IT-Sicherheit im Online-Handel

Carina Überle

ibi research an der Universität Regensburg GmbH

ERFOLGREICH HANDELN

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

Agenda

01 Initiative „Erfolgreich handeln“

02 Momentaufnahme Handel 2023

03 IT-Sicherheit im Handel

04 Gefährdungen für den (Online-)Handel

05 Tipps von Händlern für Händler

06 Vorhandene Hilfsangebote und Links

ERFOLGREICH HANDELN

01 Initiative „Erfolgreich handeln“

Projekt „Erfolgreich Handeln“ des Bayerischen Wirtschaftsministeriums

Der Handel soll wettbewerbsfähig bleiben – wir unterstützen dabei!

Die Corona-Pandemie, der Krieg in der Ukraine und die damit verbundenen Preissteigerungen haben massiven Einfluss auf den Handel.

Geändertes Einkaufsverhalten, veränderte Kundenbedürfnisse, hohe Energiekosten – wer in Zukunft noch erfolgreich sein will, muss sich anpassen.

Die Initiative „Erfolgreich handeln“, **initiiert und finanziert durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie**, hilft Ihnen dabei!

Projektlaufzeit: Januar 2023 bis Dezember 2024

Vorgängerprojekt: Die Förderinitiative „Bayern hilft seinen Händlern“

www.erfolgreich-handeln.bayern

ERFOLGREICH HANDELN

Wie sieht unser Bildungsangebot aus?

Unsere Formate

Webseite & Newsletter

Workshops

Webinare

Mediathek | Webinar-aufzeichnungen

Unsere Themen

ERFOLGREICH HANDELN

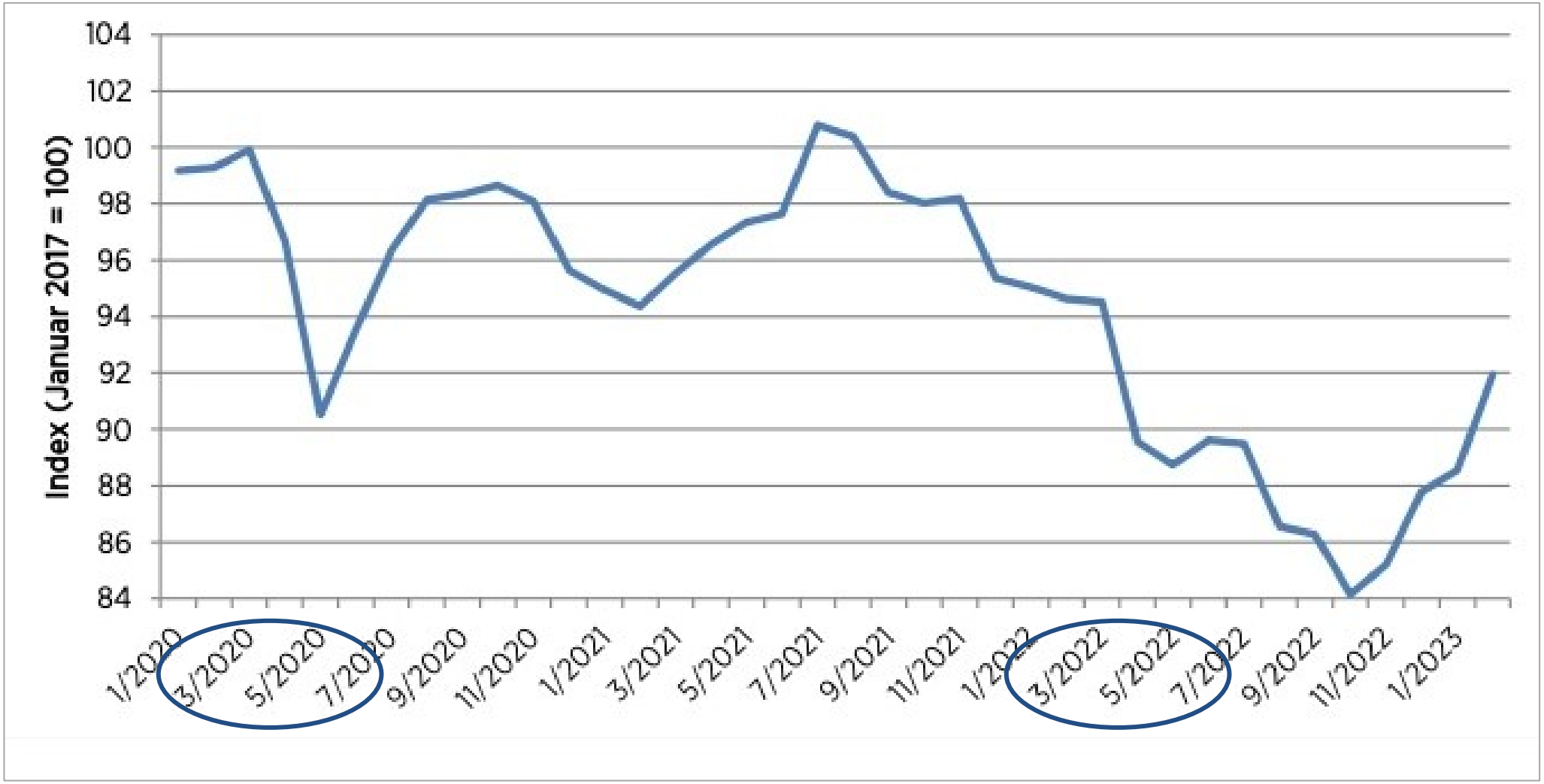
02 Momentaufnahme Handel 2023

Rückblick 2022: Handel in einem schwierigen Umfeld

- Gesamtwirtschaft behauptet sich in schwierigen Zeiten (BIP +1,9%)
- Einzelhandel 2022 mit realem Umsatzverlust
  (nominal +7,2 % (631,9 Mrd. Euro), real -0,8 %)
- Online-Handel 2022 schwächelt auf hohem Niveau
  (nominal -2,0 % (85,0 Mrd. Euro), real -6,9 %)
- Hohe Inflation (+7,9%), Lieferprobleme, Fachkräftemangel, steigende Energiekosten, Auswirkungen Ukrainekrieg bremsen Gesamtwirtschaft
- Arbeitsmarkt mit Rekorderwerbstätigkeit (45,6 Millionen Personen)
- Digitale Entwicklungen (Konsumentenverhalten) aus der Corona-Pandemie bleiben weiter relevant (z.B. unbare Zahlung, digitale Sichtbarkeit, Bedeutung der sozialen Medien, …)

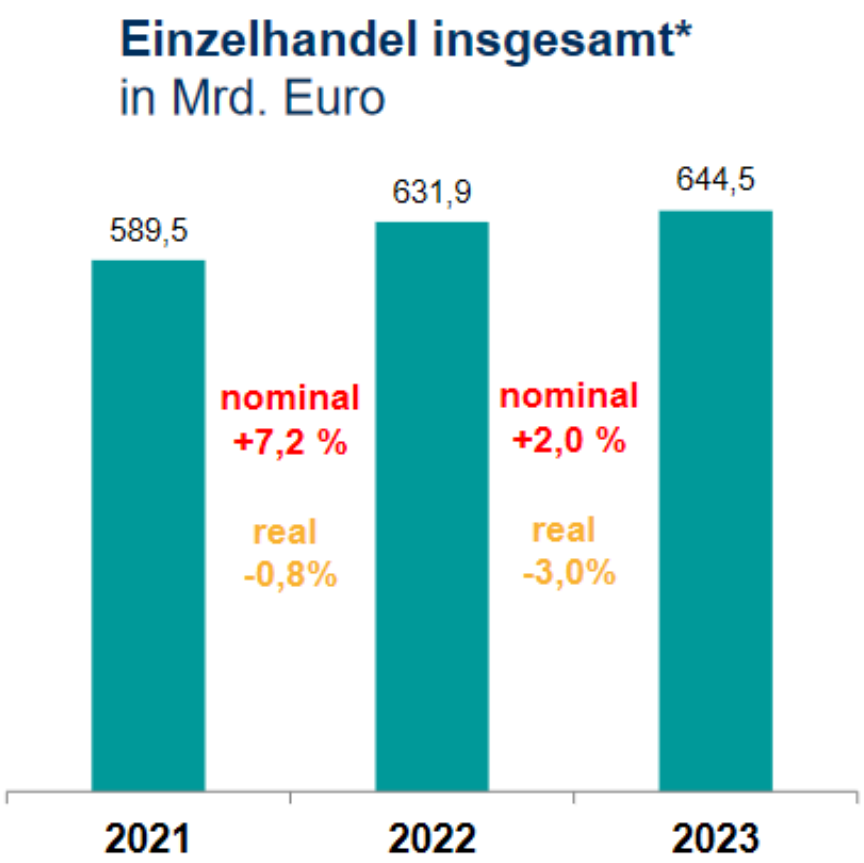
Quellen: HDE 2023; DIHK 2023; Statistisches Bundesamt 2023

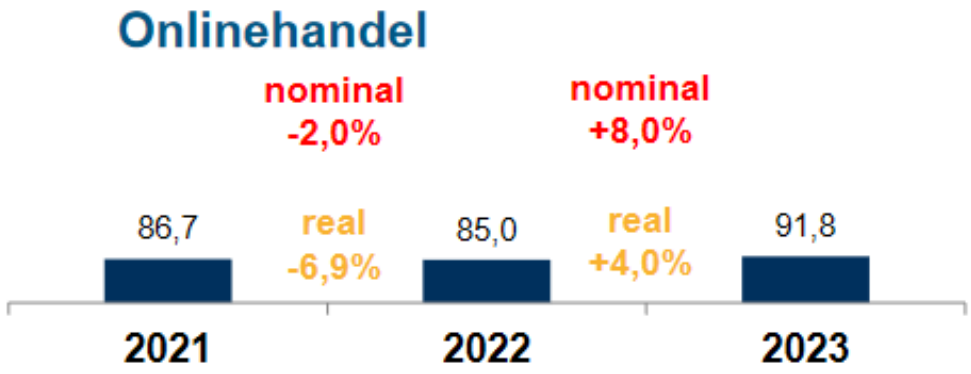
Konsumstimmung (März 2023): Erholung setzt sich fort



Quelle: HDE 2023; HDE-Konsumbarometer im März

Einzelhandel wächst 2023 nominal wieder – verliert preisbereinigt aber drei Prozent





Quelle: HDE-Prognose; HDE-Berechnungen auf Basis Destatis; nominale Veränderung zu Vorjahr; ohne Umsatzsteuer; * ohne Kfz, Tanstellen, Brennstoffe, Apotheken (WZ08-47103)

Gründe für die Nutzung oder Nicht-Nutzung des Online-Vertriebs sind im Wesentlichen unverändert und bekannt

Gründe für einen Online-Vertrieb

- Erschließung zusätzlicher Kundengruppen
- Imageverbesserung
- Kundennachfrage nach Online-Bestellmöglichkeit
- Stärkere Kundenbindung
- Druck durch Konkurrenzaktivitäten
- …

Gründe gegen einen Online-Vertrieb

- Fehlenden zeitlichen Ressourcen
- Hohe rechtliche Anforderungen
- Hohe Kosten/Hohe Provisionen
- Hohe Anforderungen an IT-Sicherheit
- Starke Abhängigkeit vom Marktplatzbetreiber
- Zu starker Wettbewerb
- …

Bei der Nutzung sozialer Medien und bei IT-Sicherheit ist der Schulungsbedarf

In welchen Bereichen sehen Sie Schulungsbedarf für Ihr Unternehmen bzw. Ihre Mitarbeiter? (Top 10)
Mehrfachauswahl möglich

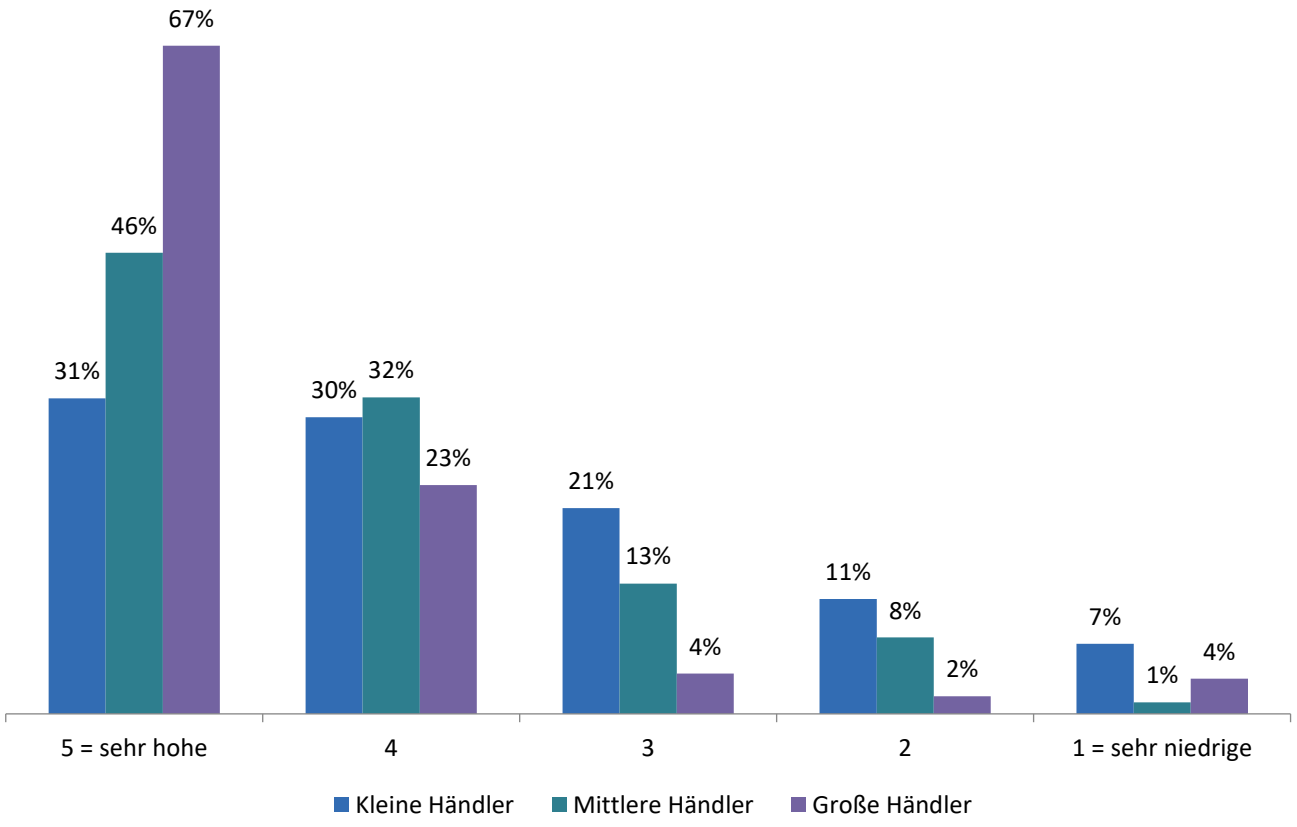
	Gesamt	Kleine Händler	Mittlere Händler	Große Händler
Soziale Medien	39%	37%	41%	50%
IT-Sicherheit	38%	36%	46%	42%
Kundenkommunikation über soziale Medien	38%	36%	44%	43%
Online-Marketing (SEO/SEA)	37%	38%	41%	28%
Datenschutz	36%	35%	39%	37%
Umgang mit dem Online-Shop	23%	24%	23%	25%
Digitalisierung von Papierdokumenten	21%	18%	30%	28%
Umgang mit Kundendaten(-anwendungen)	20%	17%	24%	43%
Umgang mit Warenwirtschaftssystemen	19%	18%	26%	18%
Umgang mit Kundenverwaltungssystemen	14%	13%	17%	33%
Wir haben keinen Schulungsbedarf	*14%*	*16%*	*8%*	*8%*

Quelle: ibi research/DIHK (2020): Der deutsche Einzelhandel 2020 – zweite IHK-ibi-Handelsstudie. n = 1.322 (alle Händler)

03 IT-Sicherheit im Handel

Je größer der Händler, desto mehr rückt das Thema IT-Sicherheit in den Fokus

Welche Bedeutung hat das Thema IT-Sicherheit in Ihrem Unternehmen?



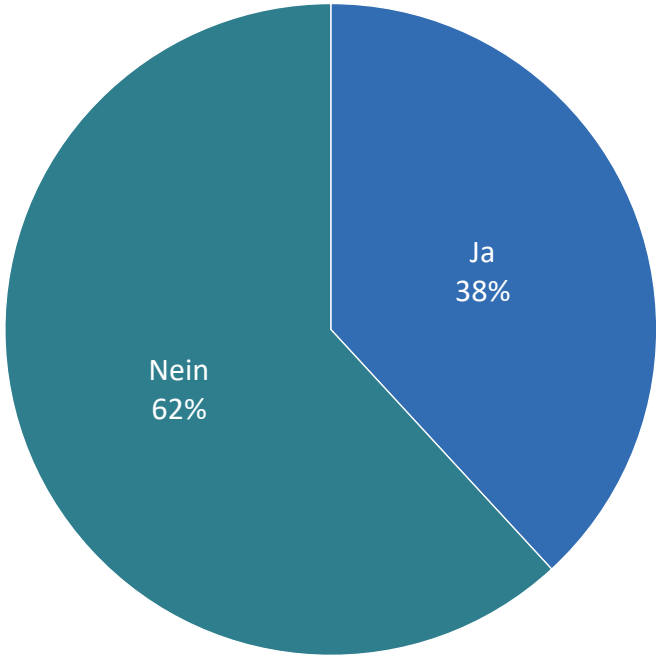
Weitere Ergebnisse zum Thema „IT-Sicherheit“

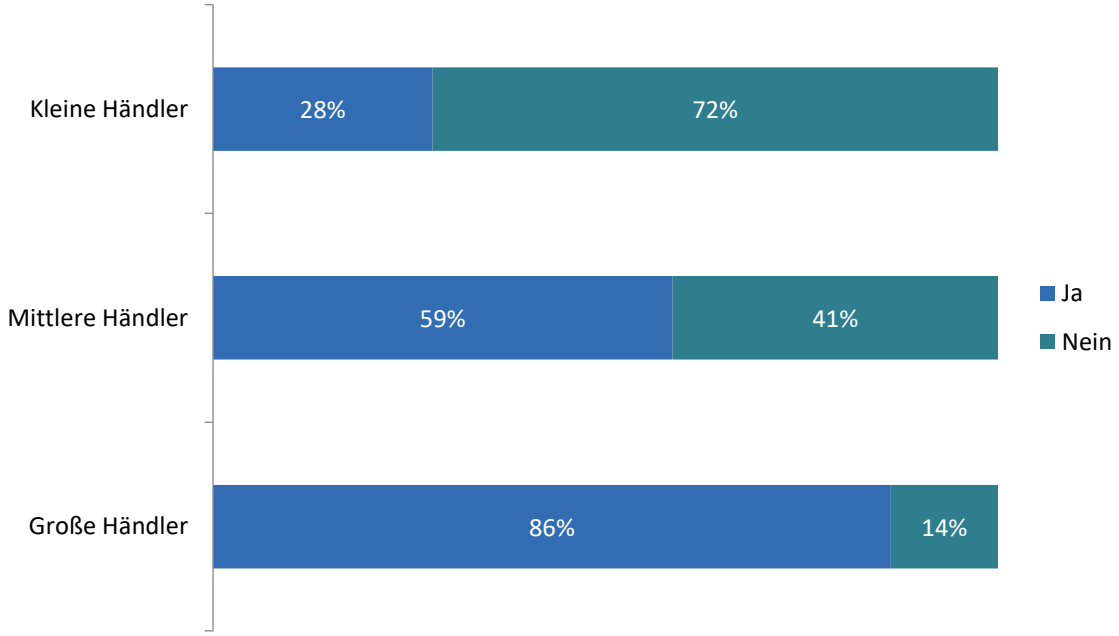
- Über 60 Prozent der Händler haben noch keine systematische IT-Sicherheitsanalyse durchgeführt; bei kleinen Händlern sind es nur 28%.
- Virenschutz, passwortgeschützte Zugänge und eine Firewall sind bei fast allen Unternehmen vorhanden.
- Zwei Drittel der Händler hatte bereits IT-Sicherheitsprobleme im Unternehmen; kleine Händler sind weniger betroffen.
- Lediglich 23% führen regelmäßige IT-Sicherheits-Schulungen durch.
- Nur knapp ein Drittel verfügt über einen Notfallplan.

Quelle: ibi research/DIHK (2020): Der deutsche Einzelhandel 2020 – zweite IHK-ibi-Handelsstudie. n = 1.124 (alle Händler)

Über 60 Prozent der Händler haben noch keine systematische IT-Sicherheits-analyse durchgeführt

Haben Sie in Ihrem Unternehmen schon einmal eine systematische IT-Sicherheitsanalyse durchgeführt?

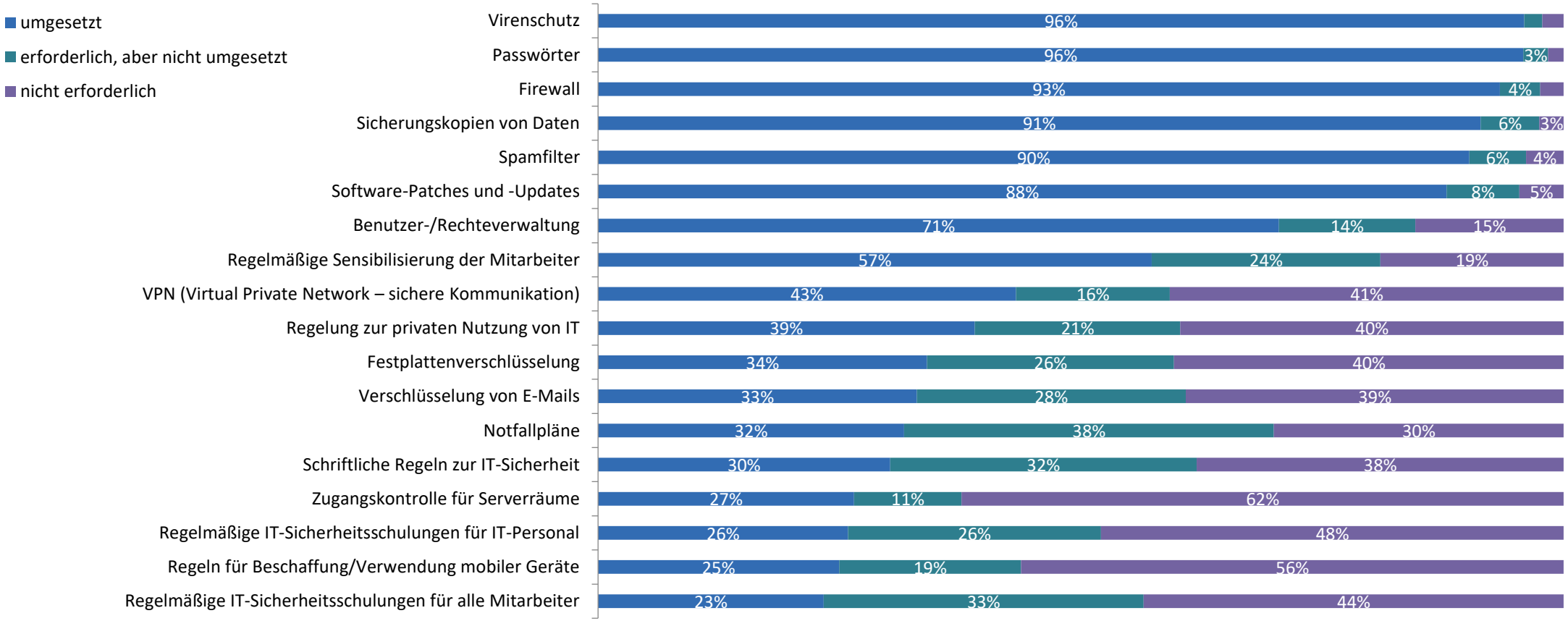




Quelle: ibi research/DIHK (2020): Der deutsche Einzelhandel 2020 – zweite IHK-ibi-Handelsstudie. n = 1.059 (alle Händler)

Virenschutz, passwortgeschützte Zugänge und eine Firewall sind bei fast allen Unternehmen vorhanden

Welche Maßnahmen halten Sie für Ihr Unternehmen für erforderlich und welche haben Sie umgesetzt?



Quelle: ibi research/DIHK (2020): Der deutsche Einzelhandel 2020 – zweite IHK-ibi-Handelsstudie. 961 ≤ n ≤ 1.178 (alle Händler); Werte kleiner drei Prozent nicht beschriftet

Ransomware-Angriff auf Media Markt Saturn – 240 Millionen US-Dollar Lösegeld gefordert

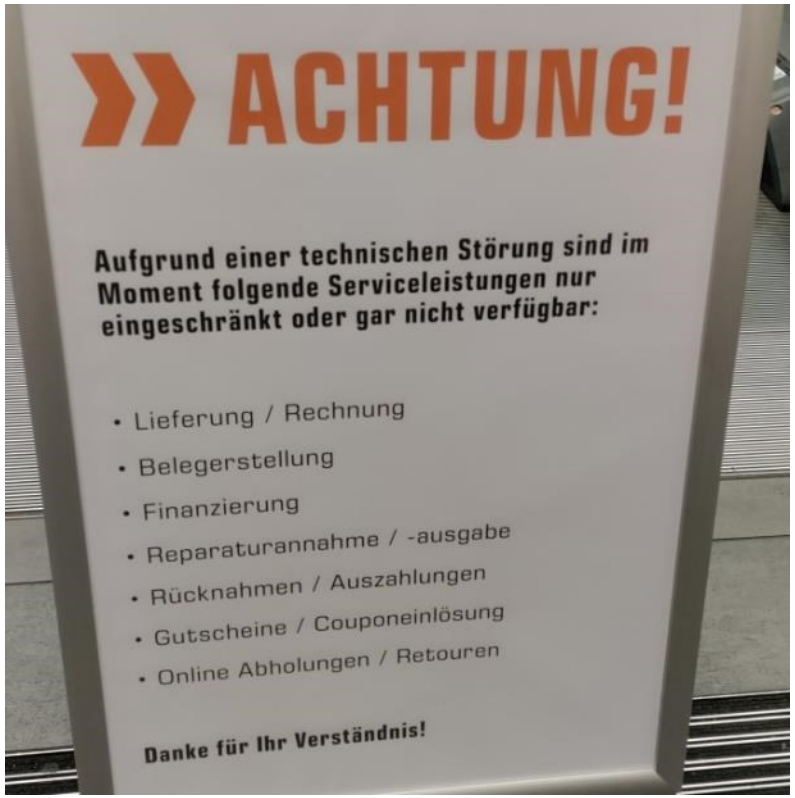
SPIEGEL Netzwelt

Verschlüsselungstrojaner

MediaMarkt-Erpresser verlangen angeblich 50 Millionen Dollar

Die Ransomware-Gruppe Hive soll zahlreiche Server von MediaMarktSaturn verschlüsselt haben – und ein hohes Lösegeld fordern. Ursprünglich wollten die Angreifer laut einem Bericht sogar noch mehr Geld.

09.11.2021, 10.20 Uhr



https://www.heise.de/news/Ransomware-Angriff-auf-Mediamarkt-und-Saturn-6260388.html
https://www.spiegel.de/netzwelt/web/mediamarkt-und-saturn-erpresser-verlangen-angeblich-50-millionen-dollar-a-5a50962b-c8ab-49bd-8291-d713375ff2d3
https://www.golem.de/news/ceconomy-ransomware-verlangt-240-millionen-dollar-von-media-markt-2111-160941.html

Ransomware – Ein Virus auf dem Vormarsch

Informationsblatt Ransomware

Schutz vor Angriffen mit Verschlüsselungssoftware

- So wie die Angriffe mit Ransomware immer ausgeklügelter werden, gewinnen ebenfalls bekannte Geschäftsmodelle in der Dark Web Sphäre an Beliebtheit. Ebenso wie Anwender:innen bei dem legalen Geschäftsmodell „Software as a Service“ (SaaS) auf ausgefeilte Programme und Infrastrukturen zurückgreifen können, bieten Entwickler:innen (Codierer:innen) von Ransomware ähnliche Modelle in kriminellen Kreisen an. Umso wichtiger ist der Schutz vor den Angriffen mit Verschlüsselungssoftware.

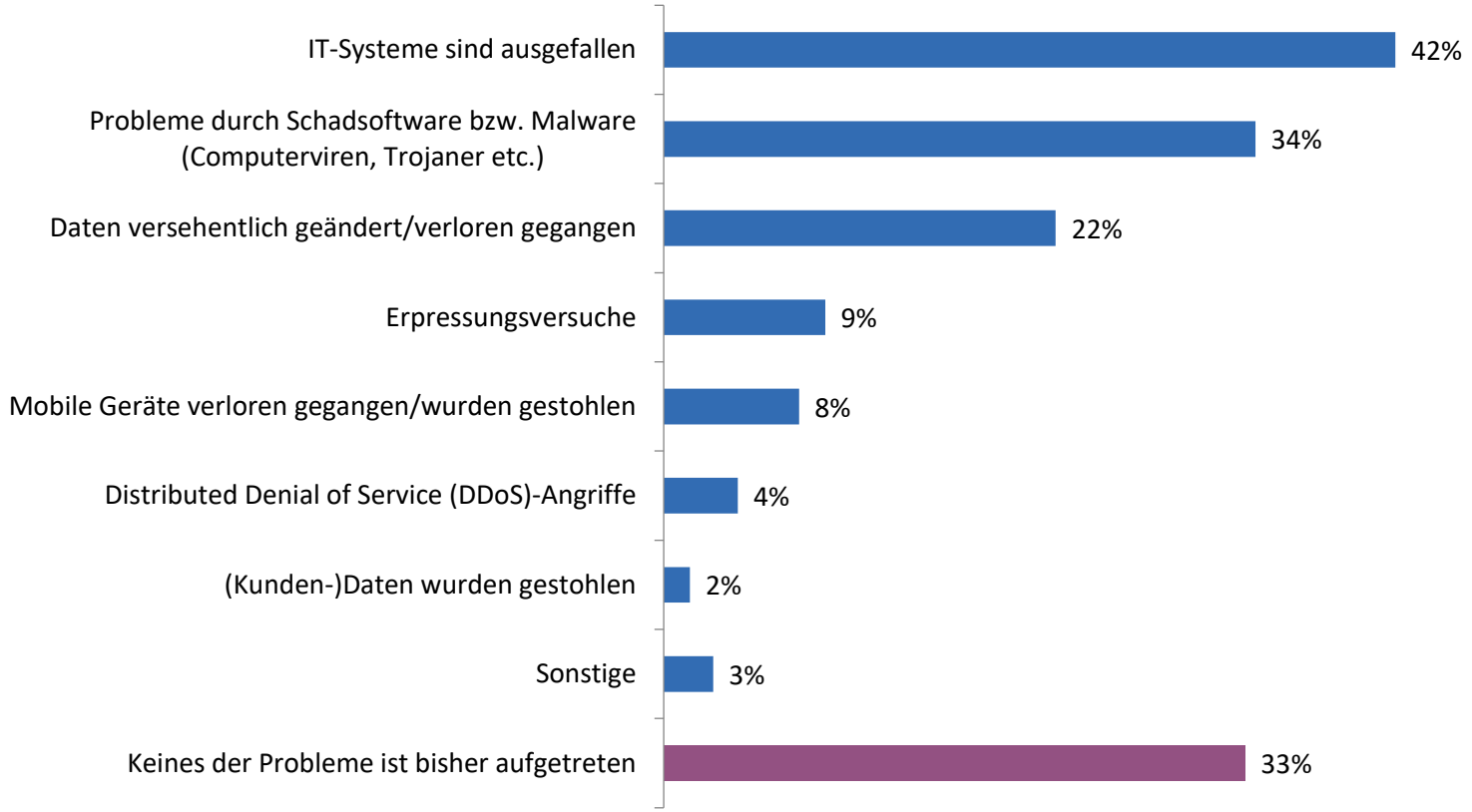
Informationsblatt Ransomware

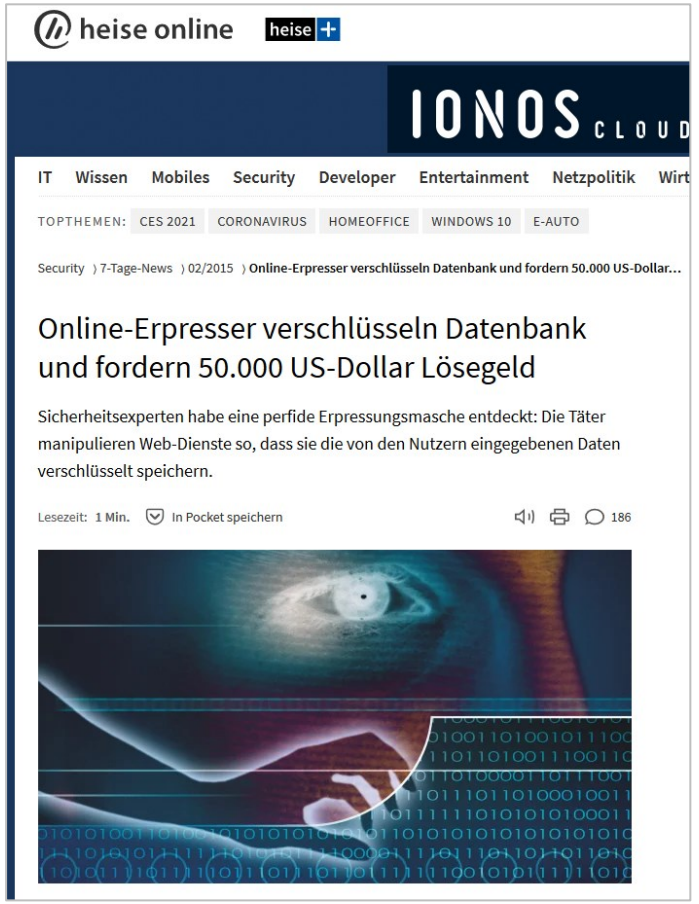
- Darum hat TISiM – die Transferstelle IT-Sicherheit im Mittelstand ein Informationsblatt erstellt mit Informationen zu Ransomware-Angriffen und wie sich Unternehmen vor diesen schützten können: https://www.tisim.de/

Download unter: https://kompetenzzentrumhandel.de/wp-content/uploads/2022/01/tisim_klaert_auf_ransomware.pdf

Jeder zehnte Händler wurde schon einmal erpresst

Haben Sie in Ihrem Unternehmen schon einmal konkrete Erfahrungen mit den folgenden IT-Sicherheitsproblemen gemacht?
(Mehrfachauswahl möglich)




heise online heise+

IONOS CLOUD

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirt

TOPTHEMEN: CES 2021 CORONAVIRUS HOMEOFFICE WINDOWS 10 E-AUTO

Security 〉7-Tage-News 〉02/2015 〉Online-Erpresser verschlüsseln Datenbank und fordern 50.000 US-Dollar...

Online-Erpresser verschlüsseln Datenbank und fordern 50.000 US-Dollar Lösegeld

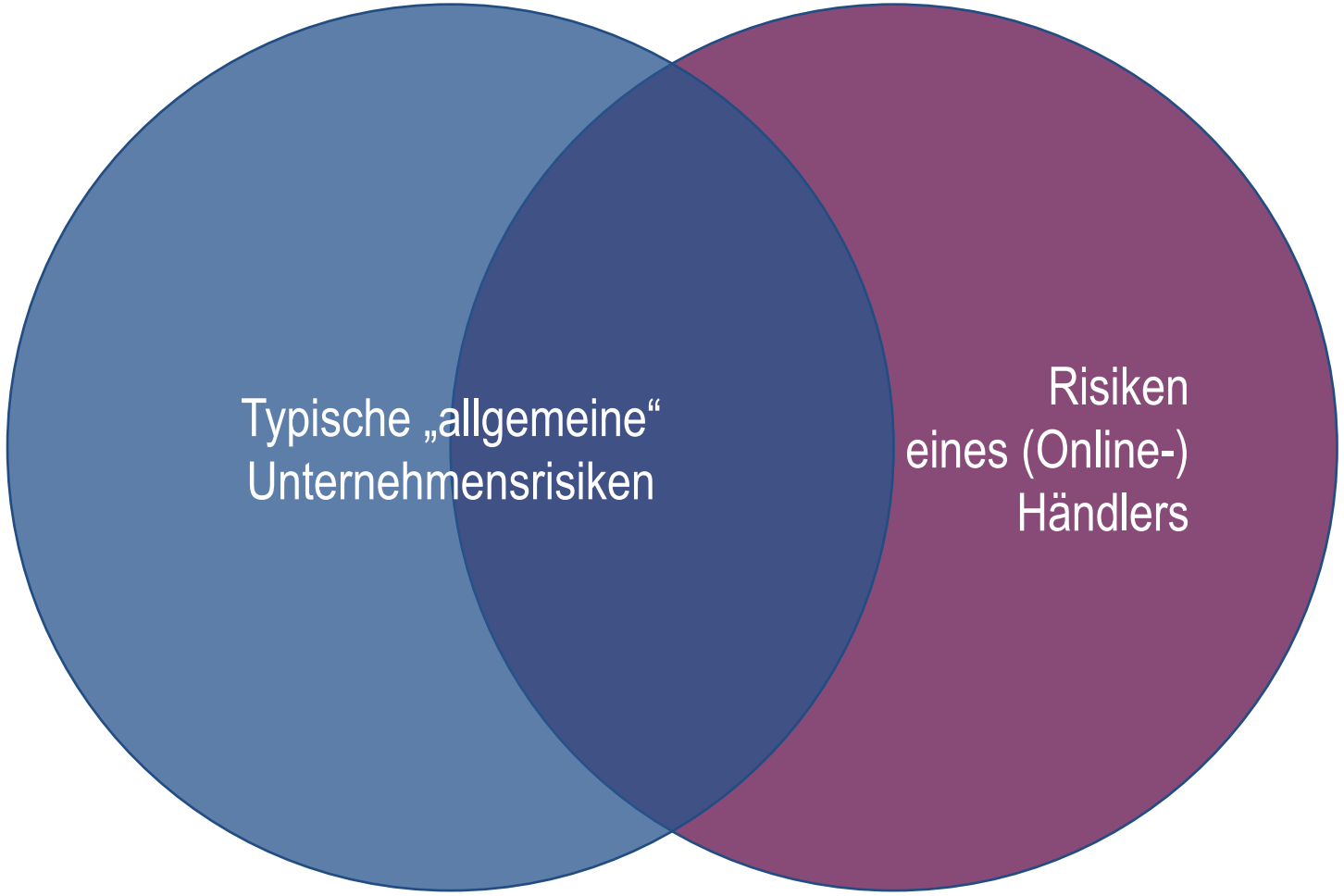
Sicherheitsexperten habe eine perfide Erpressungsmasche entdeckt: Die Täter manipulieren Web-Dienste so, dass sie die von den Nutzern eingegebenen Daten verschlüsselt speichern.

Lesezeit: 1 Min. In Pocket speichern 186

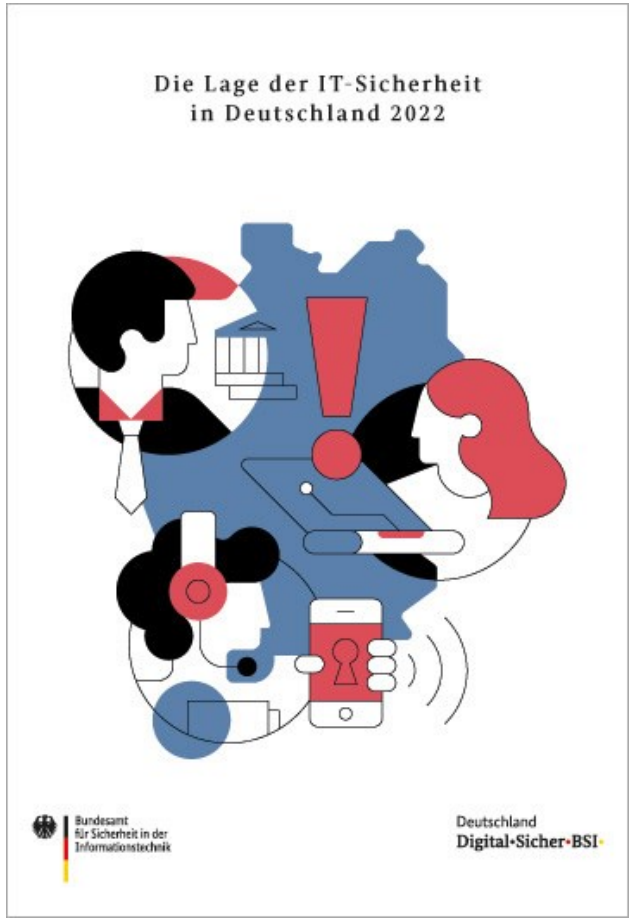
Quelle: ibi research/DIHK (2020): Der deutsche Einzelhandel 2020 – zweite IHK-ibi-Handelsstudie. n = 1.200 (alle Händler);
https://www.heise.de/security/meldung/Online-Erpresser-verschluesseln-Datenbank-und-fordern-50-000-US-Dollar-Loesegeld-2535621.html

04 Gefährdungen für den (Online-)Handel

Gefährdungen für den (Online-)Handel



IT-Sicherheitslage spitzt sich zu (BSI)



Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen, offene oder falsch konfigurierte Online-Server IT-Supply-Chain: Abhängigkeiten und Sicherheit	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000 Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000 neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall
Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

69% aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90% des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

Die Anzahl der Schadprogramme steigt stetig.
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund **116,6 Millionen** zugenommen.

Hacktivismus im Kontext des russischen Krieges:
Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits **6.220** Mitglieder.

Kollateralschaden
nach Angriff auf Satellitenkommunikation

20.174
Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Quelle: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

BSI-Studie: Viele Software-Produkte für Onlineshops sind unsicher

BSI-Studie: Viele massive Sicherheitslücken bei Online-Shops

Das BSI untersuchte E-Commerce-Plattformen und stieß auf unzureichende Passwortrichtlinien, verwundbare JavaScript-Bibliotheken und fehlende Update-Optionen.

Lesezeit: **3 Min.** In Pocket speichern 15

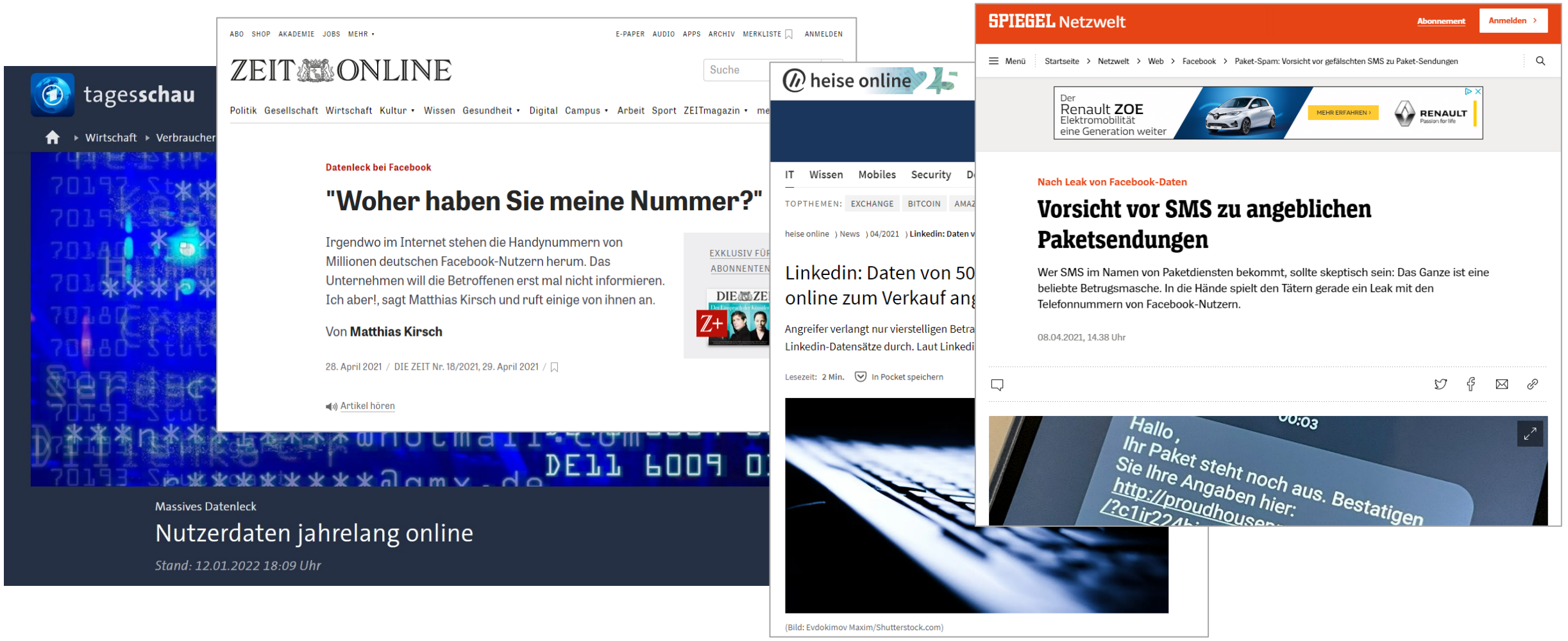
(Bild: Chiociolla/Shutterstock.com)

27.02.2023 15:33 Uhr

Von Stefan Krempl

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.html?nn=132646

Immer mehr Nutzerdaten kriminell genutzt



https://www.spiegel.de/netzwelt/web/paket-spam-vorsicht-vor-gefaelschten-sms-zu-paket-sendungen-a-2322a91b-94a7-428d-8fe1-83352e59aab9
https://www.zeit.de/2021/18/facebook-datenleck-handynummer-datenschutz-hackerangriff?utm_referrer=https%3A%2F%2Fwww.bing.com%2F
https://www.heise.de/news/Linkedin-Daten-von-500-Millionen-Nutzern-online-zum-Verkauf-angeboten-6009560.html
https://www.tagesschau.de/wirtschaft/verbraucher/datenleck-verbraucherdaten-101.html

Das leidige Thema „Passwörter“

Gefährdungen und typische Schwachstellen eines Online-Händlers (Shop/Marktplatz)

Zugangssicherung (insb. Passwort):

- Kundenzugang im Online-Shop
- Händlerzugang zum E-Mail-Account
- Händlerzugang im Backend des Online-Shops
- Händlerzugang zum Marktplatzkonto
- Weitere Anwendungen (WaWi, Payment, …)
- …

Maßnahmen:

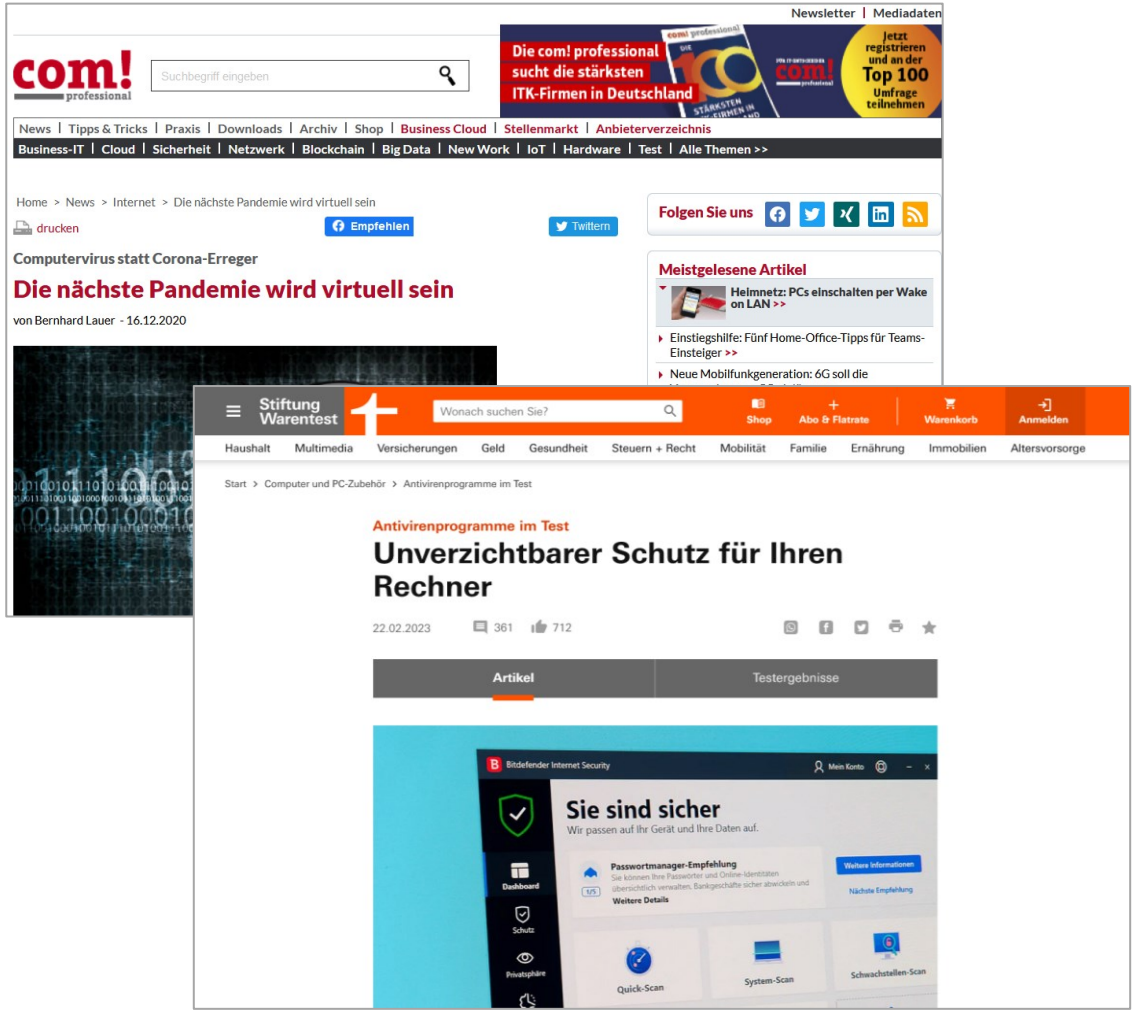
- Sichere Passwörter (https://bit.ly/3aNDlSF)
- Sicheres Passworthandling (Kenntnis, Aktualisierung, Speicherung, Zwei-Faktor-Authentifizierung, …)

Quelle: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Grippe im System – Gefahr durch Viren

Maßnahmen:

- Aktuellen Antivirensoftware einsetzen und updaten (https://www.test.de/Antivirenprogramme-im-Test-4993310-0/)
- Nicht ausschließlich auf „Online-Virenscanner“ verlassen !!!
- Firewall einsetzen/aktivieren (auch auf dem persönlichen Rechner)
- Mitarbeiter*innen sensibilisieren (öffnen von E-Mails, Downloads, …)



Verschlüsselung der Internetverbindung

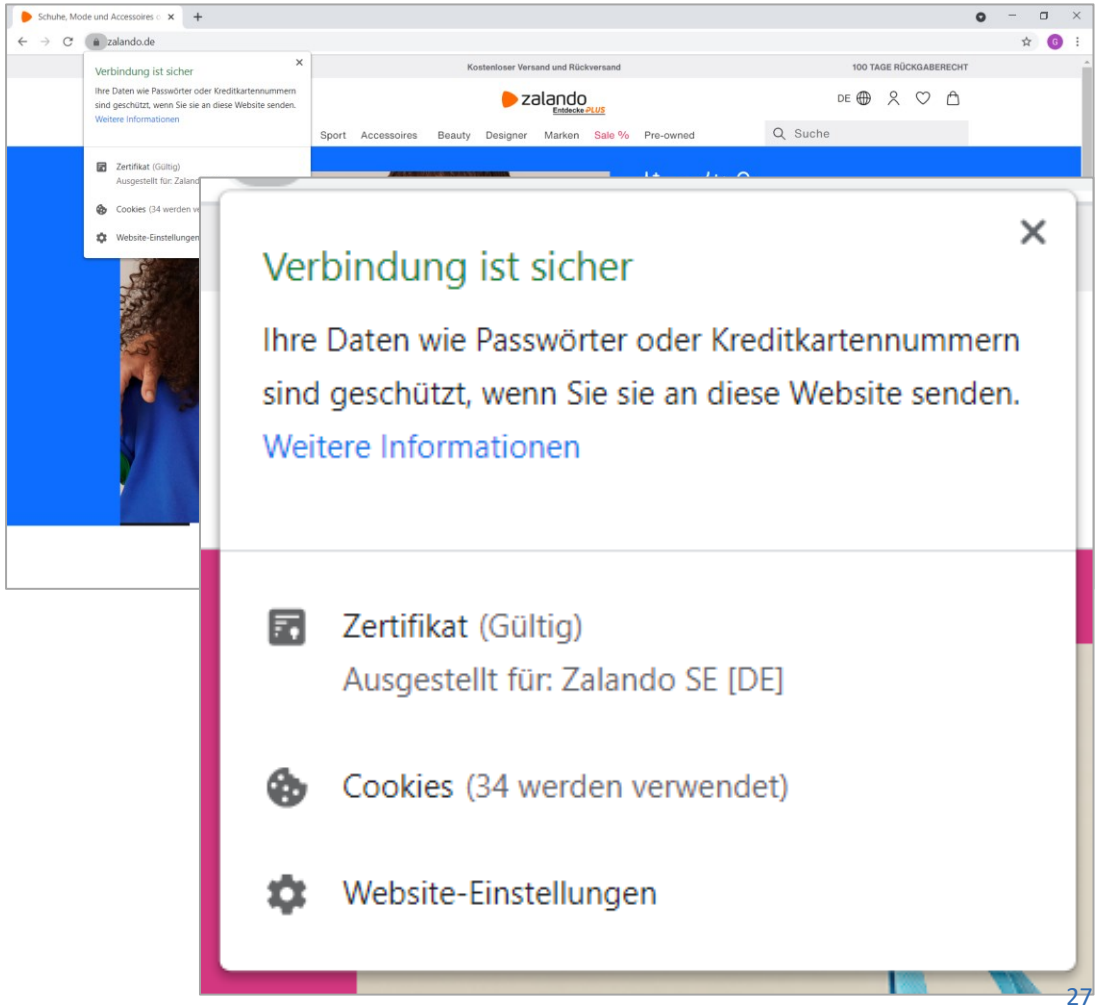
Rechtliche Vorgaben (insb. § 13 VII TMG)

- Für geschäftsmäßig angebotene Telemedien, worunter auch Online-Shops fallen, ist ein „als sicher anerkanntes Verschlüsselungs-verfahren“ → SSL-Verschlüsselungen für kommerzielle Webseiten
- Stand der Technik muss berücksichtigt werden → regelmäßige Aktualisierungen nötig

Usabilty- und Marketingaspekte

- Schutz-Aspekt und Verbrauchererwartung
- SSL-Verschlüsselung – von Google erwünscht (Ranking)
- Aufrufbarkeit durch Browser

Nicht vergessen: Geräte verschlüsseln!



Augen auf bei der Softwareauswahl – Software als Sicherheitslücke

IT-Sicherheitsaspekte bei der Auswahl mit einbeziehen – auch die IT-Sicherheit im Betrieb berücksichtigen

- IT-Sicherheit wird bei der Softwarebeschreibung thematisiert und belegt
  (Zertifikate, Auszeichnungen etc.)
- Fortlaufend Updates oder Patches werden angeboten, idealerweise kostenlos
- Nach Erfahrungen suchen (z. B. befreundete Händler, Dienstleister, Internet, Experten)

Stichwort Open Source-Programme: Nicht per se ablehnen, aber auf Integrität achten und Community prüfen

Top-10 der Shopsysteme in Deutschland und weltweit

	Deutschland*	Weltweit I*	Weltweit II*
Basis:	*Relevante Onlineshops*	*Relevante Onlineshops*	*Alexa Top 1 Million*
1	Shopware (28%)	Magento (29%)	Magento (24,6%)
2	Magento (23%)	Shopify (8%)	Woocommerce (19,8%)
3	Oxid Esales (9%)	Shopware (8%)	Opencart (7,4%)
4	JTL Shop (8%)	Salesforce Commerce Cloud (7%)	Prestashop (6,4%)
5	Plentymarkets (5%)	Woocommerce (5%)	Shopify (5,4%)
6	Oscommerce (3%)	Prestashop (5%)	Virtuemart (3,5%)
7	Woocommerce (3%)	Sap Hybris (3%)	Interspire***
8	Salesforce Commerce Cloud (3%)	Oxid Esales (3%)	Oscommerce
9	Shopgate (2%)	Opencart (2%)	Magento Enterprise
10	SAP Hybris (2%)	IBM Websphere (2%)	Big Commerce
11			Zen Cart
12			IBM Websphere
13			Volusion
14			Yahoo Stores
15			Ubercart

Quelle: https://efuchs.net/marktanteile-der-shopsysteme-in-deutschland/

Betrug und andere Risiken im Online-Handel

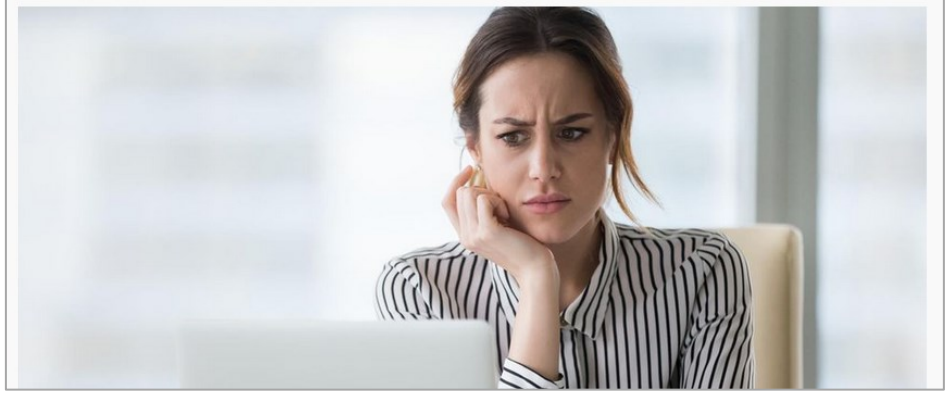
stern

Panorama Politik Kultur Lifestyle Digital Wirtschaft Sport Gesundheit Genuss Reise Familie Auto Gutscheine

Digital > Online > Betrug im Online-Handel nimmt während Corona zu – das sind die beiden wichtigsten Warnsignale

ABZOCKE

Betrug im Online-Handel nimmt während Corona zu: Das sind die beiden wichtigsten Warnsignale



ZDF Rubriken Barrierefrei Live-TV Sendung verpasst Suche

Zu viele Sicherheitslücken

Justiz bei Betrug im Onlinehandel überlastet

von Maja Helmer 02.12.2020 14:30 Uhr

Das Onlinegeschäft boomt. Damit wächst auch der Anteil der Bestellbetrugsdelikte. Das bringt die Strafverfolgungsbehörden an Grenzen. Sie kritisieren laxe Sicherheitsvorkehrungen.

Die Fälle von Onlinebetrug steigen, die Zahl der aufgeklärten Fälle sinkt.

Quelle: dpa

Betrug und andere Risiken im Online-Handel

Mögliche Anzeichen eines Betrugsversuchs

- Der Warenkorb kann einem Händler bereits erste Anzeichen dafür geben, ob ein möglicher Betrugsversuch im Gange ist (viele hochpreisige Artikel oder auch Waren mehrfach enthalten)
- Mehrfach wiederholte Bestellungen mit sehr ähnlichen Warenkörben in kurzer Zeit
- Plausibilitätsaspekte – Passt die E-Mail zum Namen des Bestellers? Ist die E-Mail sehr kryptisch? Auch der Aufbau der E-Mail-Adresse kann Aufschlüsse geben, sowie Auffälligkeiten in den Stammdaten (z.B. der Name Donald Duck oder die Altersangabe von 95 Jahren)
- Abweichende Lieferadresse – Adressen weichen sehr weit voneinander ab und die Bestellung geht an eine völlig andere Person
- Versand an Packstation (meist in Kombination mit Auffälligkeiten in den Stammdaten)
- Auffällige Bestellmuster – Warenkorb wird immer um einen Artikel erhöht, um das Limit auszutesten

Aus Sicht der Händler konzentriert sich Betrug mehrheitlich auf die Identitätsnutzung sowie den Versand

Identitäten

Identitätsdiebstahl

Account Take Over

Adressmanipulation
(Abänderung von Adressen, ähnliche Adressen, z.B. im Hochhaus)

Zahlungsmittelbetrug
(z.B. Kreditkartendaten)

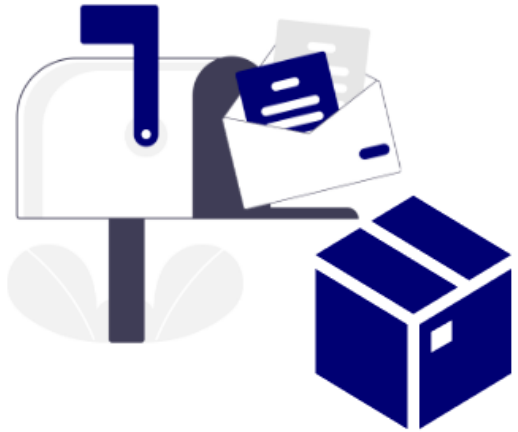
Versand

„Abfangen" der Pakete

Involvierte Paketzusteller/ Filialen

Packstationen

Versand in grenznahe Gebiete oder ins Ausland



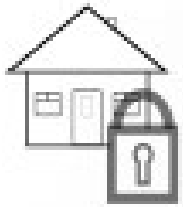
Quelle: IFH/SCHUFA 2020; https://www.schufa.de/media/documents/studien/IFH_Studie_Koeln_Fraud_Prevention_eCommerce_SCHUFA_Holding_AG.pdf

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

Bundesamt
für Sicherheit in der
Informationstechnik

Klar geregelt:

Kommunizieren Sie klare und verbindliche IT-Sicherheitsregelungen.



Hier gibt es nichts zu sehen:

Stellen Sie sicher, dass Unbefugte keinen Einblick in Ihre Daten haben.

Eindeutige Verifizierung:

Kommunizieren Sie nur über Kanäle, die vertrauenswürdig sind.

Vorsicht Phishing:

Durch COVID-19 können vermehrt Phishing-Mails im Umlauf sein.

VPN:

Kommunikation per VPN ist der Standard.
Informieren Sie sich über sichere Lösungen.

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

Tipps für sicheres mobiles Arbeiten (BSI)

1. Regelungen für Telearbeiter / Sicherheitsrichtlinie für die Telearbeit

2. Sensibilisierung der Telearbeiter

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

… kontinuierliche Sensibilisierung der Mitarbeiter

Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

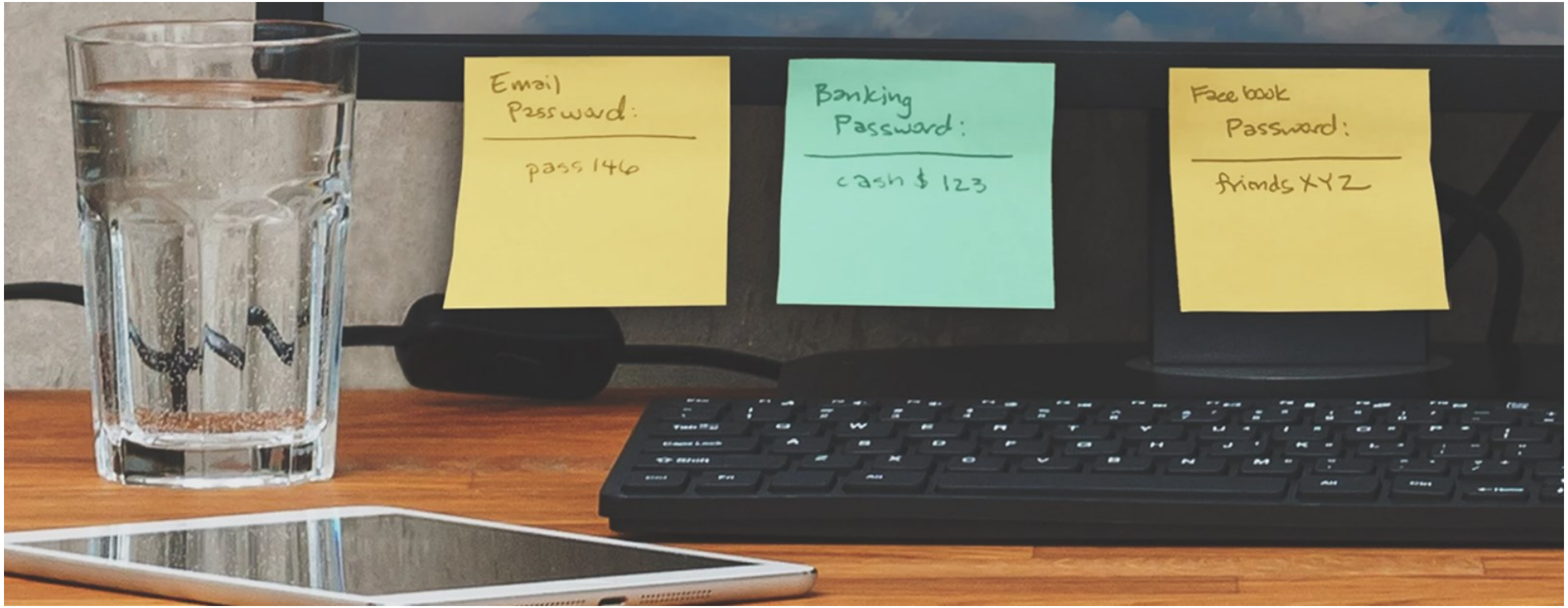
05 Tipps von Händlern für Händler

Einige Tipps aus Gesprächen mit Händlern

- Regelmäßige Backups aller relevanten Daten schützen vor üblen Konsequenzen wie Datenverlust. Diese lassen sich auch automatisieren.
- Software sollte angesichts immer neuer Gefahren immer auf dem neuesten Stand sein. Angebote mit Updates und Support sorgen vor.
- Genutzte Software sollte die Anforderungen der DSGVO erfüllen, nicht nur im Sinne der Kundschaft.
- Nutzen Sie ausgewählte Dienstleistungen zur Risikoreduktion (Payment-Absicherung, Risikomanagement, Betrugsprävention, …)
- Bei der Arbeit unterwegs, im Hotel im Urlaub, der Bahn etc. sollten besondere Vorkehrungen getroffen werden (bspw. geschütztes Wlan, VPN-Tunnel)
- Die Gefahr geht besonders im Internet nicht von einer einzelnen böse dreinschauenden Person mit Skimaske an einem Laptop aus, wie Stockfotos gerne vermitteln. Sie sollte durchaus ernst genommen werden.
- Mitarbeiter immer wieder auf die Gefahren hinweisen, sensibilisieren und kontinuierlich schulen. Auch immer wieder Hilfestellungen anbieten.
- Halten Sie sich über die Bedrohungen auf dem Laufenden und bilden Sie sich weiter!

Quelle: In Anlehnung an https://www.onlinehaendler-news.de/digital-tech/cyberkriminalitaet/132667-how-to-it-sicherheit-betreiber-online-shops

Eigenen Schweinehund besiegen!



Quelle

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

Startseite > Meine TISiM

Sec-O-Mat

Der Sec-O-Mat startet mit einer Befragung zu Bereichen Ihres Unternehmens, wo IT-Sicherheit eine Rolle spielt – wie Personalmanagement oder Logistik. Im Anschluss erhalten Sie Ihren TISiM-Aktionsplan mit konkreten Handlungsempfehlungen für Ihre IT-Sicherheit. So haben Sie Ihre IT-Sicherheit immer gut im Blick.

Sec-O-Mat

Schwachstellen aufdecken und Aktionsplan gestalten

TISiM-Aktionsplan

Unser Sec-O-Mat liefert Ihren passgenauen TISiM-Aktionsplan in wenigen Minuten. Sie erhalten eine Übersicht zu Ihren konkreten Sicherheitsbedarfen mit passenden Umsetzungsvorschlägen. Garantiert herstellerneurtal: Von kostenfreien Schulungen bis zu aufwändigeren IT-Sicherheitslösungen. Sie bestimmen, wo und wann Sie starten möchten. Ihr TISiM-Aktionsplan zeigt Ihnen Fortschritt über Ihre Aktivitäten.

Aktionsplan

Zusammenfassung des Webinars

- Geschäftsmodelle im Handel müssen an die veränderten Gegebenheiten angepasst werden – IT-Sicherheit darf dabei bitte nicht vergessen
- Das stationäre Ladengeschäft ist nach wie vor der dominierende Kanal, Online-Kanäle gewinnen immer mehr an Bedeutung – Multikanal ist die Zukunft!
- Digitalisierung findet nicht nur an der Kundenschnittstelle statt – interne Abläufe sind oft stärker betroffen und bieten mehr Potenzial – hier werden Sicherheitsthemen oft vernachlässigt
- Bei der „eiligen“ Umsetzung nicht die Sicherheit vernachlässigen
- Händlern – insbesondere kleinen und mittleren – fehlen oft Zeit und Ressourcen, um die erreichte Digitalisierung weiter sicher voranzutreiben – Standards und Dienstleister nutzen!
- Händler müssen selber für Veränderung bereit sein („Mindset“) – BWA im Auge behalten und weiter sensibilisieren und schulen
- Bei aktuelle Investitionen muss an die zukünftigen Bedürfnisse, Trends und insbesondere die IT-Sicherheit gedacht werden!

06 Vorhandene Hilfsangebote und Links

Hilfreiche Links und mehr

- Folge 69: IT-Sicherheit im Onlinehandel (https://digitalzentrumhandel.de/podcasts/)
- Checkliste IT-Sicherheit im Online-Handel (https://digitalzentrumhandel.de/wp-content/uploads/2021/12/it_check_kompetenzzentrum.pdf)
- Transferstelle IT-Sicherheit im Mittelstand (https://www.tisim.de/)
- Leitfaden zur Basis-Absicherung nach IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Leitfaden_Basisabsicherung/Leitfaden_Basisabsicherung_node.html)
- IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/grundschutz.html)
- IT-Grundschutz-Kompendium (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html)
- Online-Kurs zum IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/itgrundschutzschulung_node.html)
- Standard-Datenschutzmodell (https://www.datenschutzzentrum.de/sdm/)
- Basics für ein sicheres Netz (https://www.polizei-beratung.de)
- Polizei - Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen (https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html)
- …


Fragen?

Kommende Webinare

- 14.06.2023 | 08:30 Uhr | **Erfolgreich nachhaltig Handeln** –
  Wie sich Nachhaltigkeit im Handelsumfeld erfolgreich umsetzen lässt
- 20.06.2023 | 08:30 Uhr | **Einstieg in die Suchmaschinenoptimierung**
- 27.06.2023 | 08:30 Uhr | **Digitale Sichtbarkeit** – überlebenswichtig, aber kein Hexenwerk
- 04.07.2023 | 08:30 Uhr | **Was macht eine gute Website aus?**
- 11.07.2023 | 08:30 Uhr | **Kundenkommunikation im Multikanalvertrieb erfolgreich gestalten**
- 12.07.2023 | 08:30 Uhr | **E-Commerce im Mittelstand** – Erfolgsfaktoren digitaler Champions
- 13.07.2023 | 08:30 Uhr | **Die Kunden verstehen** – Wie ticken Verbraucher in Bayern?

und weitere: https://www.stmwi.bayern.de/erfolgreich-handeln/veranstaltungskalender

Über ibi research

- 1993 gegründet mit dem Ziel des Wissenstransfers in der Wirtschaftsinformatik zwischen Akademia und Praxis
- Angewandte Forschung und Beratung in der Digitalisierung zweier Bereiche: Finanzdienstleistungen sowie Handel
- Arbeit mit der Objektivität der Wissenschaft an den Anwendungen des Praktikers
- Partnernetz von über 40 großen und kleinen Unternehmen
- Ca. 20 Mitarbeiter vom erfahrenen Manager bis zum innovativen Doktoranden

Vielen Dank für Ihre Aufmerksamkeit!

ibi research an der Universität Regensburg GmbH

Galgenbergstr. 25

93053 Regensburg

Tel.: 0941 943-1901

Fax: 0941 943-1888

E-Mail: info@ibi.de

ERFOLGREICH HANDELN

Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie