Mittelstand-Digital Zentrum Handel

IT-Sicherheit im Handel

Die IT-Sicherheit gewinnt immer mehr an Bedeutung und darf in keinem Unternehmen mehr fehlen. Die Angriffe, denen Unternehmen dabei ausgesetzt sind, sind vielseitig und werden immer professioneller. Ransomware, Brute Force, DDoS und Co. fügen den Unternehmen erhebliche Schäden zu. Der für die deutsche Wirtschaft entstandene Schaden durch Cyber-Kriminalität beläuft sich für das Jahr 2021 auf 203 Milliarden Euro. Dieser Schaden wird, Prognosen zur Folge, für das Jahr 2022 noch höher ausfallen. Durch die Vielfalt an Möglichkeiten/Gefahren und deren fortschreitende Automatisierung ist kein Unternehmen sicher. In diesem Infoblatt zeigen wir Ihnen, wie kleine und mittlere Handelsunternehmen die Sicherheit im eigenen Betrieb eigenständig erhöhen können. Welche Präventionsmaßnahmen können ergriffen werden? Wie schützen Sie Ihre Daten? Und was ist im Schadensfall zu tun? Wir liefern Ihnen einen Überblick über die wichtigsten Schritte.

Präventionsmaßnahmen

- Sichere Passwörter verwenden
- Software aktualisieren
- Vorsicht bei Downloads
- Gesicherte Netzwerke nutzen
- Safe Browser
- Hardware schützen
- Backups erstellen
- Personal sensibilisieren
- HTTPS verwenden
- Notfallplan erstellen

INFO BLATT

Um 300 Prozent

stieg die Anzahl an Cyber-Verbrechen während der Corona-Pandemie.

18 Prozent

deutscher Unternehmen gaben an, im letzten Jahr Schäden durch Phishing-Angriffe erhalten zu haben.

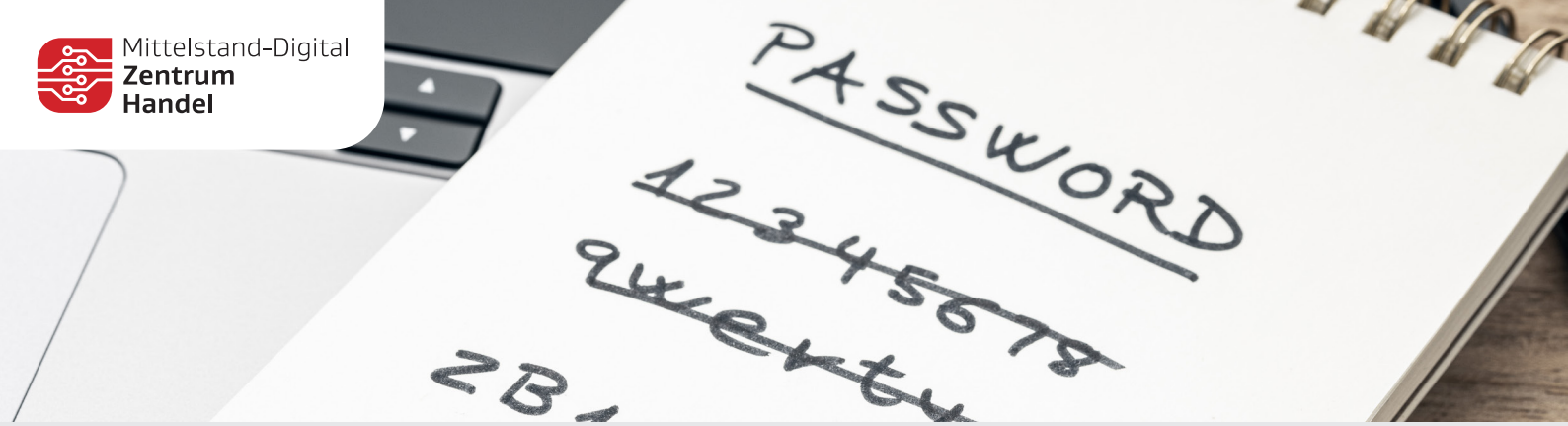
1,85 Millionen Euro

beträgt der durchschnittliche Geldschaden, der für ein Unternehmen durch Ransomware-Angriffe entsteht.

Mehr Informationen unter:
digitalzentrumhandel.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages



1. Verwenden Sie sichere Passwörter

Für Passwörter sind strikt vorgegebene Richtlinien zwingend erforderlich. Diese sollten eine Länge von mindestens 12 Zeichen besitzen und sowohl Groß- und Kleinbuchstaben, Zahlen als auch Sonderzeichen enthalten. Eine Ausnahme stellt WPA3 (Wi-Fi Protected Access 3) dar. Hier sollte unter den gleichen Vorgaben ein Passwort mindestens 20 Zeichen lang sein.

Zur Generierung oder zur Speicherung von Passwörtern können Sie einen Passwort-Generator bzw. ein Passwort-Container-Programm, wie zum Beispiel RoboForm, NordPass oder Dashlane, verwenden. Diese kosten nur wenig Geld, aber zahlen sich innerhalb kürzester Zeit aus. Bei der Benutzung müssen Sie sich nur noch ein Master-Passwort merken und können von vielen Geräten aus auf die gespeicherten Informationen zugreifen. Weiter ermöglichen diese Programme oft das automatische Ausfüllen von Online-Formularen und dadurch wird der Aufenthalt im Internet sicherer und komfortabler. Abschließend gibt es noch die nachfolgende Liste an grundlegenden Tipps mit dem Umgang von Passwörtern.

- **Verwenden Sie keine Wörter aus dem Wörterbuch.**
- **Vermeiden Sie gängige Varianten und Tastaturmuster wie z. B. „qwertz" oder „6789yxcv".**
- **Verwenden Sie nie dasselbe Passwort für mehrere Anwendungen.**
- **Geben Sie Passwörter nie an Dritte weiter.**
- **Verwenden Sie nie voreingestellte Passwörter.**
- **Verwenden Sie, wo es möglich ist, die Zwei-Faktor-Authentifizierung (2FA).**
- **Mehr Informationen zur Passwortsicherheit finden Sie z. B. hier.**

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

2. Halten Sie Ihre Software auf dem neuesten Stand

Die meisten Menschen werden diese Meldung kennen: „Ein Software-Update ist verfügbar“. Oftmals erscheint sie zu einem unpassenden Zeitpunkt und wird ignoriert. Betriebssysteme und verwendete Programme können jedoch genau dann erhebliche Schwachstellen darstellen. Deshalb ist es wichtig, zum einen Software, die Sie nicht mehr benötigen, von den Computern zu entfernen und zum anderen Software-Updates schnellstmöglich zu installieren. Das Installieren von Updates erhöht den Sicherheitsstatus der verwendeten Geräte erheblich, da diese oft kritische Sicherheitslücken schließen. Denn veraltete Versionen von Software sind oft Einladungen für Hacker.

1.

Software sollte, bevor sie heruntergeladen wird, überprüft werden (z. B. die URL), um sich vor gefälschten Anwendungen zu schützen, die darauf abzielen, Daten zu stehlen.

2.

Aktivieren Sie automatische Updates für mobile Endgeräte als auch für Computer.

3.

Überprüfen Sie Software, die sich nicht automatisch aktualisiert, regelmäßig auf Updates.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

3. Vorsicht beim Download von Software

Grund zur Vorsicht beim Download von Software liefern vor allem Schadsoftware/-programme, die sich bei einem Download verstecken können. Oftmals gibt es sogenannte Fake-Seiten, also Internetseiten, die dem Original nachempfunden sind. Wird eine Software von solch einer Webseite heruntergeladen, so lädt man häufig Adware oder andere Malware herunter. Dadurch wird es möglich, sensible Daten abzugreifen oder über das Internet Angriffe auf andere Computer innerhalb des Unternehmens durchzuführen. Es können so zum Beispiel alle Daten des Unternehmens verschlüsselt und unzugänglich gemacht werden. Laden Sie eine Software nur von vertrauensvollen Quellen herunter und wenn möglich direkt vom Hersteller. Prüfen Sie stets alle Downloads vor der Installation bzw. Anwendung mit Hilfe eines Antivirus-Programms.

Prüfen Sie die Internetadresse:

- Achten Sie auf Buchstabendreher.
- Hinterfragen Sie ungewöhnliche Domainendungen (z. B. „.de.com").
- Prüfen Sie die Internetadresse (URL).

Betrachten Sie das Impressum und die Allgemeinen Geschäftsbedingungen (AGB):

- Sind Fehler enthalten (etwa durch schlechte Übersetzungen von Übersetzungsprogrammen)?
- Fehlen Angaben?

Benutzen Sie Antivirus-Software:

- Prüfen Sie Software mit Hilfe eines Antivirusprogramms.
- Führen Sie regelmäßig Virenscans durch.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

4. Sichern Sie Ihr Netzwerk

Die Verwendung einer Firewall und einer Antivirensoftware sind in der heutigen Zeit unerlässlich. Schadprogramme wie Viren, Trojaner und Würmer nisten sich schnell auf Computern ein, ohne dass man von deren Existenz weiß.

Sichern Sie den ein- und ausgehenden Verkehr mit Hilfe eines VPN-Clients und denken Sie dabei auch an die mobilen Endgeräte.

Vorsicht ist vor allem bei der Verwendung von öffentlichen WLAN-Netzwerken geboten. Stellen Sie die Funktion, dass sich Ihr Gerät automatisch mit öffentlichen WLAN-Netzwerken verbindet, ab. Geben Sie niemals in einem öffentlichen Netzwerk Passwörter ein oder öffnen Sie wichtige/sensible Daten, denn hier kann jederzeit die Datenübertragung abgefangen werden (sog. Man-in-the-Middle-Angriff).

Des Weiteren ist es wichtig, Ihre eigenen WLAN-Router zu sichern. Diese werden häufig mit minimalen Sicherheitsstufen ausgeliefert. Stellen Sie die Sicherheitsstufe auf die höchstmögliche, ersetzen Sie das Standardpasswort und führen Sie regelmäßig Wartungen durch. Denn auch hier sind Patches/Bugfixes von großer Wichtigkeit.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

5. Nutzen Sie Safe-Browser-Funktionen

Am häufigsten werden zur Verbreitung von Schadsoftware infizierte Webseiten missbraucht. Deshalb ist es wichtig, einen modernen Browser mit robusten Sicherheits-standarts zu verwenden.

Aktivieren Sie ...

... lediglich die Inhalte, die für das Surfen im Internet benötigt werden.

... im Browser selbst die präventive Schutz-möglichkeiten vor Web-seiten. Diese heißen Safe-Browsing.

... optional Werbungs-Blocker wie „AdBlock" oder „Ublock Origin".

... die höchste Sicher-heitsstufe in den Sicher-heitseinstellungen.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

6. Schützen Sie Ihre Hardware

Die meisten Unternehmen arbeiten mit Geräten wie zum Beispiel Computer, Notebooks, Smartphones oder Tablets. Auch diese Geräte müssen vor Datenverlust geschützt werden. Dazu sollten Sie einige Regeln aufstellen:

Abschließen

Halten Sie Räume verschlossen, auch bei kurzzeitiger Abwesenheit.

Überwachung

Lassen Sie Besucher und Kundschaft nie mit Ihrer Hardware allein.

Abtrennung

Trennen Sie, wenn möglich, Betriebsräume von Räumen mit Publikumsverkehr.

Physisch absichern

Verwenden Sie ein Laptopschloss für die Diebstahlsicherung von mobilen Endgeräten.

Passwörter vergeben

Machen Sie Computer nur nach Autorisierung zugänglich.

Daten verschlüsseln

Verschlüsseln Sie sensible Daten und vergeben Sie sichere Passwörter.

Daten sichern

Sichern Sie Ihre Daten regelmäßig und bewahren Sie das Speichermedium an einem geeigneten Ort auf.

Regelmäßig prüfen

Überprüfen Sie regelmäßig die Integrität Ihres Netzwerks und Ihrer Datenbackups.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

7. Sichern Sie Ihre Daten

Es ist notwendig, Daten regelmäßig zu sichern. Dies schützt einerseits vor Datenverlust und andererseits verringert es die Erpressbarkeit. Ein Datenverlust geschieht aus den unterschiedlichsten Gründen, wie zum Beispiel durch Überschreiben von Daten, fehlende Speicherung wichtiger Daten, defekte Festplatten, Hardware-Probleme und Stromausfälle.

Zu Erpressungen kommt es durch Ransomware. Diese Schadsoftware sperrt die Daten oder Endgeräte und droht damit, diesen Zustand auch aufrecht zu erhalten. Häufig kommt es auch zu Lösegeldforderungen, um die Daten bzw. Endgeräte wieder zu entsperren. Es ist deshalb wichtig, das erstellte Backup regelmäßig auf Funktionalität, Konsistenz und Aktivität zu überprüfen. Wurde ein Backup erstellt, so sollte es auf einer externen Speichermöglichkeit gesichert werden, wie zum Beispiel auf einem USB-Stick oder einer externen Festplatte. Denn dann ist es im Schadensfall möglich, die verloren geglaubten Daten jederzeit wieder abzurufen.

Tipp: Erstellen Sie ein 3-stufiges Backup mit verschiedenen Backup-Medien und Backup-Ständen.

1. Lokales Backup

Ein mit dem Computer verbundenes lokales Backup kann regelmäßig auf den neuesten Stand gebracht werden.

2. Offline-Backup

Ein Offline-Backup wird mit externen Speichermedien erstellt und sollte sicher gelagert werden.

3. Externes Backup

Eine Backup-Datei befindet sich auf einem ortsunabhängigen Medium (z. B. an einem anderen Unternehmensstandort/ separaten Rechenzentrum).

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

8. Personal als wichtigster Bestandteil

Mitarbeiterinnen und Mitarbeiter sind der Schlüsselfaktor eines jeden Unternehmens in Sachen IT-Sicherheit. Diese gilt es dahingehend zu sensibilisieren und auf mögliche Angriffsmethoden aufmerksam zu machen.

Vermitteln Sie Ihren Mitarbeiter:innen in regelmäßigen Schulungen folgende Richtlinien:

1. Klicken Sie nie auf Links/Anhänge in E-Mails, vor allem wenn deren Absender unbekannt ist oder verdächtige E-Mail-Adressen benutzt.
2. Öffnen Sie keine Speichermedien, deren Herkunft unbekannt ist (z. B. USB-Stick).
3. Wenden Sie die Vorgaben für Passwörter an.
4. Laden Sie Programme/Daten aus dem Internet herunter, so muss vorher eine Untersuchung auf Schadsoftware erfolgen.
5. Geben Sie Daten nie leichtsinnig preis (Zugangsdaten auf einer Webseite oder in sozialen Netzwerken).

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

9. Verwenden Sie für Ihre Webseite HTTPS: Verschlüsselung sollte Standard werden

Warum sollten Webseiten HTTPS (HyperText Transfer Protocol Secure) verwenden? Über HTTPS werden gesendete Daten geschützt. Dies erstreckt sich über drei Sicherheitsebenen:

1. **Verschlüsselung:** Daten werden verschlüsselt übermittelt (können nicht gelesen oder abgefangen werden).
2. **Datenintegrität:** Übermittelte Daten können nicht verändert oder beschädigt werden.
3. **Authentifizierung:** Dies verstärkt das Vertrauen der Nutzer, denn hier wird sichergestellt, dass nur Nutzer:innen selbst und niemand anders mit der gewünschten Webseite kommuniziert. Durch die Erhöhung der Sicherheit auf Ihrer Webseite steigern Sie das Vertrauen der Nutzer:innen und auch deren Sicherheit.

Tipp: Sie erhalten HTTPS, wenn Sie ein SSL-Zertifikat oder ein TSL-Zertifikat von einer Zertifizierungsstelle anfordern & selbst installieren oder Ihr Webhosting-Anbieter dies unterstützt. Einige Browser weisen darauf hin, dass Webseiten ohne SSL-Zertifikat (= Secure Sockets Layer) unsicher sind (persönliche Daten in Eingabefelder können leicht bei der Übermittlung abgegriffen werden).

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

10. Die Entwicklung eines Notfallplans

Sollten Sie in Ihrem Unternehmen einen Schadensfall erleiden, ist es enorm wichtig, einen Notfallplan zu haben. Dieser sollte selbstverständlich für alle zugänglich sein und ist am besten auch nicht nur auf den verwendeten Endgeräten hinterlegt. Denn sollten diese ausfallen, so besteht nicht mehr die Möglichkeit, darauf zuzugreifen.

Der Notfallplan sollte außerdem **zwingend folgende Punkte enthalten**:

- die wichtigsten Kontaktpersonen mit Telefonnummern
- die Verhaltensweisen im Schadensfall

Aus den genannten Präventionsmaßnahmen lässt sich eine kleine Checkliste ableiten, die zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen beitragen kann:

- ☐ Verwenden Sie sichere Passwörter.
- ☐ Halten Sie Software immer auf dem aktuellsten Stand.
- ☐ Schützen Sie Ihre Hardware.
- ☐ Backup – Sichern Sie Ihre Daten.
- ☐ Vorsicht beim Download von Software.
- ☐ Sichern Sie Ihr Netzwerk.
- ☐ Verwenden Sie Safe Browser.
- ☐ Sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter.
- ☐ Verwenden Sie Internetseiten mit HTTPS.

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Handel

Was tun, wenn der Schadensfall eintritt?

1. Bewahren Sie Ruhe.
2. Stellen Sie die Arbeit an dem betroffenen Gerät ein.
3. Trennen Sie alle Geräte vom Netzwerk (Ausbreitung vermeiden).
4. Informieren Sie, falls vorhanden, Ihren Cyberexperten.
5. Dokumentieren Sie den Angriff (durchgeführte Schritte und Unregelmäßigkeiten).
6. Setzen Sie die betroffenen Geräte neu auf (alle Daten müssen restlos gelöscht werden).
7. Spielen Sie ein externes Backup wieder auf.
8. Ändern Sie alle vorher verwendeten Passwörter.
9. Beobachten Sie das Verhalten der Geräte genau.
10. Bei weiterhin verdächtigem Verhalten beginnt der Prozess von vorne.

Das Mittelstand-Digital Zentrum Handel gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Infoblatt: IT-Sicherheit im Handel – April 2023
Mittelstand-Digital Zentrum Handel
c/o ibi research an der Universität Regensburg GmbH

digitalzentrumhandel.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages