
IHK MAGDEBURG
Digital, aber sicher –
auch der Tourismussektor ist im Blick der Cyberkriminellen

Von Anfang bis Ende – immer mehr läuft digital

Inspiration

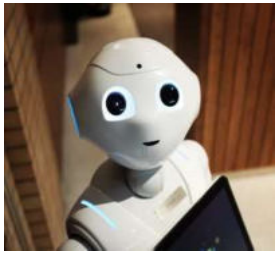
Buchung

Zufriedenheit

Recherche

Erlebnis

…es entstehen an allen Ecken neue Anforderungen …



Fachkräfte

- ✓ Recruiting
- ✓ Digitale Arbeitskräfte
- ✓ Arbeitswelt 4.0
- ✓ ….

Gesetze / E-Government

- ✓ Digitale Verwaltung/OZG
- ✓ Digitale Arbeitszeiterfassung
- ✓ OpenData
- ✓ …

Digitale Schnittstellen

- ✓ Payment
- ✓ Kooperationspartner
- ✓ Service- und Wartung
- ✓ ...

Neue Entwicklungen

- ✓ Smart Home
- ✓ Augmented Reality
- ✓ Künstliche Intelligenz
- ✓ …

Offen für die digitale Zukunft ….

- **94%** Chancen der Digitalisierung
- **75%** Vorteile bei Flexibilisierung von Prozessen/Workflows (2021: 51%)
- **43%** Kostensenkung sowie Kundenanforderungen als Treiber
- **26%** neue Dienstleistungen, Produkte oder Geschäftsmodelle

3,1 **Schulnote (Gesamtwirtschaft: 2,9)**

Herausforderungen verlangsamen digitale Transformation

- **37%** erheblicher Zeitmangel (bisher Platz 2)
- **34%** hohe Kosten und Komplexität
- **28%** fehlende Akzeptanz bei Mitarbeitern
- **75%** technische Maßnahmen für IT-Schutz im Einsatz
- **30%** organisatorische Maßnahmen für IT-Schutz getroffen

Risiken durch Digitalisierung und Vernetzung

2023: Angriff auf Nobelrestaurant: Webseite zeigt jetzt Speisekarte und Fotos einer Fastfoodkette

04.01.2023

Nach Cyberangriff auf H-Hotels:

Cyberkriminelle bieten entwendete Daten im Darknet an

Schon wieder Hacker-Angriff auf Marriott

07. Juli 2022 10:43 Uhr | Hotellerie

2023: Cyberangriff auf Heidelberger Lokal: Es werden an Kunden und Nichtkunden Zahlungsaufforderungen per E-Mails versandt - sowohl im Inland und Ausland

9 von 10 Unternehmen werden Opfer

- **68%** geben an, dass Daten (E-Mails, Kunden- und Zugangsdaten) entwendet wurden
- **34%** können erst nach 3 Tagen den "Normalbetrieb" aufnehmen (15 % nach 7 Tagen)
- **45%** sind nach einer Cyberattacke in der Existenz gefährdet ist
- **Cyberangriffe durch:**
  - **25 %** Diebstahl von Passwörtern (2021: 21 %)
  - **25 %** Phishing (2021: 18 %)
  - **14 %** Cross-Site-Scripting (2021: 9%)
  - **48 %** Versuche von Social Engineering (2021: 41%)

Umfrage Bitkom zum Wirtschaftsschutz im Jahr 2022

Passwörter – ein wichtiger Beitrag für mehr Schutz

Unsicher, aber seit Jahren beliebt!

123456 123456789 passwort

qwertz qwertz111 1111111111

Im Jahr 2022 in die TOP 10 gerückt:

1qay2wsx3edc

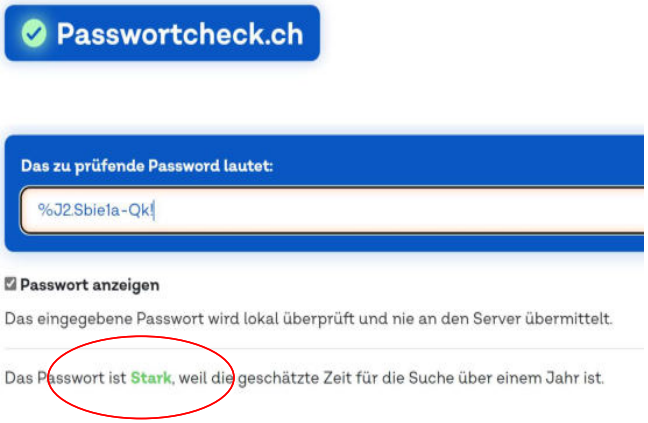
Sichere Passwörter verwenden

- Lange Passwörter
- Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen
- Sonderzeichen nicht nur am Anfang und Ende
- Keine Namen, Wörter, Muster (Tastatur)

TIPP **Passwort aus Satz ableiten**

Jeden **2. S**onntag **b**acke **i**ch **e**inen **1a-K**äse**k**uchen!

%J2.Sbie1a-Qk!



Umgang mit Passwörtern

- Sperren bei Verlassen des Arbeitsplatzes
- Passwörter nicht weitergeben oder notieren
- Mehrfaktorauthentifizierung
- Regelmäßiger Wechsel, keine Mehrfachverwendung zulassen
- Auch Tablets und Smartphones schützen

TIPP **Passwortmanager einführen**
z. Bsp. Keepass

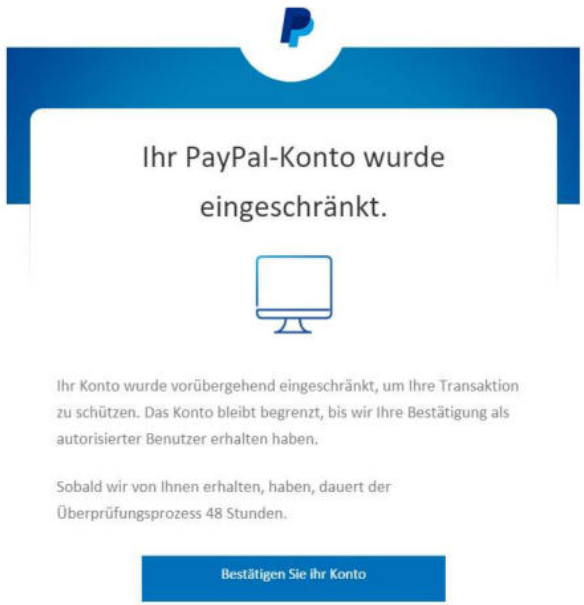
regelmäßig E-Mailadressen überprüfen
kostenfrei über Hasso-Plattner-Institut Potsdam möglich (https://sec.hpi.de)

TOP 5 der Bedrohungen

1. Einschleusen von Schadsoftware über externe Geräte
2. Infektion mit Schadsoftware über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage
4. Einbruch über Fernwartungszugänge
5. Social Engineering und Phishing

TIPP **Mitarbeiter regelmäßig schulen und sensibilisieren!**

Phishingsmail



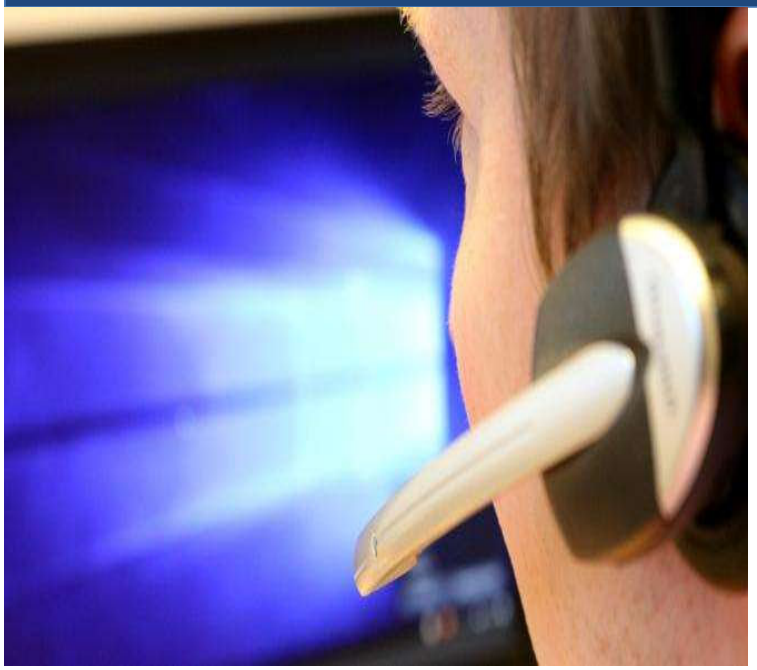
E-Mail sieht glaubwürdig aus, aber es gibt Hinweise…

1. unpersönliche E-Mail (ohne Anrede)
2. Schreibfehler im Text
3. Keine Nennung des Grundes für die Einschränkung vorhanden
4. Aufforderung zu Aktivitäten (meist mit Zeitdruck)

⇒ Link führt zur Unterseite: www.paipalll.com

⇒ Unterseite führt dann zur Betrugsseite www.paypal-anmelden.com (richtig: www.paypal.com)

Social Engineering



Aktuelle Warnung:

Mitarbeiter des technischen Supports von Microsoft versuchen per Telefon oder aufgrund von Warnungen auf dem Bildschirm, Zugriff auf Ihren Rechner zu erlangen.

Wenn keine sofortige Reaktion oder Problemlösung erfolge, könnte ein Virus das System lahmlegen.

Hinweis: Microsoft hat seit 2017 keinen telefonischen Support mehr!

Vorbereitung für den Notfall treffen!

- **Erstellen Sie einen betrieblichen Notfallplan**: Halten Sie alle notwendigen Maßnahmen im Ernstfall fest. Lassen Sie sich hier von Experten unterstützen.

- **Bestimmen Sie einen IT-Sicherheitsbeauftragten:** Ernennen Sie einen Verantwortlichen aus dem Betrieb, der sich mit den gängigen Sicherheitsfragen beschäftigt.

- **Unterziehen Sie den Notfallplan einem Test in der Praxis**.

- **Informationen bei:** IHK Magdeburg, Mittelstand-Digital-Zentren, Allianz für Cybersicherheit, Bundesamt für Sicherheit in der Informationstechnik

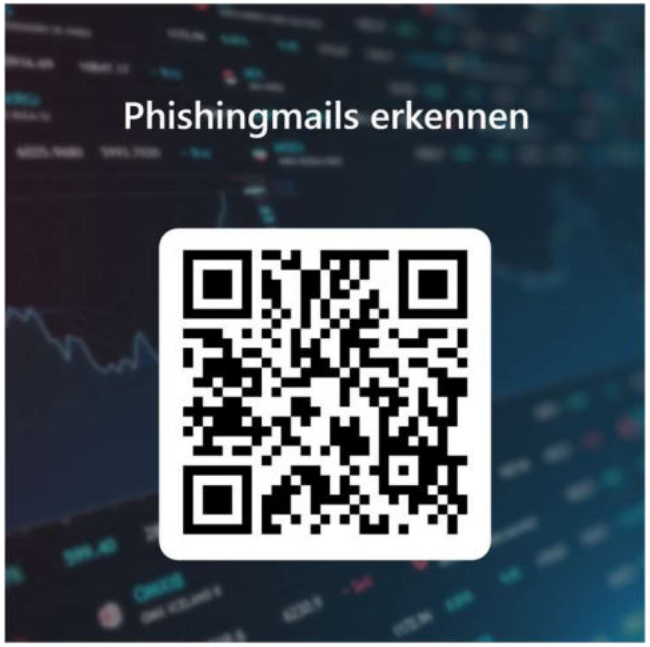
Kontaktdaten

Annett Gröger-Rost
Referentin für Digitalisierung und Innovation
Telefon: 0391 5693 154
E-Mail: annett.groeger-rost@magdeburg.ihk.de

Ksenia Backert
Referentin für Tourismus und Dienstleistung
Telefon: 0391 5693 132
E-Mail: ksenia.backert@magdeburg.ihk.de

IHK Magdeburg I Alter Markt 8 I 39104 Magdeburg I www.ihk.de/magdeburg

Ein kleiner Test gefällig?



Stellen Sie sich vor:

Sie heißen Max Müller und Ihre E-Mail lautet 'max.mueller.1973@web.de‘.

Sie erwarten ein wichtiges Paket.

Ist die Information des Paketdienstleisters echt oder nicht?

https://forms.office.com/e/pzgxgfAccP