Mittelstand 4.0
Kompetenzzentrum
Handel

CHECKLISTE

IT-Sicherheit im Online-Handel
Die wichtigsten Fakten im Überblick

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Der Online-Handel boomt, und das nicht erst seit der Pandemie. Umso wichtiger wird das Thema IT-Sicherheit für kleine und mittlere Unternehmen (KMU). Gestiegen ist nämlich auch die Anzahl illegaler Angriffe und Hacks: Rund die Hälfte aller deutschen Einzelhandelsunternehmen wurde mindestens einmal Opfer einer Cyber-Attacke, 90 Prozent mindestens einmal Opfer von Betrug oder Betrugsversuchen. Besagte Handelsunternehmen sind besonders gefährdet: Sie haben in den meisten Fällen keine oder nur unzureichende Sicherheitsvorkehrungen und sind für Hacker deutlich leichtere Beute. Schlimmstenfalls führt ein solcher Angriff für kleine Unternehmen gar zum Bankrott. Im Folgenden erhalten Sie eine Übersicht über die größten Risiken für Online-Händler:innen – und wie Sie sich gegen Angriffe schützen.

1 Wo liegen die Gefährdungen?

IT-Sicherheit
wird häufig mit externen Einflüssen wie Hackern in Verbindung gebracht. Dabei spielen noch weitere Faktoren eine Rolle bei der IT-Sicherheit und erhöhen die Dringlichkeit, Maßnahmen zu ergreifen. Folgende Risiken gilt es zu beachten:

Höhere Gewalt
wie Wasser, Blitzschlag, Krankheit, etc. können unvorhergesehene Komplikationen in Hinblick auf sensible IT-Daten darstellen.

Organisatorische Mängel
Fehlende/unklare Regelungen und Konzepte sind oft ein erhebliches Risiko für die Cybersicherheit eines Unternehmens. Es lohnt sich also, klare Konzepte zu entwickeln und diese den Mitarbeitern zur Verfügung zu stellen:

Menschliche Fehlhandlungen
erweisen sich oftmals als die größte Sicherheitslücke in IT-Systemen. Die relevantesten Gefahrenphänomene sind hier:

- **Insider Threat (dt.: Insider-Bedrohung)**

  Missbräuchlicher Zugriff einer unternehmensinternen Person auf sensible Informationen und Systeme des Unternehmens. Bei diesen Insidern kann es sich um Mitarbeiter:innen, Drittanbieter:innen, Auftragnehmer:innen und Partner:innen handeln, die dem Unternehmen durch Ausnutzen ihres autorisierten Zugriffs auf Informationen Schaden zufügen.

  Quelle: proofpoint.com

- **Weakest Link (dt.: schwächstes Glied)**

  Ein IT-Sicherheitssystem ist nur so sicher wie sein schwächster Punkt. Durch winzige Schwachstellen in einer Sicherheitskette können massive Schäden an der IT-Sicherheit verursacht werden.

  Quelle: techrepublic.com

- **Social Hacking – Angriff auf das „menschliche Betriebssystem“**

  Das Ausnutzen menschlicher Eigenschaften durch Cyberkriminelle mit dem Ziel, sich Zugang zu IT-Systemen zu verschaffen.

  Quelle: brandmauer.de

  Technisches Versagen wie Systemabstürze oder Plattencrashs können zu teilweisem bzw. vollständigem Datenverlust und Systemausfall führen.

  Vorsätzliche Handlungen wie Angriffe durch Hacker, Viren, Trojaner, Ransomware und Distributed Denial-of-Service sind ebenfalls ein ernstzunehmendes Sicherheitsrisiko für ihr Unternehmen.

2 Wichtige Grundlage: Passwörter

Das Hacken von Online Accounts ist der häufigste Fall von Internetkriminalität, allerdings nicht nur auf der Nutzerseite. Besonders kritisch ist dies bei Administrator-Passwörtern, mit denen auf das Shop-System zugegriffen wird. Auch das Knacken von Passwörtern auf Accounts von Marktplattformen wie z. B. eBay kann desaströse Folgen haben.

Am besten schützen Sie sich, indem Sie ausschließlich Passwörter verwenden, die länger als 12 Zeichen sind. Es sollte sich nicht um Namen oder Wörter aus dem Wörterbuch handeln. Gute Passwörter enthalten Sonderzeichen und Zahlen. Passwörter für die Systemverwaltung sollten bestenfalls aus mehr als 16 Zeichen bestehen. Um die sicheren und komplexen Passwörter unternehmensintern verwalten zu können, eignet sich zum Beispiel ein Passwortmanager.

3 Mehr Käufe dank https

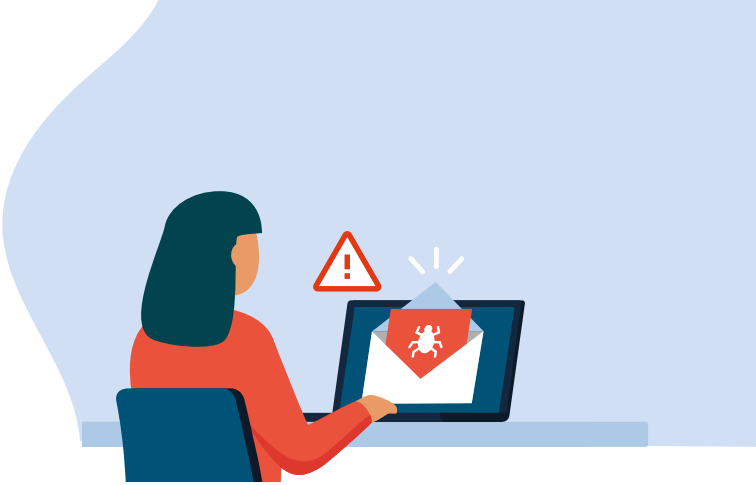
Ein nicht zu unterschätzender Faktor für die Sicherheit Ihres Online-Shops wird durch einen einzigen Buchstaben in Ihrer Domain bestimmt: Aus dem klassischen http:// wurde das sicherere https://. Das hinzugekommene „s“ steht für „secure“ (dt.: sicher). Mittels eines sogenannten TSL-Zertifikats (früher SSL) können somit nur Nutzer:innen und die abgerufene Webseite wissen, welche Daten eingegeben wurden. TLS („Transport Layer Security“, der Nachfolger von SSL für „Secure Sockets Layer“) ist die Standard-Technologie für die Sicherheit von Webseiten. Auch rechtliche Vorgaben (insb. § 13 VII TMG) für geschäftsmäßig angebotene Telemedien, worunter auch Online-Shops fallen, sind ein „als sicher anerkanntes Verschlüsselungsverfahren“.

Das Zertifikat wirkt mittlerweile auch wie ein Gütesiegel für Online-Käufer:innen. So zeigen alle gängigen Browser an, dass auf unverschlüsselten Seiten ein Sicherheitsrisiko besteht. Das Zertifikat erhöht damit die sogenannte Conversion-Rate, also die Zahl potentieller Käufer:innen auf Ihrem Online-Shop. Außerdem werden Sie mit einer SSL-Verschlüsselung in der Google-Suche höher gelistet.

4 Freies WLAN? Vorsicht!

In Home-Office Zeiten gehört mobiles Arbeiten zum Berufsalltag dazu. Schnell erledigt man einige Aufgaben im Zug oder im Café nebenan. Ein Sicherheitsrisiko: Die offenen Netzwerke sind häufig nicht verschlüsselt, Ihre Daten gelangen relativ leicht in falsche Hände. Vermeiden Sie in solchen Netzwerken das Eingeben heikler Daten und Passwörter.

Wenn Sie keine andere Wahl haben, als auf solche Netzwerke zuzugreifen, nutzen Sie einen sogenannten VPN-Client. Damit verschlüsseln und schützen Sie Ihre Daten. Mit VPN oder Virtual Provate Network können Sie eine sichere Verbindung zu einem anderen Netzwerk aufbauen (Kostenpflichtig).



5 Der Faktor Mensch

Laut dem einst meistgesuchten Hacker der Welt, Kevin Mitnick, gibt es keinen effektiveren Weg in gesicherte Computersysteme, als über die Menschen selbst. So gelange man um ein Vielfaches schneller an Daten und Passwörter, als durch komplexe technische Angriffe. Das sollten auch Sie sich zu Herzen nehmen: Unter dem Namen Phishing ist die wohl berühmteste Ausprägung des „Social Engineering“ bekannt: In E-Mails oder SMS meldet sich ein vermeintlich vertrauenswürdiges Unternehmen und fordert Sie dazu auf, Daten einzugeben oder Geld zu überweisen.

Noch perfider wird das „Social Hacking“, wenn Ihr Unternehmen und sogar einzelne Mitarbeiter:innen gezielt ausgespäht werden, um persönlich „gehackt“ zu werden: Wenige Informationen reichen schon, um ein Telefonat oder eine E-Mail des vermeintlichen Vorgesetzten real aussehen zu lassen und schlimmstenfalls im Handumdrehen das gesamte System zu kapern.

Hier hilft nur eines: Die Belegschaft muss für solche Gefahren sensibilisiert werden. Allein das Wissen um derartige Maschen kann zur raschen Erkennung versuchter Angriffe führen.

6 Erhöhte Sicherheit durch automatische Updates

Der grundlegendste Schritt zur Sicherung der internen IT-Sicherheit liegt in den Updates der verwendeten Programme: Schieben Sie die Installation neuer Updates nie auf, stellen Sie am besten gleich „Automatische Updates“ ein. So bleiben Ihre Programme stets auf dem neusten Stand der Sicherheitsstandards.

7 Gefährdungen und typische Schwachstellen von Online-Shops und Marktplätzen

Zugangssicherung (insb. Passwort)

Um Schwachpunkte effektiver zu schützen, ist eine angemessene Zugangssicherung wichtig. Diese gewährleisten Sie am besten durch die Nutzung sicherer Passwörter.

Kundenzugang im Online-Shop

Zur Zugangssicherung zählen nicht nur die firmeneigenen Zugänge, sondern auch die der Kund:innen. Hierbei sollten sie als Betreiber:in eines Online-Shops folgende Einstellungen vornehmen:

1. Ein verschlüsseltes Eingabe-/Vergabeverfahren für Kund:innen
2. Eingabe von Groß-/Kleinbuchstaben, Sonderzeichen und Zahlen. Es sollte eine Mindestlänge von 8 Zeichen haben.
3. Speicherung des Passworts im Online-Shop System erfolgt verschlüsselt (Stichwort: Hash-Funktion)

Händlerzugang im Backend des Online-Shops (siehe Kundenzugang)

Auch der Zugang zum Backend sollte durch ein Passwort mit hohen Sicherheitsstandards gesichert werden (s. Einstellungen Kundenzugang).

Händlerzugang zum Marktplatzkonto (siehe Kundenzugang)

Ihr Marktplatzkonto kann ebenso eine potenzielle Schwachstelle der IT-Sicherheit darstellen. Daher sollte auch hier auf einen Schutz durch starke Passwörter geachtet werden.

Weitere Anwendungen (WaWi, Payment etc.)

Darüber hinaus stellen alle weiteren Zugänge von Unternehmenssystemen ein Sicherheitsrisiko dar. Warenwirtschaftssysteme und Zahlungs- und Bankzugänge sollten deshalb auch mit gut verschlüsselten Passwörtern versehen werden.

8 EXTRA: HOME-OFFICE

Das Home-Office ist für viele im Laufe der Pandemie zur Normalität geworden. Es birgt allerdings gewisse IT-Sicherheitsrisiken, die berücksichtigt werden sollten. Mit folgenden Tipps für sicheres mobiles Arbeiten können Sie wesentliche IT-Gefahren für ihr Unternehmen reduzieren.

Tipps für sicheres mobiles Arbeiten

1. Regelungen für Telearbeiter/Sicherheitsrichtlinie für die Telearbeit
2. Kontinuierliche Sensibilisierung der Telearbeiter:innen für das Thema Cybersicherheit
3. Zutritts- und Zugriffsschutz
4. Sicherheitstechnische Anforderungen an die, für die Telearbeit eingesetzten, IT-Systeme/Härtung der eingesetzten IT-Systeme
5. Verschlüsselung von tragbaren IT-Systemen und Datenträgern
6. Nutzung von Bildschirmschutzfolien
7. Sicherer Remote-Zugriff auf das Netz der Institution
8. Datensicherung
9. Zeitnahe Verlustmeldung
10. Support für Telearbeitsplätze
11. Arbeiten mit fremden IT-Systemen/Netzen
12. Entsorgung von vertraulichen Informationen
13. Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am Telearbeitsplatz
14. Eindeutige Verifizierung
15. Vorsicht Phishing

Quelle: BSI

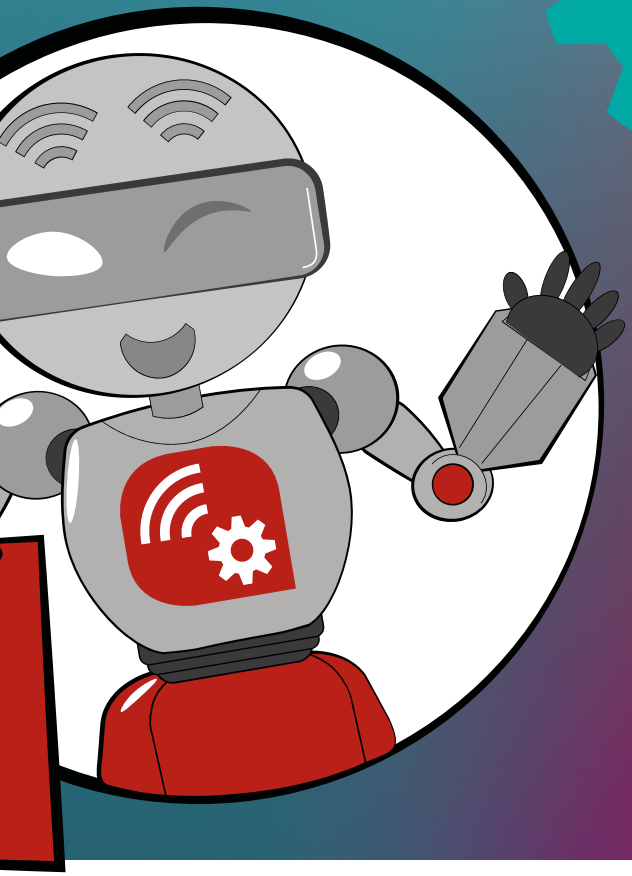
Prävention

Prävention ist der beste Schutz vor Angriffen auf Ihre Daten. Viele Maßnahmen zur Verbesserung der IT-Sicherheit sind dabei auch ohne große Investitionen umsetzbar. Es bedarf jedoch klarer Strukturen und Abläufe, um das IT-Sicherheitsniveau nachhaltig zu erhöhen. Vor allem kleinere Betriebe, die in der Regel über keine eigene IT-Abteilung verfügen, können ihren Grundschutz bereits durch kleine Vorsichtsmaßnahmen deutlich erhöhen.

Zum Beispiel mit TISiM – der Transferstelle IT-Sicherheit im Mittelstand. TISiM schafft erstmals ein bundesweites und kostenfreies Angebot, bei dem sich Betriebe und Unternehmen anbieterneutral über IT-Sicherheit informieren und konkrete Umsetzungsmaßnahmen planen können. Durch das zentrale Tool von TISiM dem Sec-O-Mat erhalten Unternehmen nach einer kurzen Befragung passgenaue Umsetzungsvorschläge zur Verbesserung ihrer IT-Sicherheit. Die Umsetzungsvorschläge bündeln dabei bereits bestehende Angebote und Initiativen und bereitet diese praxisnah auf. Der Sec-O-Mat bietet dabei einen niedrigschwelligen Einstieg in das Thema IT-Sicherheit.

Weitere Informationen entnehmen Sie der der Broschüre IT Grundschutz des Bundesamts für Sicherheit in der Informationstechnik.

Mittelstand 4.0
Kompetenzzentrum Handel



Online Sichtbarkeit

Prozesse digitalisieren

Innovationen auf der Fläche

Wir unterstützen Händler:innen **kostenfrei** bei der Digitalisierung!

kompetenzzentrumhandel.de

Mittelstand 4.0-Kompetenzzentrum Handel
@Mittelstand 4.0-Kompetenzzentrum Handel
@handelkompetent

Mittelstand-Digital

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

Über das Mittelstand 4.0-Kompetenzzentrum Handel

Das Mittelstand 4.0-Kompetenzzentrum Handel gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Weitere Informationen unter:

https://kompetenzzentrumhandel.de

Über Mittelstand-Digital

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte 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:

https://www.mittelstand-digital.de

Impressum

Herausgeber:
Handelsverband Deutschland – HDE e.V.
Am Weidendamm 1A
10117 Berlin

Tel.: +49 (0)30 72 62 50 – 0
Fax: +49 (0)30 72 62 50 – 99

info@kompetenzzentrumhandel.de
www.kompetenzzentrumhandel.de

Text:
Jennifer Kleemann
Luisa Dreckmann

Layout:
Ariane Skibbe

Fotos:
© Shutterstock
Titel: © Tero Vesalainen/Shutterstock

Stand: November 2021

Literaturverzeichnis

- Proofpoint:
  https://www.proofpoint.com/de/resources/threat-reports/human-factor
- BRANDMAUER IT GmbH:
  https://www.brandmauer.de/blog/it-security/social-hacking-definition-was-ist-social-hacking
- TechRepublic:
  https://www.techrepublic.com/article/cybersecurity-pros-are-humans-really-the-weakest-link/
- Bundesamt für Sicherheit in der Informationstechnik (BSI):
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/home-office_node.html

Mittelstand 4.0
Kompetenzzentrum
Handel

Folgen Sie dem Kompetenzzentrum Handel auf:

handelkompetent

@handelkompetent

Kompetenzzentrum Handel

Kompetenzzentrum Handel

handelkompetent

oder melden Sie sich für den Newsletter an:
kompetenzzentrumhandel.de/newsletter

kompetenzzentrumhandel.de

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages