12. November 2025


Unser Thema heute

# Cybersicherheit – Wie schütze ich meinen Betrieb online?

TOURISMUSNETZWERK BRANDENBURG

teejit

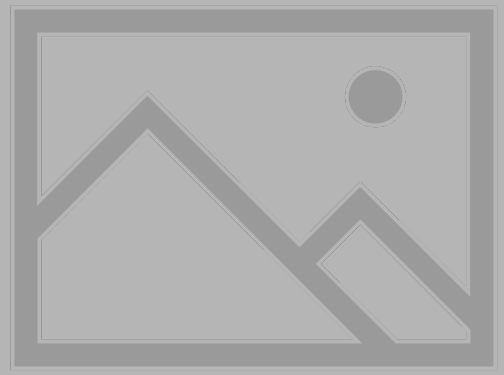
# Teejit GmbH


## Christoph Paul

**Head of Content**

**E-Mail: christoph@teejit.de**

**Phone: +491713286837**



# DAS TEAM

Unser Team vereinigt Medien- und IT Kompetenz mit langjähriger Tourismusexpertise. Wir verstehen Ihre Anliegen!

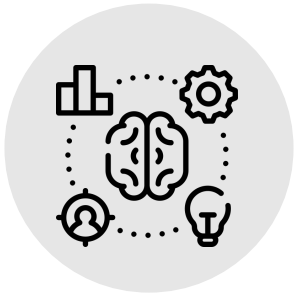
# UNSER ANSATZ

## AGENDA

Strategie

Data & Survey

Trends



## BILDUNG

Lernreihen

Multiple Formate

Operative Verknüpfung

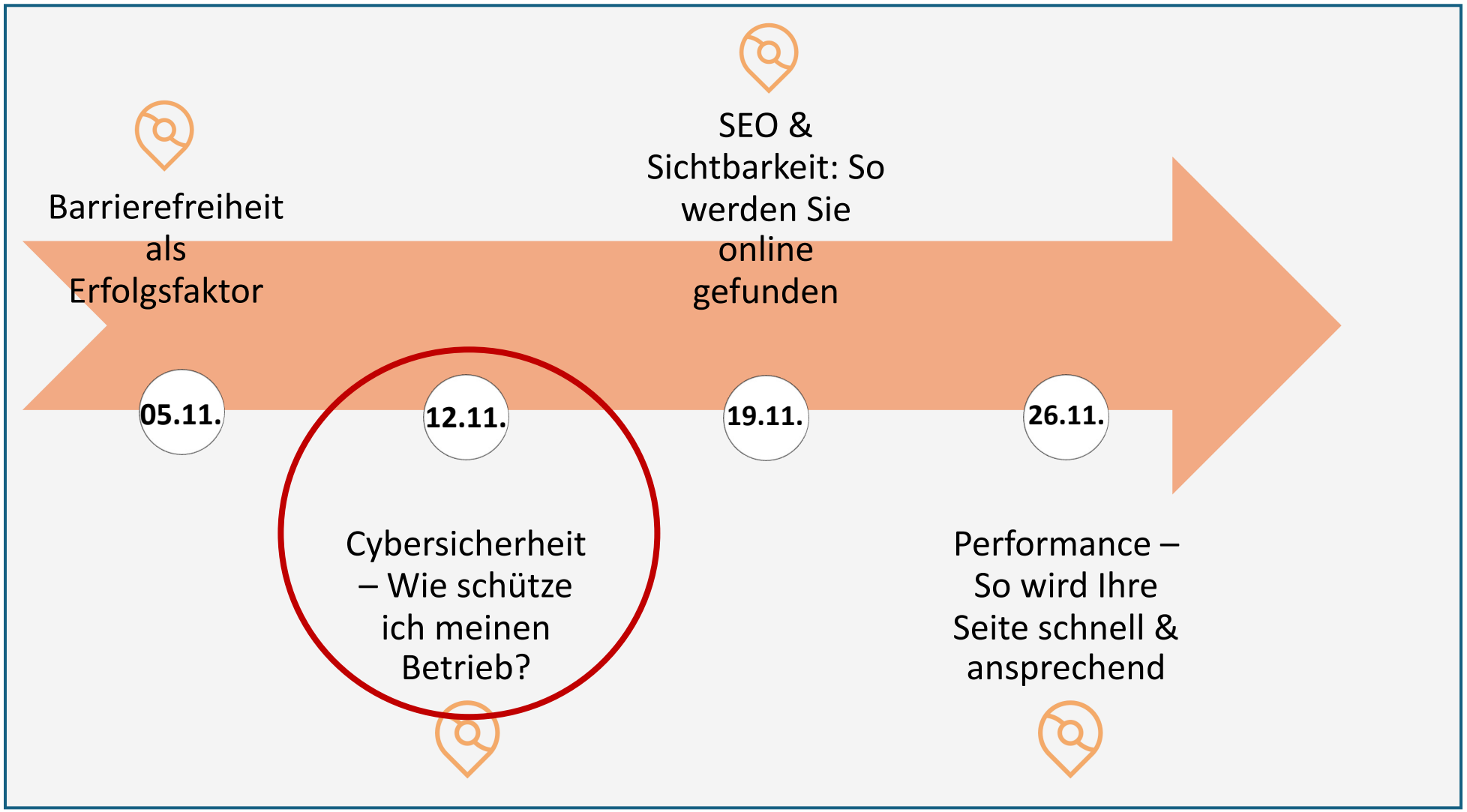
## NETZWERKE

Identifikation

Kollaboration

Multiplikation

# UNSERE WEBSEITEN-THEMENREIHE



# Unser Webinar heute: Cybersicherheit

**Einstieg**

Aktuelle Bedrohungen und Arten

**Phishing**

Einer der größten Risikofaktoren

**SPF, DKIM, DMAR, HTTPS & SSL**

Viele Begriffe, gute Übersicht

**Google Fonts, Rechtliches und Alltagsroutinen**

Wir runden unser Gelerntes ab

# Cybersicherheit

Ein Einstieg

# Teejit GmbH


## Christoph Paul

**Head of Content**

**Email: christoph@teejit.de**

**Phone: +491713286837**

VOL. 10, NO. 4 ✳ BREAKING NEWS ✳ 12. NOVEMBER 2025

# NACHRICHTEN

## CYBERANGRIFF LEGT DEUTSCHES HOTEL LAHM – GÄSTE KÖNNEN NICHT EINCHECKEN


### RESERVIERUNGS-SYSTEM TAGELANG OFFLINE – WEBSEITE NICHT ERREICHBAR

Cyberangriffe treffen inzwischen vor allem kleine und mittlere Unternehmen. Laut Bitkom entstehen in Deutschland jährlich Schäden in Milliardenhöhe.

### HACKER FORDERN LÖSEGELD FÜR FREIGABE SENSIBLER DATEN

Nach einem Cyberangriff wurden Kundendaten des Betriebs verschlüsselt und teilweise kopiert. Die Täter verlangen ein Lösegeld, um die Daten wieder freizugeben. Der Betrieb arbeitet mit IT-Forensikern und Datenschutzbehörden zusammen, um den Schaden zu begrenzen.

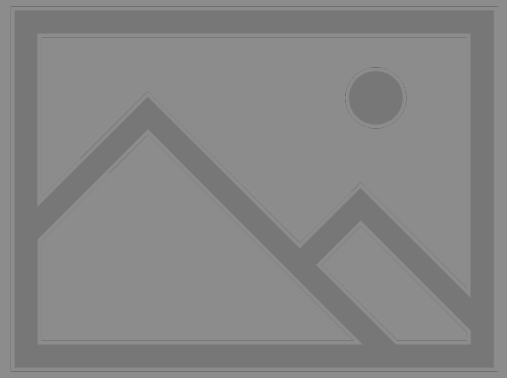
# Business Woche News

NEWS

Auf der Website eines touristischen Betriebs wurden nach einem Angriff unbemerkt Kontaktinformationen verändert. Statt der echten Telefonnummer führte der Link zu einer betrügerischen Seite, die Kreditkartendaten abfragte.
Der Betrieb bemerkte den Angriff erst nach Kundenbeschwerden. Der Fall zeigt: Cyberangriffe müssen nicht immer Systeme lahmlegen – oft reichen kleine Manipulationen, um großen Schaden anzurichten.

# Was steckt dahinter?

- 70 % aller Cyberangriffe richten sich gegen kleine und mittlere Unternehmen (Bitkom 2024).
- Angriffe sind meist automatisiert, keine gezielte Attacke.
- Folgen: Website offline, Kundendaten verloren, Imageschaden, Kosten.
- Jeder Betrieb mit Online-Präsenz kann Ziel sein.



KI-generiert

# Cyberangriffe sind vielfältig

| Art des Angriffs / Akteurs | Wie es passiert | Was das im Alltag bedeutet | Beispiel aus der Praxis |
|---|---|---|---|
| **Automatisierte Angriffe** | Bots durchsuchen das Internet nach offenen Ports, schwachen Passwörtern oder veralteten Plugins | Betriebe werden zufällig getroffen – oft ohne direktes Ziel | **2023: WordPress-Massenscan** – Zehntausende Websites automatisch kompromittiert, weil ein veraltetes Plugin offen war. Ein Angriff, der in Sekunden auch kleine Betriebe treffen kann. (Heise / Wordfence) |
| **Cyberkriminelle Gruppen** | Organisierte Angriffe zur Erpressung oder zum Datendiebstahl, meist mit Schadsoftware (Ransomware) | Systeme blockiert, Daten verschlüsselt, Lösegeldforderung in Kryptowährung | **2021: Nordic Choice Hotels** – Ransomware legte Check-in- und Buchungssysteme lahm. Gäste konnten nicht einchecken, Mitarbeitende arbeiteten vorübergehend mit Stift und Papier. (Visma) |
| **Angriffe über Dritte (Supply Chain)** | Kompromittierte Dienstleister oder Schnittstellen schleusen Schadcode ein | Eigene Website oder Buchungssystem fällt aus, obwohl der Angriff extern stattfand | **2023: MOVEit-Hack** – Eine Sicherheitslücke in der Dateiübertragungssoftware führte zu Datenlecks bei über 2 000 Organisationen. Viele Firmen bemerkten den Angriff erst, als Kundendaten bereits kursierten. (Hadrian / Wikipedia) |
| **Menschlicher Faktor & soziale Manipulation** | Angreifer nutzen Vertrauen, Routine oder Stress – z. B. durch Phishing-Mails, Social Media oder organisatorische Versäumnisse | Mitarbeitende oder Verantwortliche handeln unbewusst riskant, geben Daten frei oder übersehen Sicherheitslücken | **2022: Uber** – Ein Hacker täuschte einen Mitarbeitenden mit einer gefälschten Multi-Faktor-Nachricht. Über den internen Zugriff gelangte er in zentrale Systeme und veröffentlichte interne Chats und Code. (Axios / BBC) |

# Typische Angriffspunkte

Das Bild wurde mit KI erstellt.

| Bereich | Was passiert dort? | Warum gefährlich? |
|---|---|---|
| **Website** | Austausch von Nutzerdaten (Formulare, Buchungen, Cookies) | Offene oder veraltete Plugins können Schwachstellen enthalten. |
| **E-Mail** | Kommunikation mit Kunden, Lieferanten, Agenturen | Mails können gefälscht werden (Phishing, Spoofing). |
| **Online-Zahlung / Buchungssysteme** | Schnittstellen zu Zahlungsdiensten oder Buchungsportalen | Daten fließen über Drittanbieter – Angriffe auf die Schnittstelle möglich. |
| **Cloud-Dienste / Backups** | Speicherung externer Daten | Angreifer zielen auf Zugriffsdaten oder schlecht gesicherte Freigaben. |
| **Mitarbeitende / Social Engineering** | Menschliche Interaktion (Anhänge, Links, Passwörter) | Falsche Mails oder Anrufe tricksen Menschen aus – kein technischer Hack nötig. |

# Die Entwicklung

- > 200 000 Fälle von Cybercrime in Deutschland,weitere ~ 130 000 Täter im Ausland.
- Rund 90 % Dunkelfeld – die meisten Vorfälle bleiben unentdeckt oder werden nicht gemeldet.
- 178,6 Mrd. € wirtschaftlicher Schaden durch Cyberattacken (2024), 2023 waren es 148,2 Mrd. €.
- 950 Ransomware-Angriffe zur Anzeige gebracht, Erpressungssummen teils über 1 Mio. US-$.
- 29 399 DDoS-Angriffe auf deutsche Ziele, rund 30 % mehr als im Vorjahr.
- 400 000 Phishing-Mails allein in Nordrhein-Westfalen gemeldet

Quelle: Bundeskriminalamt (2024): Bundeslagebild Cybercrime – Berichtsjahr 2024. Infografik:

KI-generiert

# Phishing

....

Einer der größten Risikofaktoren

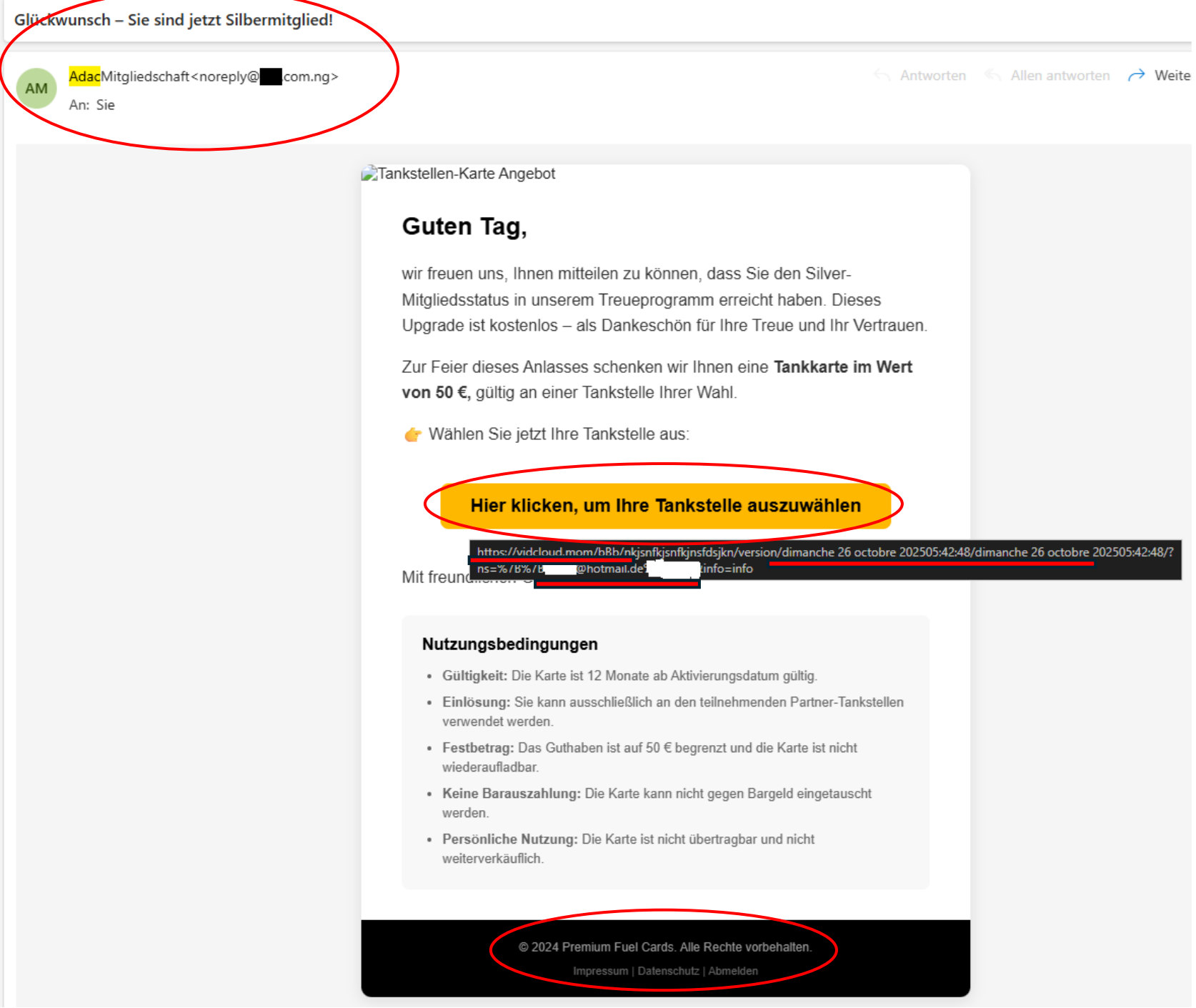
KI-generiert

# Was steckt dahinter?

- **Digitale Täuschung** über E-Mail, SMS oder soziale Netzwerke.
- **Ziel:** Klicks, Anhänge oder Logins, um Daten oder Zugänge zu stehlen.
- Angreifer setzen auf Vertrauen, Routine und Zeitdruck – nicht auf Technik.
- **Kritisch:** private Kommunikation am Arbeitsplatz öffnet oft unbemerkt das Tor ins Unternehmensnetz.
- Rund 1,2 % aller E-Mails sind Phishing-Versuche (Keepnet Labs 2025) – mehr als 3 Milliarden täglich.
- Weil der Angriff über **echte Kanäle** läuft, greifen Filter zu spät – Wachsamkeit ist der wirksamste Schutz.



KI-generiert




- Absendername passt, **Mailadresse** aber nicht (z. B. „ADAC“ → endet auf .ng).
- **Unerwartetes Geschenk** oder „Bonus“ ohne Anlass.
- **Dringender Ton** oder Zeitdruck („Jetzt aktivieren“).
- **Linkziel passt nicht** zur Marke (Maus drüberhalten: fremde Domain).
- **Eigene Mailadresse** steckt im Link – Hinweis auf personalisierte Phishing-Seite.
- **Impressum/Datenschutz-Links** führen ins Leere oder sind Platzhalter.

# In die Falle getappt?

-**Zwei E-Mail-Adressen nutzen** – eine für Kommunikation, eine für Newsletter.

-**Browser-Addons aktivieren**: uBlock Origin, Privacy Badger.

-**Verdächtige Links** mit VirusTotal oder Google Safe Browsing prüfen.

-**Mailvorschau und automatische Bilderanzeige ausschalten** – so werden verdächtige Inhalte nicht automatisch geladen.

-**Als Phishing oder Spam markieren** – verbessert die Filter.

-**PAUSE-Regel merken**: Prüfen, Ansehen, Umgehen, Sichern, Erledigen.

**Ruhe bewahren** – kein Grund zur Panik, aber schnell reagieren.

**Internetverbindung trennen**, falls eine Datei geöffnet wurde.

**Kennwörter sofort ändern**, beginnend mit E-Mail- und Bankkonten.

**Zwei-Faktor-Authentifizierung aktivieren**, falls noch nicht aktiv.

**System prüfen:** Virenscan mit aktueller Sicherheitssoftware durchführen.

**Mail und Link an IT oder Provider melden**, um Filter zu verbessern.

**Verdächtige Zahlung oder Datenweitergabe**? → Bank und ggf. Polizei informieren.

**haveibeenpwned.com**

**How secure is my password**

**KI-generiert**

# SPF, DKIM & DMARC

....

Ihre Internet-Türsteher

KI-generiert

# Wo sind Ihre E-Mail-Türsteher?

*Stellen Sie sich vor, jemand steht vor Ihrer Haustür, trägt Ihre Kleidung, kennt Ihren Namen und behauptet, Sie zu sein – und geht dann mit Ihrer Identität beim Nachbarn klingeln, um Daten zu sammeln und andere über das Ohr zu hauen.*

- **SPF prüft, wer überhaupt rein darf** – nur eingetragene Absender dürfen in Ihrem Namen Mails senden.
- **DKIM versieht jede Mail mit einem digitalen Siegel**, das zeigt: „Diese Nachricht wurde unterwegs nicht verändert."
- **DMARC kontrolliert, ob beide Regeln eingehalten wurden** – und sortiert Fälschungen automatisch aus.

MXToolbox SPF-Check

# SPF, DKIM & DMARC – Ihre E-Mail-Türsteher

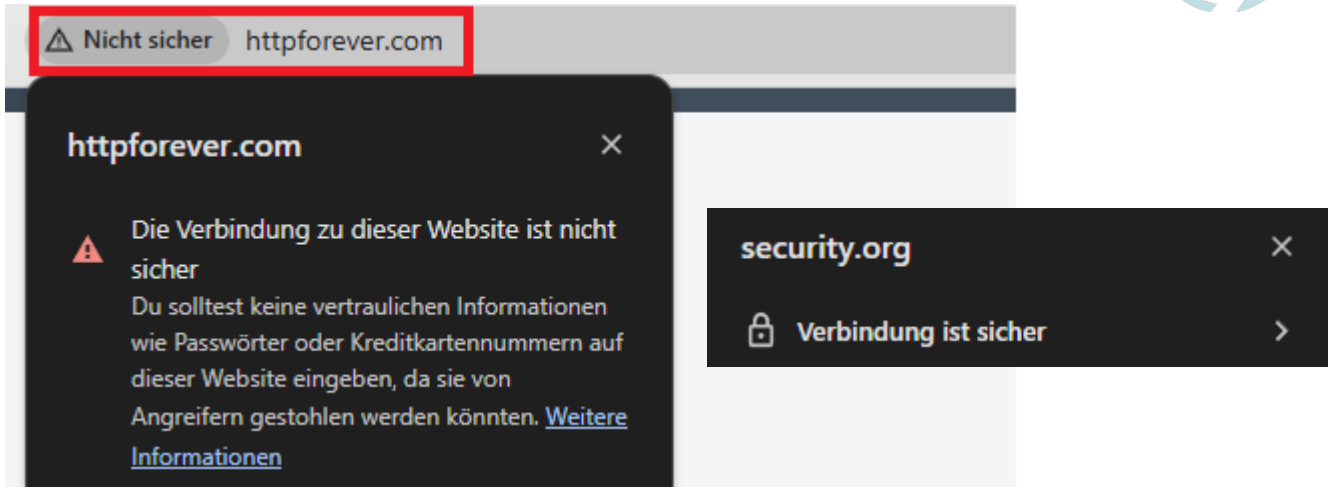
| Kriterium | Typische Meldung bei MXToolbox | Bedeutung | Nächster Schritt |
|---|---|---|---|
| **SPF**<br>*Sender Policy Framework* | No SPF record found / SPF fail | Legt fest, **welche Server berechtigt sind**, E-Mails im Namen Ihrer Domain zu versenden. Ohne SPF kann **jede fremde IP-Adresse** Mails mit Ihrer Domain verschicken. | Domain- oder E-Mail-Anbieter kontaktieren und SPF-Eintrag einrichten (Standardfunktion bei allen Hostern). |
| **DKIM**<br>*DomainKeys Identified Mail* | No DKIM record found / DKIM fail | Fügt E-Mails eine **digitale Signatur** hinzu. Damit wird geprüft, ob Nachrichten **unterwegs verändert** wurden. Ohne DKIM bleibt Manipulation unbemerkt. | Beim Mailanbieter prüfen, ob DKIM aktiviert ist.<br>Falls nicht: Support fragen, wie man die Signatur einschaltet. |
| **DMARC**<br>*Domain-based Message Authentication, Reporting & Conformance* | No DMARC record found❌<br>DMARC Policy Not Enabled ⚠️ | DMARC **verknüpft SPF und DKIM** und legt fest, **was mit verdächtigen Mails passiert**. – **No DMARC record:** kein Schutz, keine Kontrolle.<br>**Policy Not Enabled:** Überwachung aktiv, aber **keine Abwehrmaßnahme** – Mails werden nicht blockiert. | Provider oder IT bitten, einen DMARC-Eintrag zu setzen.<br>Wenn vorhanden, Policy auf **„quarantine“ oder „reject“** stellen, sobald SPF & DKIM stabil laufen. |

# HTTPS und SSL-Zertifikat

Website verschlüsseln

KI-generiert

# Das bekannte Warnsymbol im Browser




- Das Schloss-Symbol in der Browserzeile zeigt, ob eine Website verschlüsselt ist.
- Fehlt es, bedeutet das: Daten können mitgelesen oder verändert werden – etwa bei Kontaktformularen oder Loginfeldern.
- Manchmal erscheint die Warnung auch dann, wenn **Teile der Seite** (z. B. Bilder, Schriftarten oder eingebettete Karten) **nicht sicher eingebunden** sind.

## Wenn Sie so eine Seite sehen

- Keine Formulare ausfüllen und keine persönlichen Daten eingeben.
- Keine Zahlungen oder Logins initiieren.
- Seite schließen oder die Adresse manuell mit „https://“ neu laden.

## Wenn es Ihre eigene Website betrifft

- Prüfen, ob das SSL-Zertifikat aktiv ist (bei Ihrem Hosting-Anbieter oder Webdesigner nachfragen).
- Wenn das Schloss trotzdem fehlt: liegt oft an unsicheren Elementen auf der Seite – z. B. ein Bild, das über http:// eingebunden ist.
- Agentur oder Webdesigner bitten, alle Inhalte über https:// zu laden – besonders Fonts, Karten, Bilder.

*Stellen Sie sich vor, Sie schicken eine Postkarte – jeder auf dem Weg kann sie lesen.Mit SSL wird daraus ein verschlossener Umschlag: Nur Empfänger und Absender wissen, was drinsteht.*

http://httpforever.com/ https://webbkoll.5july.net/de/

**Mit KI erstellt.**

# Google Fonts

....

*Stellen Sie sich vor, Sie gestalten ein wunderschönes Schaufenster, um Passanten anzulocken – und merken nicht, dass bei jeder Interaktion auch jemand Fremdes durchs Fenster schaut, der beobachtet, wer vorbeikommt, wie lange und was ihm gefällt.*

*So elegant Google Fonts wirken, so neugierig sind sie mitunter auf die Daten dahinter.*

KI-generiert

# Was steckt dahinter?

- Viele Websites laden Inhalte von externen Servern, z. B. von Google.
- Google Fonts werden dabei automatisch nachgeladen – meist unbemerkt.
- Es gibt keine Warnung, doch im Hintergrund fließen Daten oft ohne Zustimmung in die USA.
- Früher Standard, heute datenschutzrechtlich riskant (Abmahnung möglich).
- Lösung: Schriften lokal speichern, statt sie extern zu laden.
- URL

KI-generiert

# Wie prüfen wir das?

**Browser-Check** 🕵️

- Eigene Website öffnen
- Rechtsklick → Untersuchen (DevTools)
- Reiter Network → Suchfeld fonts.googleapis
- Wenn Treffer erscheinen → Fonts werden extern von Google geladen

**Alternativ** 💡

- http://google-fonts-checker.dataskydd.net/
- webbkoll.dataskydd.net
- → zeigen externe Schriftquellen auf einen Blick

**Backend-Check** ⚙️

- Im CMS (z. B. WordPress, Jimdo, Typo3) unter *Design / Schriftarten* nachsehen
- Wenn dort ein Link mit https://fonts.googleapis.com/ steht → betroffen

**Wenn betroffen** 🚨

- In WordPress: Plugin **OMGF** aktivieren (lädt Fonts lokal)
- Sonst: Webdesigner oder Agentur bitten, Schriften lokal zu speichern
- Danach: Website neu prüfen – keine Verbindungen mehr zu fonts.googleapis.com

# Rechtliche Grundlagen

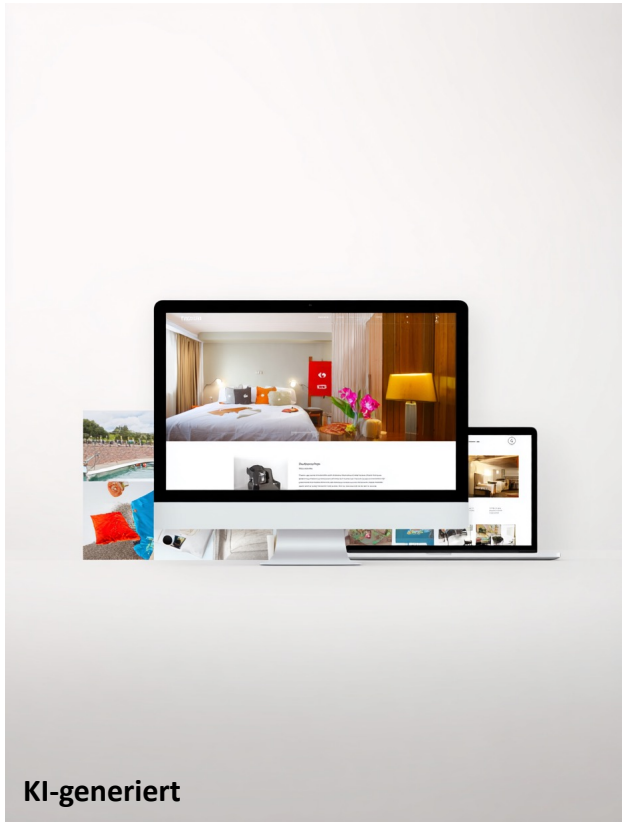
Cybersicherheit ist auch reglementiert

KI-generiert

# Rechtssicherheit ist vielfältig

| | |
|---|---|
| IT-Sicherheitsgesetz 2.0 | • nationale Vorgaben für technische und organisatorische Schutzmaßnahmen |
| NIS-2-Richtlinie (EU) | • europaweiter Rahmen für Mindeststandards und Meldepflichten bei IT-Vorfällen |
| DSGVO (Datenschutz-Grundverordnung) | • regelt den Umgang mit personenbezogenen Daten und Informationspflichten |
| Impressumspflicht | • sorgt für Transparenz: Verantwortliche und Kontaktdaten müssen öffentlich genannt werden |
| Datenschutzerklärung | • informiert Nutzer, welche Daten verarbeitet werden und zu welchem Zweck |
| Auftragsverarbeitungsvertrag (AVV) | • verpflichtet externe Dienstleister (z. B. Hoster, Newsletter-Tools) zur Einhaltung der Datenschutzregeln |

*Rechtslagen ändern sich kontinuierlich! Diese Übersicht und die nachfolgenden Inhalte erheben keinen Anspruch auf Vollständigkeit und ersetzen keine Rechtsberatung.*




| Gesetz / Richtlinie | Ziel | Relevanz & Umsetzung für Ihre Website / Ihren Betrieb |
|---|---|---|
| **IT-Sicherheitsgesetz 2.0 (Deutschland)** | Digitale Systeme widerstandsfähiger machen – Schutz vor Angriffen, Datenverlust und Ausfällen | • Fördert sicheres technisches Grundniveau in Unternehmen<br>• Grundlage für verschlüsselte Verbindungen (**HTTPS**) und aktuelle Systeme<br>• Bedeutet: **regelmäßige Updates, Backups und sichere Passwörter**<br>• Betriebe sollten mit ihrem **Hoster oder ihrer Agentur** Sicherheitsstandards klären (z. B. Firewall, Monitoring, DDoS-Schutz) |
| **NIS-2-Richtlinie (EU)** | Einheitliches Sicherheitsniveau und klare Verantwortlichkeiten in ganz Europa schaffen | • Gilt europaweit und bezieht auch **kleinere Betriebe über Dienstleister** mit ein<br>• Verlangt ein grundlegendes **Risikomanagement** und klare Zuständigkeiten<br>• Wichtig: **Verantwortliche Person für IT-Sicherheit** im Betrieb benennen<br>• Zusammenarbeit mit **externer IT oder Hosting-Anbietern** auf Sicherheitsmaßnahmen prüfen |

# IT-Sicherheitsgesetz 2.0 & NIS-2-Richtlinie

# DSGVO & Auftragsverarbeitungsverträge

KI-generiert

| Rechtsgrundlage | Ziel | Relevanz für Ihre Website / Ihren Betrieb |
|---|---|---|
| **DSGVO – Datenschutz-Grundverordnung (EU)** | Schutz personenbezogener Daten und Transparenz für Nutzerinnen und Nutzer | Betrifft jede Website, die mit **Kunden- oder Gästedaten** arbeitet – etwa bei Formularen, Buchungen oder Newsletter-Anmeldungen. Besucher müssen nachvollziehen können, **welche Daten verarbeitet werden und wofür**. (Umsetzung: aktuelle Datenschutzerklärung, klare Cookie-Hinweise) |
| **Auftragsverarbeitungsvertrag (AVV)** | Sicherstellen, dass externe Dienstleister DSGVO-konform handeln | Relevant bei allen **externen Diensten**, die Daten speichern oder verarbeiten – z. B. Hosting, Buchungssysteme oder Newsletter-Anbieter.<br>Der Betrieb bleibt verantwortlich, muss aber per Vertrag festlegen, **dass der Dienstleister Datenschutz einhält**. (Abschluss meist direkt im Kundenkonto möglich) |

# Impressum & Datenschutzerklärung



| Pflichtseite | Ziel | Relevanz für Ihre Website / Ihren Betrieb | Hilfreiche Generatoren / Tools |
|---|---|---|---|
| **Impressum** | Transparenz und rechtliche Verantwortlichkeit herstellen | Macht sichtbar, **wer hinter der Website steht** – Pflichtangaben wie Name, Adresse, Kontakt, ggf. Handelsregister und USt-ID. Besucher und Behörden müssen den Verantwortlichen leicht erreichen können. (Immer **im Footer verlinkt** und von jeder Seite abrufbar.) | e-recht24.de/impressum-generator<br>datenschutzgenerator.de |
| **Datenschutz-erklärung** | Information über Art, Zweck und Umfang der Datenverarbeitung | Erklärt offen, **welche Daten auf der Website verarbeitet werden** – z. B. durch Formulare, Cookies, Karten, Schriftarten oder Analyse-Tools. Sie schafft Vertrauen und ist **rechtlich vorgeschrieben**, sobald personenbezogene Daten verarbeitet oder externe Dienste eingebunden sind. (Regelmäßig aktualisieren.) | datenschutz-generator.de<br>e-recht24.de/datenschutzerklaerung |

# Grundlegendes für den Betriebsalltag

....

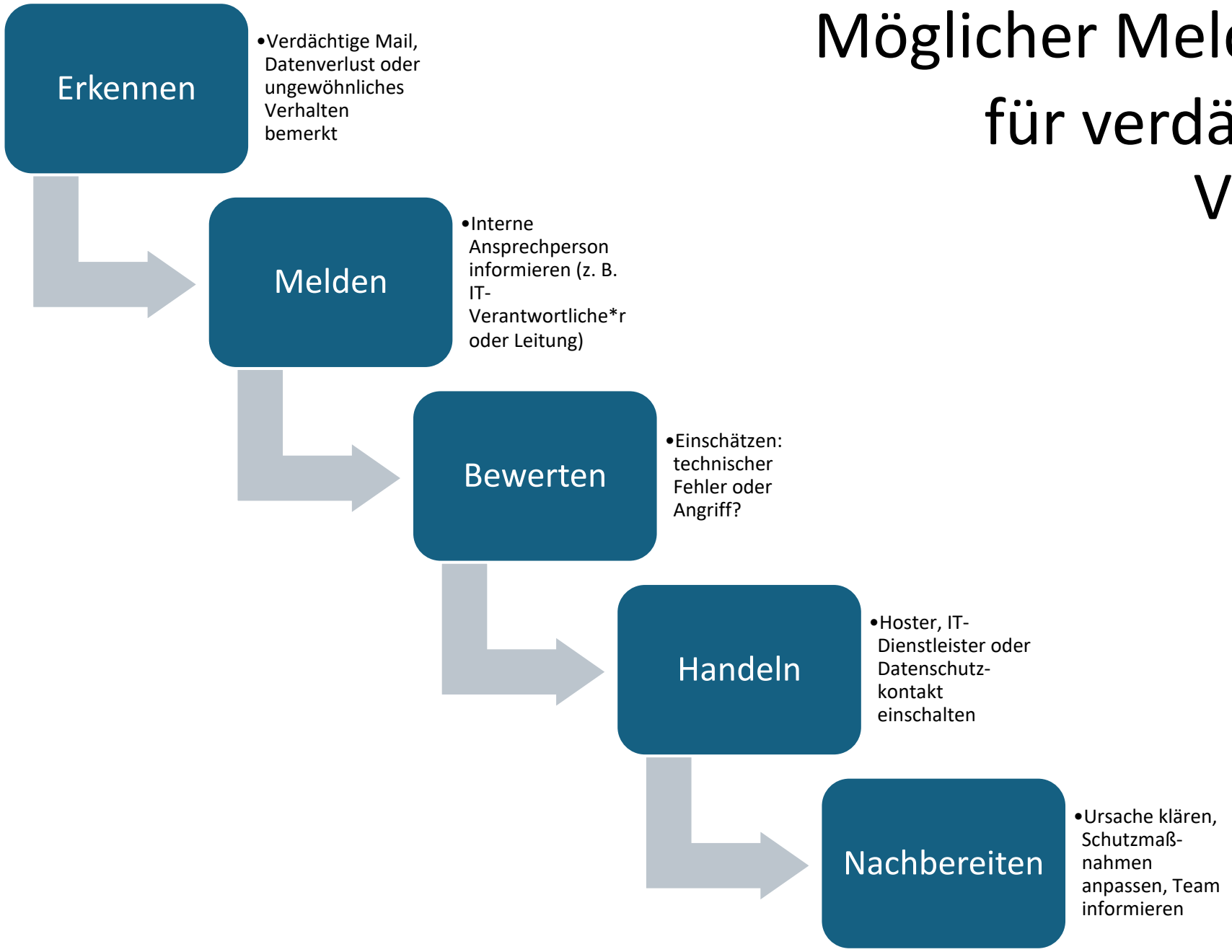
Routinen und Awareness

KI-generiert

# Routinen für Technik & Team

| Technische Routinen | Teamroutinen |
|---|---|
| Systeme regelmäßig updaten (CMS, Plugins, Server) | Zuständigkeiten für IT-Sicherheit klar festlegen |
| Automatische Backups prüfen und extern speichern | Sicherheitsfragen regelmäßig im Teammeeting besprechen |
| HTTPS / SSL aktiv halten und Zertifikate prüfen | Kurze Awareness-Impulse oder Schulungen einplanen |
| Zugänge verwalten (alte Accounts löschen, starke Passwörter nutzen) | Meldewege für verdächtige Vorfälle definieren |
| Sicherheitsstandards mit Hoster oder IT-Agentur abklären | Offene Fehlerkultur leben – Vorfälle werden geteilt, nicht vertuscht |

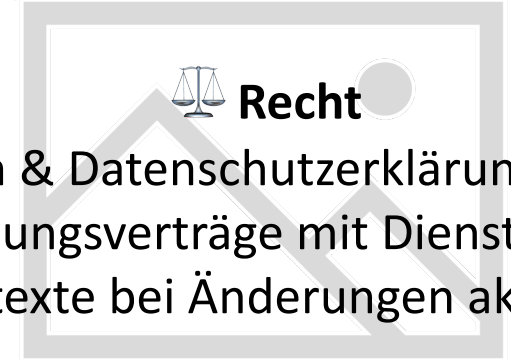
# Möglicher Meldeweg für verdächtige Vorfälle



# Finaler Check

## ⚙️ Technik

- Website läuft über HTTPS / SSL aktiv
- Updates & Backups regelmäßig durchgeführt
- Zugänge & Passwörter sicher verwaltet



## ⚖️ Recht

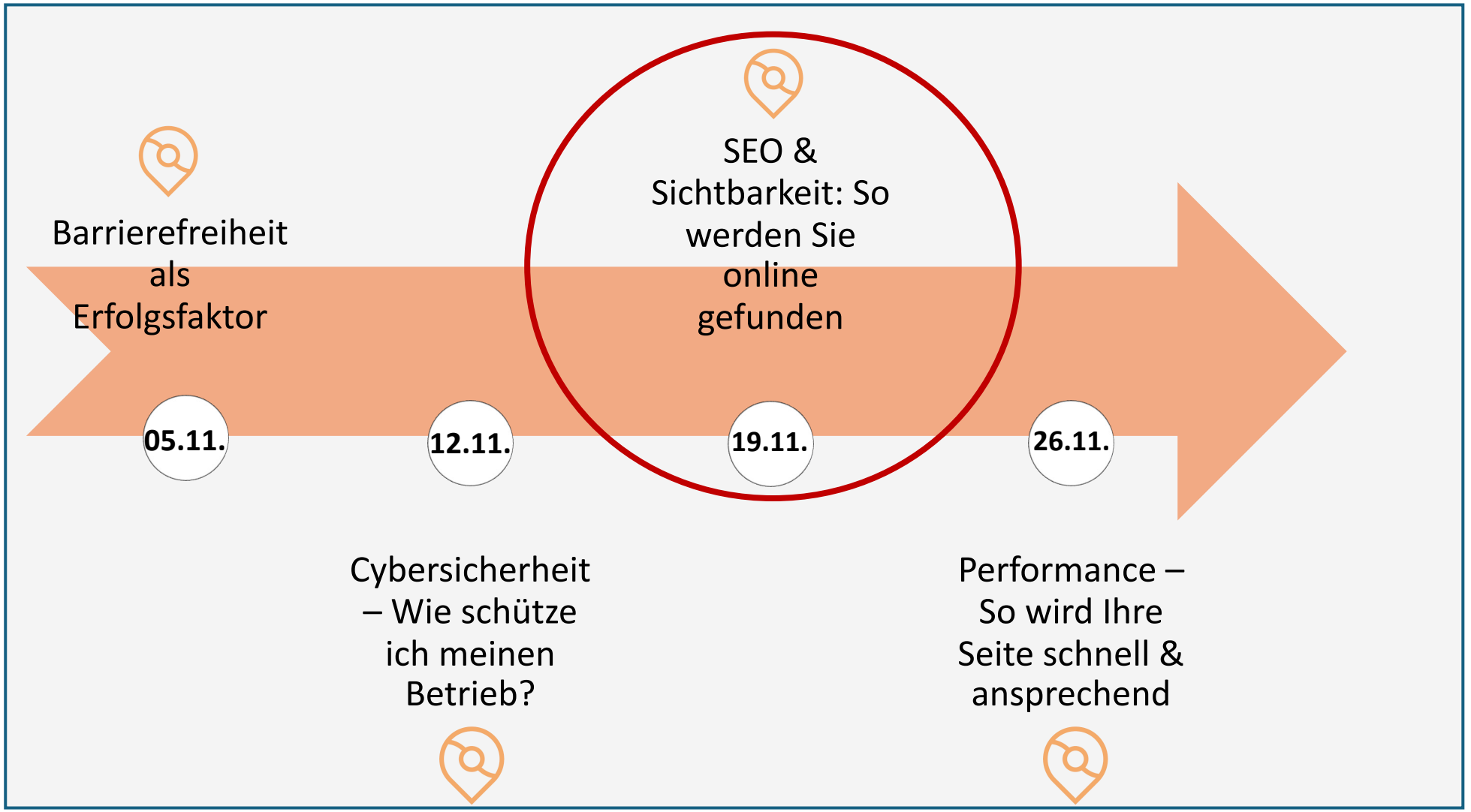
- Impressum & Datenschutzerklärung vollständig
- Auftragsverarbeitungsverträge mit Dienstleistern vorhanden
- Rechtstexte bei Änderungen aktualisiert

## 👥 Team

- Zuständigkeiten & Meldewege klar definiert
- Cybersicherheit regelmäßig im Team besprechen
- Offene Fehlerkultur statt Schuldzuweisungen

**KI-generiert**

# UNSERE WEBSEITEN-THEMENREIHE




https://tourismusnetzwerk-brandenburg.de/termine?thema=All&veranstaltungstyp=All&region=All&zielgruppe=All&keys=webseiten

| Tool / Website | Funktion | Einsatz im Webinar | Nutzen auf den Punkt gebracht |
|---|---|---|---|
| **MXToolbox**https://mxtoolbox.com | Prüft DNS-Einträge (SPF, DKIM, DMARC, Mailserver-Gesundheit) | Live-Demo zur E-Mail-Authentifizierung | Zeigt, ob meine Domain gefälschte Mails abwehren kann – quasi der Gesundheitscheck fürs E-Mail-System. |
| **Have I Been Pwned**https://haveibeenpwned.com | Prüft, ob E-Mail-Adressen in Datenlecks aufgetaucht sind | Awareness-Block „Phishing & Datenlecks“ | Hier sieht man, ob eigene Daten schon in Leaks kursieren – Weckruf für Passwort-Hygiene. |
| **Webbkoll**https://webbkoll.5july.net/de/ | Datenschutz- und Sicherheitsanalyse von Websites | HTTPS- und Datenschutz-Demo | Zeigt auf einen Blick, ob eine Website verschlüsselt ist und Daten an Dritte sendet. |
| **VirusTotal**https://www.virustotal.com | Scannt verdächtige E-Mails, Links oder Dateien mit vielen Virenscannern gleichzeitig | Beispiel für Phishing-Prüfung | Wenn man unsicher ist, ob ein Anhang sauber ist – hier kann man’s gefahrlos prüfen. |
| **Let’s Encrypt**https://letsencrypt.org | Kostenloses SSL-Zertifikat | Bei HTTPS/SSL-Abschnitt | Mit Let’s Encrypt kann jeder in Minuten HTTPS aktivieren – kostenlos und DSGVO-konform. |
| **OMGF / Local Google Fonts Plugin**https://wordpress.org/plugins/host-webfonts-local/ | Lädt Google Fonts lokal | Demo bei „Externe Inhalte prüfen“ | Damit lädt die Schriftart direkt von der eigenen Website – kein Datentransfer an Google mehr. |
| **How Secure Is My Password**https://howsecureismypassword.net | Schätzt Passwortstärke | Awareness-Teil / Teamroutinen | Ein witziger, aber eindrucksvoller Check – wie lange ein Rechner bräuchte, mein Passwort zu knacken. |
| **Backup-Plugin (z. B. UpdraftPlus)** | Automatische Datensicherung in WordPress | Technische Routinen | Backups sind die Versicherungspolice jeder Website – am besten automatisch. |
| **Let’s Debug**https://letsdebug.net | Testet SSL-Konfiguration & mögliche Fehler | Vertiefung bei HTTPS-Teil (optional) | Wenn HTTPS nicht klappt, zeigt Let’s Debug, wo’s hängt – perfekt zur Fehlersuche. |

**KI-generiert**

# Teejit GmbH


## Christoph Paul

**Head of Content**

**Email: christoph@teejit.de**

**Phone: +491713286837**

# Wir freuen uns auf Ihr Feedback

Umfrage-Link

TOURISMUSNETZWERK BRANDENBURG

teejit

# Vielen Dank für Ihre Beiträge