Regeln für den Umgang mit einem Sicherheitsvorfall

Die 10 Regeln sollen Ihnen helfen, die Funktionsfähigkeit Ihrer IT-Systeme effizient zu schützen und im Schadensfall wiederherzustellen.

Handlungsempfehlungen bei IT-Sicherheitsvorfällen

Die Broschüre des BKA bietet Hilfestellung, wenn Unternehmen von Cybercrime-Straftaten betroffen sind. Es werden Empfehlungen zum Umgang mit solchen Angriffen gegeben darüber informiert, was Sie in solchen Fällen von der Polizei erwartet werden können.

Checkliste IT-Notfallplan

Checkliste des Mittelstand 4.0 Kompetenzzentrums Berlin zur richtigen Reaktion nach Eintritt eines Ernstfalls.

Meldestelle des BSI

Um einen Beitrag zum vom Bundesamt für Sicherheit in der Informationstechnik zu erstellenden Lagebild zu leisten, sollten Sicherheitsvorfälle und Cyber-Angriffe auf Unternehmen gemeldet werden. Um dies zu erleichtern, wir ein Online-Meldeformular zur Verfügung gestellt. Die Meldestellennutzung ist auch anonym möglich.

Identifizierung von Ransomware

Angebot zur Identifizierung der Ransomware, die die Daten verschlüsselt hat.

Leitfaden IT-Forensik

Der "Leitfaden IT-Forensik" des BSI richtet sich insbesondere an Betreiber von IT-Systemen, Administratoren und Sicherheitsverantwortliche. Er beschreibt IT-Forensik als eine methodisch vorgenommene Datenanalyse auf Datenträgern und Computernetzen zur Aufklärung von IT-Sicherheitsvorfällen.

Es stehen Ihnen zahlreiche Angebote von öffentlich geförderten Initiativen oder Verbänden zur Verfügung, die Sie beim Thema IT-Sicherheit unterstützen.

BSI

Website des Bundesamtes für Sicherheit in der Informationstechnik mit zahlreichen Informationen zur IT-Sicherheit.

BSI für Bürger

Die Informationen und Hilfestellungen sind auch für Unternehmen interessant. Themen ins u.a. Schadprogramme, Basisschutz, WLAN und Kosten.

Deutschland sicher im Netz

Informationen, Ratgeber und Tools bieten u.a. Unternehmen vielfältige Unterstützung bei Themen wie Entwicklung der IT-Sicherheit, Cloud, Mitarbeiterschulung und Datenverschlüsselung. Es handelt sich um eine Initiative unter der Schirmherschafft des Bundesministeriums des Innern.

Allianz für Cybersicherheit

Im Fokus der Initiative des BSI steht die Unterstützung von KMUs. Neben einem umfangreichen

Informationspool fördert die Allianz auch den Erfahrungsaustausch durch Veranstaltungen, Expertenkreise und Workshops.

IT-Sicherheit in der Wirtschaft
Die Initiative des Bundesministeriums für Wirtschaft und Energie (BMWi) bietet Hilfestellungen und Angebote rund um das Thema IT-Sicherheit speziell für Unternehmen.

botfrei-Beratungszentrum
Der Verband der Internetwirtschaft e.V. (eco) bietet u.a. Tools an, mit denen Sie prüfen können, ob Ihr Computer von einer Malware-Infektion befallen oder Teil des Avalanche-Botnetz ist. Es werden zudem Informationen zum Thema Ransomware, Anleitungen und weitere nützliche Werkzeuge zur Verfügung gestellt.

Ihre Bemühungen zur Verbesserung der IT-Sicherheit in Ihrem Unternehmen kann gefördert werden:

Förderprogramm "Mittelstandrichtlinie - Informationsschutz"
Der Freistaat Sachsen unterstützt im Rahmen der Mittelstandsrichtlinie Projekte von sächsischen KMU zur Verbesserung des Informationssicherheitsniveaus im Unternehmen. Ziel ist es damit, vorhandene Engpässe und Lücken des eigenen Schutzniveaus zu erkennen sowie geeignete Maßnahmen im Zuge einer stringenten Schutzstrategie abzuleiten. Bis zu 50% Zuwendung (maximal 50.000,00 Euro) gibt es für Beratungsleistungen durch qualifizierte IT-Dienstleister, den Erwerb von vorhabensbezogener Software und Hardware oder die Schulung von Mitarbeitern.

Förderprogramm "go-digital"
Der Bund unterstützt kleine und mittlere Unternehmen der gewerblichen Wirtschaft bei Beratungsleistungen u.a. zur IT-Sicherheit. Das Programm umfasst:

- Risiko- und Sicherheitsanalyse (Bewertung von Bedrohungen und möglichen Schwachstellen) der bestehenden oder neu geplanten betrieblichen IKT-Infrastruktur
- Maßnahmen zur Initiierung/Optimierung von betrieblichen IT-Sicherheitsmanagementsystemen
- Ziel: Vermeidung von wirtschaftlichen Schäden sowie Minimierung von Risiken durch Cyberkriminalität; selbständiger Betrieb von grundlegenden erforderlichen IT-Sicherheitsmaßnahmen

Was Sie zum Thema IT-Sicherheit noch wissen sollten.

Wir haben für Sie weitere Informationen zum Einstieg in das Thema IT-Sicherheit zusammengefasst. Beleuchtet werden Aspekte wie Organsiation, Mitarbeiter, Mobilität und Social Media.

Jetzt weiterlesen!

Veranstaltungshinweise

- Do, 10.10.2019, 16:00 - 18:30 Uhr, Sichere E-Mail-Kommunikation im Unternehmen

- Do, 05.12.2019, 14:00 - 19:00 Uhr, IT-Forensik-Tag - Analyse digitaler Spuren für mehr IT-Sicherheit im Unternehmen