

**CYBER KOMPAKT /
RISIKOFREI
UNTERWEGS.**

Marcus Unger, ARTUS Osnabrück

WAS SIE IN SACHEN CYBER-SICHERHEIT UNTERWEGS BEACHTEN MÜSSEN.

Geschäftsreisen, Urlaube und Abwesenheiten stellen Unternehmen und Mitarbeitende vor besondere Herausforderungen in Sachen IT- und Informationssicherheit. Unterschiedliche Standorte, wechselnde Netzwerke und erhöhte Angriffsrisiken erfordern ein bewusstes und konsequentes Sicherheitsverhalten. **Unsere Factsheets bieten kompakte, praxisnahe Empfehlungen zu den wichtigsten Themen – von der physischen Gerätesicherung über sichere Kommunikation bis hin zur Vorbereitung vor der Abwesenheit.**

Sie dürfen klare Handlungsempfehlungen, praktische Checklisten und verständliche Hintergrundinfos erwarten, die sich leicht im Alltag umsetzen lassen.

DAMIT SIE OPTIMAL VORBEREITET SIND, UM SENSIBLE DATEN ZU SCHÜTZEN, COMPLIANCE-ANFORDERUNGEN ZU ERFÜLLEN UND CYBERRISIKEN AUF REISEN EFFEKTIV ZU MINIMIEREN /

CYBER KOMPAKT / IDENTITÄTSBETRUG UND PHISHING IN DER URLAUBSZEIT

Gefahrenlage /

Die Urlaubszeit ist für viele die schönste Zeit des Jahres – doch leider auch eine besonders beliebte Phase für Cyberkriminelle, um gezielte Betrugsversuche zu starten. Mit gefälschten E-Mails, SMS oder Webseiten versuchen Angreifer, an Ihre Daten zu gelangen oder finanzielle Schäden an Ihrem Unternehmen zu verursachen. Gerade in Zeiten, in denen viele Mitarbeitende im Urlaub sind, steigt das Risiko, auf solche Tricks hereinzufallen.

Umso wichtiger ist es, wachsam zu bleiben und typische Fallen zu erkennen.

- > GEFÄLSCHTE BUCHUNGSBESTÄTIGUNGEN ODER REISEANGEBOTE
- > PHISHING-MAILS MIT „URLAUBSGRÜSSEN“ VON ANGEBLICHEN KOLLEGEN
- > FAKE-PORTALE FÜR FLÜGE, HOTELS ODER FERIENHÄUSER
- > SMISHING: Z. B. ANGEBLICHE PAKET-BENACHRICHTIGUNGEN MIT SCHADLINK

Chef-Masche /

Betrüger geben sich als verreiste Führungskraft aus und fordern z. B. Überweisungen oder sensible Infos. Out-of-Office-Mails helfen ihnen, gezielt Personen anzuschreiben.

Was Sie tun sollten /

- > **MISSTRAUEN BEI URLAUBSBEZOGENEN MAILS:**
Betreffzeilen wie „Reiseänderung“ oder „Urlaubsangebot“ kritisch prüfen. Keine Links oder Anhänge öffnen ohne Verifizierung.
- > **NUR OFFIZIELLE BUCHUNGSPORTALE NUTZEN:**
Adressen manuell eingeben, auf HTTPS und Zertifikate achten. Kein Klick auf Reise-Links aus E-Mails.
- > **MITARBEITER SCHULEN:**
Klare Regeln für Datenweitergabe und Zahlungsfreigaben. Beispiele für Betrug zeigen und Rückfragepflicht etablieren.
- > **ABWESENHEITSNOTIZEN SCHÜTZEN:**
Keine Details zur Nichterreichbarkeit. Nur Vertretung und ggf. Rückkehrdatum nennen.

ARTUS
CYBER
TIPP
/

Im Zweifel lieber nachfragen –
intern oder beim vermeintlichen Absender.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
[www.artus-gruppe.com/leistungen/produkte/
cyberversicherung](http://www.artus-gruppe.com/leistungen/produkte/cyberversicherung)



CYBER KOMPAKT /**WLAN- UND NETZ-
WERKSICHERHEIT
AUF REISEN**

Geschäftlich oder privat unterwegs, sind wir oft auf fremde Netzwerke angewiesen – sei es im Hotel, Café oder am Flughafen. Diese öffentlichen WLANs sind jedoch häufig nicht ausreichend geschützt und bieten Cyberkriminellen eine gute Gelegenheit, Daten abzugreifen oder Schadsoftware einzuschleusen. Umso wichtiger ist es, die Risiken zu kennen und gezielt Schutzmaßnahmen zu ergreifen, damit Ihre Verbindung auch unterwegs sicher bleibt.

Gefahrenlage /

Unterwegs greifen viele auf öffentliche WLANs zurück – ein beliebtes Ziel für Cyberangriffe.

Typische Risiken sind:

- > GEFÄLSCHTE HOTSPOTS („EVIL TWINS“)
- > OFFENE NETZE OHNE VERSCHLÜSSELUNG
- > UNSICHERE HOTEL-WLANs
- > INFIZIERTE ÖFFENTLICHE PCS
(Z. B. MIT KEYLOGGERN)

Auch Mobilfunknetze sind unterwegs wichtig – sicherer, aber teils teuer. Viele weichen daher auf WLAN aus, oft ohne ausreichende Absicherung.

Was Sie tun sollten /

- > **NUR OFFIZIELLE NETZWERKE NUTZEN:**
WLAN-Namen & -Passwort immer beim Anbieter erfragen. Offene Netzwerke nur für Unwichtiges.
- > **VPN NUTZEN:**
Vor der Reise einen VPN einrichten. Die Verbindung wird so verschlüsselt – besonders wichtig für E-Mails, Firmendienste und alles rund ums Banking.
- > **MOBILFUNK STATT RISIKONETZ:**
Kritische Vorgänge besser über LTE/5G durchführen. Lokale SIM oder mobiler Hotspot können eine sichere Alternative sein.
- > **GERÄTEEINSTELLUNGEN ANPASSEN:**
Automatisches Verbinden mit WLAN deaktivieren. WLAN & Bluetooth ausschalten, wenn nicht in Nutzung. Netzwerk auf *öffentlich* stellen, Firewall aktivieren.
- > **ÖFFENTLICHE PCS VERMEIDEN:**
Keine sensiblen Daten eingeben oder speichern. Wenn nötig: Bildschirmtastatur nutzen, Verlauf und Cache löschen.



CYBER KOMPAKT /SICHERHEIT
VON GERÄTEN
AUF REISEN

Mobile Geräte wie Smartphones, Laptops oder Tablets sind auf Reisen unverzichtbar – aber auch anfällig für Diebstahl und digitale Angriffe. Gerade auf Reisen ist der Schutz von Geräten und Daten entscheidend, um Missbrauch oder Datenverlust zu vermeiden.

Gefahrenlage /

- > GERÄTEVERLUST DURCH DIEBSTAHL ODER UNACHTSAMKEIT
- > VERALTETE SOFTWARE MIT SICHERHEITSLÜCKEN
- > UNZUREICHENDER ZUGRIFFSSCHUTZ BEI GERÄTEN ODER APPS
- > UNKONTROLLIERTE NUTZUNG FREMDER GERÄTE ODER SMARTER HELFER
- > DATENABFLUSS BEI VERBINDUNG ZU MIETWAGEN, HOTEL-TV ODER SMART-ASSISTENTEN

Was Sie tun sollten /

- > **GERÄTEAUSWAHL BEGRENZEN:**
Nehmen Sie nur wirklich notwendige Geräte mit. Weniger Geräte bedeuten weniger Angriffsfläche.
- > **ALLE SYSTEME AKTUALISIEREN:**
Vor der Reise Betriebssystem, Apps und Sicherheitssoftware auf den neuesten Stand bringen – idealerweise im Heim- oder Firmennetz.
- > **GERÄTESCHUTZ AKTIVIEREN:**
Jedes Gerät sollte durch starke Passwörter, PIN oder Biometrie geschützt sein. Speicher-Verschlüsselung aktivieren, wenn möglich 2-Faktor-Authentifizierung einrichten.
- > **AUF DIEBSTAHL VORBEREITEN:**
Funktionen wie „Mein Gerät finden“, Fernsperrung und Ortung aktivieren. Seriennummern notieren – hilfreich für Anzeigen bei der Polizei und auch für die Versicherung.
- > **SMARTE GERÄTE ABSICHERN:**
Standard-Passwörter bei tragbaren Gadgets ändern. Nicht genutzte Funkverbindungen wie Bluetooth oder NFC deaktivieren. Geliehene Geräte meiden oder konsequent nach Nutzung bereinigen.

ARTUS
CYBER
TIPP
/

Sicherheit beginnt vor der Abreise –
prüfen Sie Ihre Geräte, bevor Sie unterwegs sind.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
[www.artus-gruppe.com/leistungen/produkte/
cyberversicherung](http://www.artus-gruppe.com/leistungen/produkte/cyberversicherung)



CYBER KOMPAKT /DATENSCHUTZ,
BACKUPS UND
SOCIAL MEDIA

Sensible Daten sind auf Reisen besonders gefährdet – durch Diebstahl, Verlust, Spionage oder unbedachtes Verhalten in sozialen Medien. Wer sich vorbereitet und bewusst mit Informationen umgeht, schützt sich und sein Unternehmen.

Gefahrenlage /

- > VERLUST SENSIBLER DATEN BEI GERÄTEVERLUST ODER BESCHLAGNAHME
- > UNZUREICHENDE DATENSICHERUNG VOR DER REISE
- > ZU VIELE UNNÖTIGE DATEN AUF GERÄTEN
- > INFORMATIONSLACKS DURCH SOCIAL-MEDIA-POSTS
- > UNGEWOLLTE PREISGABE GESCHÄFTLICHER DETAILS IN DER ÖFFENTLICHKEIT

Was Sie tun sollten /

- > **BACKUPS ANLEGEN:**
Vor der Reise vollständige Datensicherungen erstellen – idealerweise verschlüsselt in der Cloud oder auf externer Hardware. Nur notwendige Daten mitnehmen.
- > **GERÄTE „SAUBER“ HALTEN:**
Löschen oder auslagern, was nicht unterwegs gebraucht wird. Für Reisen in sensible Länder eventuell Geräte mit Minimaldaten einsetzen.
- > **SOCIAL-MEDIA ZURÜCKHALTEN:**
Keine Reisebilder, Standorte oder Zeitangaben öffentlich posten – weder privat noch über Firmkanäle. Inhalte besser erst nach der Rückkehr teilen.
- > **UMFELD SENSIBILISIEREN:**
Familienmitglieder und Kollegen darauf hinweisen, keine Reiseinfos öffentlich zu machen – insbesondere bei Abwesenheiten von Führungskräften.
- > **DISKRETION IN DER ÖFFENTLICHKEIT:**
Geschäftliches gehört nicht in öffentliche Gespräche oder auf offene Bildschirme. Sichtschutz für Laptops nutzen, vertrauliche Dokumente abdecken.

**ARTUS
CYBER
TIPP
/**

Je weniger Daten Sie mitnehmen, desto weniger können Sie verlieren. Guter Schutz Ihrer Daten beginnt mit kluger Zurückhaltung.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
www.artus-gruppe.com/leistungen/produkte/cyberversicherung



CYBER KOMPAKT / KONTOÜBER- WACHUNG UND ZUGRIFFS- MANAGEMENT

Während Sie unterwegs sind, sollte Ihre digitale Sicherheit nicht pausieren. Gerade in dieser Zeit und vor allem, wenn Sie im Urlaub oder auf Geschäftsreisen sind, nutzen Angreifer die reduzierte Aufmerksamkeit aus, um auf Konten zuzugreifen oder Zahlungsfreigaben zu missbrauchen. Mit wenigen Maßnahmen bleiben Sie auch aus der Ferne in Kontrolle.

Gefahrenlage /

- > UNBEMERKTE KONTOABBUCHUNGEN IM URLAUB
- > MISSBRAUCH VON ADMIN- ODER E-MAIL-ZUGÄNGEN
- > FEHLENDE LOGIN-WARNUNGEN BEI NEUEN GERÄTEN
- > KEINEN VERTRETER FÜR KRITISCHE FREIGABEN BENENNEN

Was Sie tun sollten /

- > **BANKKONTEN ÜBERWACHEN:**
Aktivieren Sie Push- oder SMS-Benachrichtigungen für jede Transaktion. Legen Sie Limits fest, ab denen

Karten automatisch gesperrt werden, und informieren Sie Ihre Bank über die Reiseroute zur Betrugsprävention.

> **KONTOBEWEGUNGEN PRÜFEN:**

Kontrollieren Sie regelmäßig (z. B. alle 2 bis 3 Tage) online Ihre Konten oder delegieren Sie diese Aufgabe an eine vertrauenswürdige Person. Sofort bei Auffälligkeiten reagieren.

> **LOGIN-WARNUNGEN AKTIVIEREN:**

Nutzen Sie Sicherheitsmeldungen bei allen wichtigen Accounts (Google, Microsoft 365 etc.) – etwa bei Logins von unbekanntem Geräten oder Passwortänderungen.

> **ZUGRIFFE EINSCHRÄNKEN:**

Falls gewisse Admin-Konten im Urlaub nicht benötigt werden: zeitweise sperren oder Passwörter ändern. Diese können in einem Passwortmanager sicher aufbewahrt werden.

> **VERTRETUNG BENENNEN:**

Legen Sie vor Abreise fest, wer Zahlungen oder IT-Freigaben übernehmen darf – so wird in Ihrer Abwesenheit keine improvisierte Lösung nötig.



CYBER KOMPAKT / CEO FRAUD UND SOCIAL ENGINEERING BEI ABWESENHEITEN

Vor allem Urlaubszeiten sind Hochsaison für Betrüger. Besonders gefährlich ist der sogenannte CEO Fraud: Dabei geben sich Täter per E-Mail oder Telefon als abwesende Geschäftsführung aus und versuchen, Mitarbeitende zu eiligen Zahlungen oder zur Preisgabe sensibler Daten zu verleiten. Vorsorge ist der beste Schutz.

Typische Masche /

- > TÄTER GEBEN SICH ALS VERREISTE FÜHRUNGSKRAFT AUS
- > KONTAKT PER GEFÄLSCHTER E-MAIL, OFT MIT ZEITDRUCK UND GEHEIMHALTUNG
- > ZIEL: ÜBERWEISUNG VERANLASSEN ODER INTERNE INFORMATIONEN ERLANGEN
- > TÄUSCHEND ECHT DURCH E-MAIL-/ TELEFON-SPOOFING
- > VORBEREITUNG OFT DURCH RECHERCHE AUF FIRMENWEBSITES UND IN SOCIAL MEDIA

Was Sie tun sollten /

- > **MITARBEITENDE SENSIBILISIEREN:**
Klären Sie Ihr Team über CEO Fraud und Support-Scams auf. Weisen Sie darauf hin, dass echte

Zahlungsaufforderungen nie spontan und ohne Rückversicherung erfolgen – schon gar nicht aus dem Urlaub.

- > **ABWESENHEITSPROZESSE FESTLEGEN:**
Jede Überweisung über Schwellenwert (z. B. 1.000 €) muss intern gegengeprüft werden – telefonisch oder per Videocall über bekannte, unabhängige Nummern. Alleinige Anweisungen aus E-Mails sind zu ignorieren.
- > **AUTHENTIFIZIERUNG VEREINBAREN:**
Definieren Sie vorher mit Buchhaltung/Teamleitung sichere Kommunikationswege (z. B. Firmemessenger) oder Codewörter. Fehlen diese Merkmale, ist Misstrauen angebracht.
- > **ONLINE-INFORMATIONEN EINSCHRÄNKEN:**
Keine öffentlichen Hinweise auf Urlaubszeiten oder Vertretungsregelungen in LinkedIn, auf der Website oder in Pressemitteilungen. Je weniger Angreifer wissen, desto geringer ihr Täuschungspotenzial.
- > **KLARE RÜCKFRAGEN-REGEL ETABLIEREN:**
Verdächtige Anweisungen? Rückruf beim Chef oder einer hinterlegten Vertrauensperson – immer. Bieten Sie Ihrem Team die nötigen Kontaktwege, damit niemand „auf gut Glück“ entscheidet.


 ARTUS
CYBER
TIPP
/

Lieber einmal zu oft nachfragen als einen sechsstelligen Schaden riskieren. Prävention beginnt mit interner Kommunikation und klaren Regeln.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
www.artus-gruppe.com/leistungen/produkte/cyberversicherung



CYBER KOMPAKT /**SIM-SWAPPING
UND MOBILFUNK-
RISIKEN**

Ihr Smartphone ist auf Reisen oft Ihr Zugang zu Bank, Mail und Sicherheitssystemen – und damit auch ein lohnenswertes Ziel für Angreifer. Besonders perfide ist SIM-Swapping: Betrüger übernehmen Ihre Rufnummer und erhalten so Zugriff auf Ihre Konten und Dienste. Die gute Nachricht: Mit ein paar Maßnahmen lässt sich das Risiko deutlich senken.

Was passiert beim SIM-Swapping /

- > ANGREIFER GEBEN SICH BEIM MOBILFUNKANBIETER ALS SIE AUS
- > IHRE RUFNUMMER WIRD AUF EINE FREMDE SIM-KARTE ÜBERTRAGEN
- > IHRE EIGENE SIM FUNKTIONIERT PLÖTZLICH NICHT MEHR
- > LOGIN-CODES, MTANS UND ANRUFGE GEHEN AN DIE BETRÜGER
- > ZIEL: ZUGANG ZU BANK, MAIL, SOCIAL MEDIA – OFT MIT FINANZIELLEN SCHÄDEN

Was Sie tun sollten /

- > **2-FAKTOR-AUTHENTIFIZIERUNG (2FA) OHNE SMS:**
Verwenden Sie für wichtige Konten Authenticator-Apps (z. B. Microsoft, Google Authenticator) oder

Hardware-Token statt SMS-Codes. Viele Banken bieten App-basierte TANs als sicherere Alternative.

> MOBILFUNK-ZUGANG SCHÜTZEN:

Richten Sie bei Ihrem Provider einen Service-PIN oder ein Kundenpasswort ein. So kann niemand mit Basisdaten (z. B. Name oder Geburtsdatum) leicht eine neue SIM bestellen. Ideal: Änderungen nur im Shop mit Ausweis.

> PERSÖNLICHE DATEN ZURÜCKHALTEN:

Vermeiden Sie öffentlich zugängliche Informationen wie Geburtstag, Haustiernamen oder Wohnadresse in sozialen Netzwerken – sie dienen Angreifern als Baustein für Identitätsdiebstahl.

> WARNSIGNALE ERKENNEN:

Kein Empfang ohne erkennbaren Grund? Ungewöhnliche Account-Meldungen? Sofort handeln: Handy neu starten, Provider anrufen, Passwörter ändern, ggf. Bank oder IT informieren.

> SICHER REISEN:

Nutzen Sie nur vertrauenswürdige Roaming- oder lokale Anbieter. Vermeiden Sie SMS-basierte Logins über öffentliche WLAN-Hotspots. Versenden Sie keine vertraulichen Daten per SMS – nutzen Sie sichere Messenger oder VPN-Dienste.



CYBER KOMPAKT /**REISEMALWARE
UND TECHNISCHE
GEFAHREN
UNTERWEGS**

Auf Geschäfts- und Privatreisen lauern neben offenen WLANs auch versteckte technische Fallen. Besonders heimtückisch: „Juice Jacking“ an öffentlichen USB-Ladestationen und präparierte Kabel oder Geräte, die Malware einschleusen. Auch gefälschte Apps oder infizierte USB-Sticks stellen ein Risiko dar. Vorsicht ist also geboten!

Wichtige Risiken im Überblick /

- > JUICE JACKING: MALWARE-INSTALLATION ÜBER MANIPULIERTE USB-LADESTATIONEN
- > GEFÄLSCHTE REISE-APPS: SCHADSOFTWARE IN VERMEINTLICHEN OFFLINE-GUIDES ODER WÄHRUNGSRECHNERN
- > SPIONAGE IN HOTEL-WLANs: GEZIELTE INFESTIONEN ÜBER UNGESICHERTE NETZE
- > INFIZIERTE USB-STICKS: TROJANER AUF DATENTRÄGERN, Z. B. BEI MESSEN ODER KONFERENZEN
- > ÖFFENTLICHE COMPUTER: GEFAHR DURCH VIRENBEFALL UND DATENKLAU BEIM ANSCHLUSS EIGENER MEDIEN

Was Sie tun sollten /

- > **EIGENE LADEGERÄTE UND POWERBANKS NUTZEN:**
Vermeiden Sie öffentliche USB-Ports. Laden Sie nur

mit eigenem Netzteil an Steckdosen oder mit Powerbank. Wenn Sie öffentliche USB-Ladestationen nutzen müssen, verwenden Sie Datenblocker („Charge-Only-Adapter“), die Datenübertragung verhindern.

> **KEINE FREMDEN USB-KABEL ODER GERÄTE ANSCHLIESSEN:**

Stecken Sie keine unbekanntes Kabel in Smartphone oder Notebook. USB-Kabel können Schadsoftware übertragen („USB-Killer“). Auch das Verbinden mit fremden Computern per USB vermeiden.

> **APPS NUR AUS OFFIZIELLEN STORES INSTALLIEREN:**

Laden Sie Reise-Apps ausschließlich über Google Play oder Apple App Store. Misstrauen Sie Links in Mails oder Webseiten, die zum Download auffordern. Prüfen Sie App-Berechtigungen kritisch.

> **GERÄTE SCHÜTZEN UND REGELMÄSSIG PRÜFEN:**

Halten Sie Antivirus- und Sicherheitssoftware aktuell. Scannen Sie USB-Sticks vor Verwendung an Firmenrechnern. Erstellen Sie Backups und erwägen Sie bei Verdacht auf Malware einen Werks-Reset.

> **SENSIBLE TÄTIGKEITEN NUR IN SICHEREN UMGEBUNGEN:**

Vermeiden Sie Online-Banking, Firmensystem-Logins oder das Öffnen vertraulicher Dokumente an öffentlichen PCs oder unsicheren Netzwerken.



CYBER KOMPAKT / PHYSISCHE SICHERHEIT & DIEBSTAHLSCHUTZ

Neben Cybergefahren sind physische Risiken auf Geschäftsreisen nicht zu unterschätzen. Laptop, Smartphone und Co sind begehrte Ziele für Diebe – am Flughafen, im Café oder im Hotel. Verlust bedeutet nicht nur materiellen Schaden, sondern auch Gefahr für vertrauliche Daten und Compliance-Verstöße.

Wichtige Risiken im Überblick /

- > DIEBSTAHL ODER LIEGENLASSEN VON GERÄTEN
- > VERLUST SENSIBLER UNTERNEHMENS DATEN
- > DATENSCHUTZVERSTÖSSE UND MELDEPFLICHTIGE VORFÄLLE
- > PHYSISCHE SPIONAGE (Z. B. „EVIL MAID ATTACK“) DURCH HOTELZIMMER-ÜBERWACHUNG ODER HARDWARE-MANIPULATION

Was Sie tun sollten /

- > **GERÄTE WIE BARGELD BEHANDELN:**
Laptops und Smartphones gehören ins Handgepäck, nie ins aufgegebene Gepäck. Lassen Sie Geräte nie unbeaufsichtigt – auch nicht kurz in Bahnen, Lounges oder Meetingräumen.
- > **SICHERUNG AM KÖRPER UND KABELSCHLOSS NUTZEN:**
Tragen Sie Ihre Geräte nah am Körper, z. B. Trageschleife der Tasche um Bein/Stuhl wickeln. Für

längere Aufenthalte in öffentlichen Räumen empfiehlt sich ein Laptop-Kabelschloss.

> HOTEL-SAFE NUR BEDINGT VERTRAUEN:

Verwahren Sie Geräte im Zimmersafe, aber bedenken Sie, dass Hotelpersonal oft Generalschlüssel hat. Nutzen Sie zusätzlich Festplattenverschlüsselung, starke Passwörter und automatische Sperren. Aktivieren Sie Funktionen zum Orten, Sperren und Löschen per Fernzugriff.

> TRACKING-HILFEN EINSETZEN:

Kleinere Geräte (Smartphones, USB-Sticks) mit Air-Tag, Tile oder ähnlichen Trackern ausstatten – erhöhen Auffindbarkeit, schrecken aber Diebe kaum ab.

> REGELMÄSSIGE KONTROLLE & CHECKLISTEN:

Prüfen Sie bei Ortswechseln (Hotel-Check-out, Taxi verlassen) immer, ob alle Geräte dabei sind. Eine kleine Checkliste (Laptop, Handy, USB-Stick, Firmenkarten) hilft gegen Liegenlassen.

> NOTFALLPLAN DEFINIEREN:

Legen Sie fest, wer im Diebstahlsfall informiert wird (Polizei, IT, Datenschutzbeauftragter, ggf. Kunden). Halten Sie Seriennummern bereit und sorgen Sie dafür, dass Geräte per Fernzugriff gesperrt oder gelöscht werden können. Ein klarer Plan reduziert Schaden und Reaktionszeit. Notieren Sie sich wichtige Nummer für den Notfall dort, wo Sie immer an sie herankommen.



CYBER KOMPAKT /SICHERE
KOMMUNIKATION
AUS DEM AUSLAND**Herausforderung /**

Im Ausland verlässt Ihre Kommunikation häufig sichere Unternehmensnetzwerke und durchläuft fremde Server. Unverschlüsselte E-Mails und Telefonate sind dort ein leichtes Ziel für Abhörversuche, z. B. durch Kriminelle oder staatliche Stellen.

Risiken /

- > MITLESEN UNVERSCHLÜSSELTER E-MAILS
- > ABHÖREN VON TELEFONATEN (INKL. ROAMING-ANRUFE)
- > BLOCKADE ODER ÜBERWACHUNG VON VPNs UND MESSENGER-DIENSTEN IN EINIGEN LÄNDERN
- > MITHÖREN IN ÖFFENTLICHEN BEREICHEN (HOTEL-LOBBY, CAFÉ)

Was Sie tun sollten /

- > **FIRMEN-VPN NUTZEN:**
Verbinden Sie sich vor der Nutzung von E-Mail, Cloud oder Firmendaten mit dem Unternehmens-VPN. So bleiben Daten bis zum Firmennetzwerk verschlüsselt.
- > **VERSCHLÜSSELTE MESSENGER UND CALLS:**

Für vertrauliche Gespräche verschlüsselte Messenger (Signal, Threema) oder sichere Meeting-Tools mit Ende-zu-Ende-Verschlüsselung verwenden. Telefonate über offene Leitungen vermeiden.

> **LOKALE VORSCHRIFTEN BEACHTEN:**

Informieren Sie sich vorab über Länderregeln zu VPN und Messenger-Nutzung. Halten Sie sich an die Gesetze, nutzen Sie erlaubte sichere Kanäle (z. B. firmenseitige VPN-Zugänge).

> **PHYSISCHE KOMMUNIKATIONSSICHERHEIT:**

Sprechen Sie nicht offen über vertrauliche Themen in der Öffentlichkeit. Suchen Sie ruhige, geschützte Räume für wichtige Calls oder Videokonferenzen.

> **NOTFALLKONTAKT & BACKUP-KANAL:**

Vereinbaren Sie einen zusätzlichen Kommunikationsweg (z. B. spezielles Roaming-Handy, sichere Messaging-Zeitpunkte) für den Fall eines Ausfalls.

> **DATENTRANSFERS MINIMIEREN:**

Verzichten Sie unterwegs wenn möglich auf den Versand großer sensibler Dateien. Nutzen Sie für notwendige Übertragungen sichere und verschlüsselte Kanäle. Teilen Sie Passwörter niemals im gleichen Kommunikationskanal.

ARTUS
CYBER
TIPP
/

Setzen Sie auf Verschlüsselung und bewusste Kommunikationsplanung – nur so schützen Sie Ihre Geschäftsgeheimnisse.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
www.artus-gruppe.com/leistungen/produkte/cyberversicherung



CYBER KOMPAKT / VORBEREITUNG DES UNTERNEHMENS VOR ABWESENHEIT

Sicherheit und reibungslose Abläufe müssen auch während der Abwesenheit von Führungskräften gewährleistet sein – sei es auf Urlaub oder Dienstreise. Klare Zuständigkeiten und IT-Sicherheitsmaßnahmen verhindern Risiken wie CEO Fraud, Datenverlust oder unerlaubte Zugriffe.

Was Sie tun sollten /

- > **VERTRETUNGEN SCHRIFTLICH FESTLEGEN:**
Benennen Sie für alle wichtigen Verantwortungsbereiche eine qualifizierte Vertretung mit klar definierten Entscheidungsbefugnissen. So vermeiden Sie Unsicherheiten und verhindern, dass Betrüger mit Fake-Anweisungen (CEO Fraud) Lücken ausnutzen.
- > **ABWESENHEITSNOTIZ MIT ANSPRECHPARTNER:**
Formulieren Sie Ihre E-Mail-Abwesenheitsmeldung so, dass externe Partner wissen, an wen sie sich bei dringenden Fällen wenden können (inkl. Kontaktdaten der Vertretung). Das schützt vor Verwirrung und Betrugsversuchen.
- > **INTERNE KOMMUNIKATION:**
Informieren Sie das Team und relevante Abteilungen rechtzeitig (z. B. Intranet, Rundmail), damit alle wissen, wann Sie nicht erreichbar sind. Sensibi-

lisieren Sie Kollegen, ungewöhnliche Aktivitäten im eigenen Namen besonders kritisch zu prüfen.

- > **IT-SICHERHEITSCHECK VOR DER ABREISE:**
Bitten Sie die IT-Abteilung, Ihre Accounts und Geräte speziell für die Abwesenheit vorzubereiten:
 - > Monitoring ungewöhnlicher Zugriffe (z. B. Login aus anderen Regionen)
 - > Temporäre Einschränkungen bei sensiblen Zugängen
 - > Backup-Gerät (Clean Device) für Notfälle
 - > Klare Regeln für Fernzugriffe, Datenlöschung oder Account-Resets im Notfall
- > **NOTFALL-KONTAKTWEGE DEFINIEREN:**
Vereinbaren Sie, wie und wann Sie im Ernstfall (z. B. großer IT-Sicherheitsvorfall) erreichbar sind. Definieren Sie, was als Notfall gilt, damit Sie nicht unnötig gestört werden, aber bei wichtigen Vorfällen sofort reagieren können.
- > **PASSWORTMANAGEMENT:**
Aktualisieren Sie vor der Reise kritische Passwörter, falls notwendig. Hinterlegen Sie verschlüsselte Zugangsdaten bei einer vertrauenswürdigen Stelle (z. B. Firmen-Passwortmanager), auf die auch Ihre Vertretung Zugriff hat. Das vermeidet unsichere Passwortweitergaben im Notfall.

ARTUS
CYBER
TIPP
/

Mit guter Vorbereitung und klaren Zuständigkeiten schützen Sie Ihr Unternehmen auch während Ihrer Abwesenheit vor Sicherheitsrisiken und gewährleisten reibungslose Abläufe.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
www.artus-gruppe.com/leistungen/produkte/cyberversicherung



CYBER KOMPAKT /**ZUSAMMEN-
FASSUNG UND
REISECHECKLISTE**

Eine sichere Geschäftsreise oder Urlaub beginnt mit guter Vorbereitung, konsequenter Vorsicht unterwegs und einer sorgfältigen Nachbereitung. Die folgende Checkliste hilft Ihnen, die wichtigsten Maßnahmen vor, während und nach Ihrer Reise im Blick zu behalten.

Checkliste**Vor der Reise /**

- Geräte aktualisieren und wichtige Daten verschlüsselt sichern
- Starke Passwörter, Zwei-Faktor-Authentifizierung (2FA) und Passwortmanager nutzen
- Nur notwendige Geräte und Zubehör mitnehmen (Ladegerät, Powerbank, VPN-App, Kabinenschloss)
- Vertretung festlegen und informieren, Abwesenheitsnotiz mit Ansprechpartner einrichten
- Privatsphäre-Einstellungen prüfen, keine Reisepläne öffentlich teilen

Während der Reise /

- Nur VPN-geschützte Netzwerke verwenden, Autoconnect und Bluetooth deaktivieren
- Keine sensiblen Logins über unsichere Verbindungen durchführen
- Geräte immer im Blick behalten oder sicher verwahren
- Verschlüsselte Messenger und sichere Kommunikationswege nutzen
- Bei ungewöhnlichen Anrufen oder Mails vorsichtig sein und nachfragen

Nach der Reise /

- Geräte auf Malware überprüfen und Sicherheitsupdates einspielen
- Passwörter ändern, wenn Verdacht auf Missbrauch besteht
- Bank- und Account-Logs auf Unregelmäßigkeiten prüfen
- Erkenntnisse im Team teilen und Sicherheitsprozesse optimieren

**GUTE
REISE**UND KOMMEN
SIE SICHER
ZURÜCK!

Mit dieser Checkliste sind Sie optimal vorbereitet, um Ihre Geschäftsreise sicher und sorgenfrei zu gestalten – so bleibt Ihnen mehr Zeit für das Wesentliche. Sollten Sie Fragen zur Cybersicherheit, zu individuellen Absicherungsmaßnahmen oder zu aktuellen Bedrohungen haben, steht Ihnen das Expertenteam von ARTUS jederzeit gerne zur Verfügung.

Nutzen Sie unsere Kompetenz, um Risiken zu minimieren und Ihr Unternehmen bestmöglich zu schützen. Kontaktieren Sie uns einfach – wir unterstützen Sie dabei, auch unterwegs cyber-sicher zu bleiben.

ARTUS ist auch in Ihrer Region.
Unsere Experten beantworten gerne Ihre Fragen.
[www.artus-gruppe.com/leistungen/produkte/
cyberversicherung](http://www.artus-gruppe.com/leistungen/produkte/cyberversicherung)



CYBER KOMPAKT / SPRECHEN SIE UNS AN!

Über ARTUS /

Die ARTUS GRUPPE gehört zu den Top-Versicherungsmaklern in Deutschland und der Schweiz mit mehr als 500 Mitarbeitern an 16 Standorten. Sie erstellt Absicherungskonzepte gegen Cybergefahren für Unternehmen des Mittelstands und der mittelständischen Industrie gegen eine Vielzahl von Risiken wie Betrugsschäden, Schadenersatzansprüchen, Vertragsstrafen, Betriebsunterbrechungen und anderer Kosten, die mit Hackerangriffen und Cyber-Gefahren zusammenhängen.

Über den Autor /

Marcus Unger ist Leiter des Competence Centers Cyber Nord und verantwortet die Bereiche Risikoerfassung, Risikobewertung und Cyber-Incident-Management. Er berät seit über 20 Jahren erfolgreich Kundenunternehmen hinsichtlich Ihrer Cyberabdeckung und Ihrer Cybersicherheit.

Das ARTUS Cyber Team berät Sie gerne /



/ MARCUS UNGER /

Head of Competence Center Cyber
Nord, Cyber-Experte
ARTUS Osnabrück

marcus.unger@artus-gruppe.com



/ MARKUS WAGNER /

Head of Competence Center Cyber
Süd, Leiter Sachversicherung
ARTUS Friedrich Ganz

markus.wagner@artus-gruppe.com



/ FELIX RÖDER /

Cyber-Experte,
Stellvertretender Leiter Analyse
ARTUS Friedrich Ganz

felix.roeder@artus-gruppe.com





ARTUS GRUPPE /

GEMEINSAM
EINFACH
MACHEN

www.artus-gruppe.com