5/26

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

LIEFERKETTENANGRIFFE

Wenn Cyberangriffe im Jahr 2026 über Geschäfts-partner erfolgen

QR-CODES

Einmal scannen, bitte – und schon sind Ihre Daten weg

powered by
PRIVACYXPERTS

Liebe Leserinnen und Leser,

Cyberangriffe kommen 2026 immer seltener direkt. Stattdessen nutzen Angreifer gezielt die Lieferkette – Softwareanbieter, Dienstleister oder kleine Zulieferer werden zum Einfallstor. Der Grund ist simpel: Vertrauen lässt sich leichter ausnutzen als eine gut gesicherte Infrastruktur.

Ob manipulierte Updates oder kompromittierte Partner – Angriffe skalieren heute über Abhängigkeiten. Wer einen Anbieter trifft, erreicht viele. Gleichzeitig geraten kleinere Unternehmen ins Visier, weil sie oft weniger geschützt sind, aber Zugang zu größeren Kunden haben. So wird aus einem scheinbar unbedeutenden Angriff schnell ein ernsthaftes Risiko.

Hinzu kommt eine zweite Entwicklung: Angriffe auf Menschen. Quishing zeigt, wie effektiv einfache Methoden sein können. Ein QR-Code, ein kurzer Scan – und Sicherheitsmechanismen werden umgangen. Der Angriff tarnt sich als Alltag.

Die zentrale Erkenntnis: IT-Sicherheit endet nicht am eigenen Netzwerk. Sie umfasst Partner, Prozesse und das Verhalten der Mitarbeitenden. Absolute Sicherheit gibt es nicht. Entscheidend ist, Risiken zu erkennen, wachsam zu bleiben und schnell zu reagieren.

Denn die Frage ist längst nicht mehr, ob ein Angriff kommt – sondern über wen. Vertrauen wird damit zur kritischsten Ressource in der digitalen Zusammenarbeit. Wer es schützt, stärkt nicht nur die eigene Sicherheit, sondern die gesamte Lieferkette.

Herzliche Grüße

Ihr Redaktionsteam von „Privacy@Work“

SEBASTIAN TAUSCH

ARBEITET ALS SELBSTSTÄNDIGER IT-BERATER UND UNTERSTÜTZT KLEINE UND MITTLERE UNTERNEHMEN PRAXISNAH IM BEREICH DATENSCHUTZ. NACH EINER KAUFMÄNNISCHEN AUSBILDUNG SAMMELTE ER VIELE JAHRE PRAKTISCHE IT-ERFAHRUNG.

ANDREAS HESSEL

IST ALS CHIEF INFORMATION SECURITY OFFICER LANGJÄHRIGER LEITER DES BEREICHES INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT EINER LANDESBANK. DANEBEN ARBEITET ER ALS EXTERNER DATENSCHUTZBEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

LIEFERKETTENANGRIFFE: WENN CYBERANGRIFFE IM JAHR 2026 ÜBER GESCHÄFTSPARTNER ERFOLGEN

Cyberangriffe richten sich nicht immer direkt gegen das eigentliche Zielunternehmen. Immer häufiger nutzen Kriminelle die Lieferkette: Sie greifen Dienstleister, Softwareanbieter oder Zulieferer an – und gelangen so ins eigentliche Ziel. Fachleute sprechen von Lieferkettenangriffen oder Supply-Chain-Attacken.

Wenn der Angriff über einen Dritten kommt

Die meisten Unternehmen arbeiten mit vielen Partnern und auch IT-Systemen. Software wird von externen Herstellern bereitgestellt oder für lokal betriebene Systeme kommen Updates automatisch über das Internet. IT-Dienstleister oder auch andere Geschäftspartner können auf Systeme zugreifen oder tauschen über Onlinespeicher und Schnittstellen Daten aus.

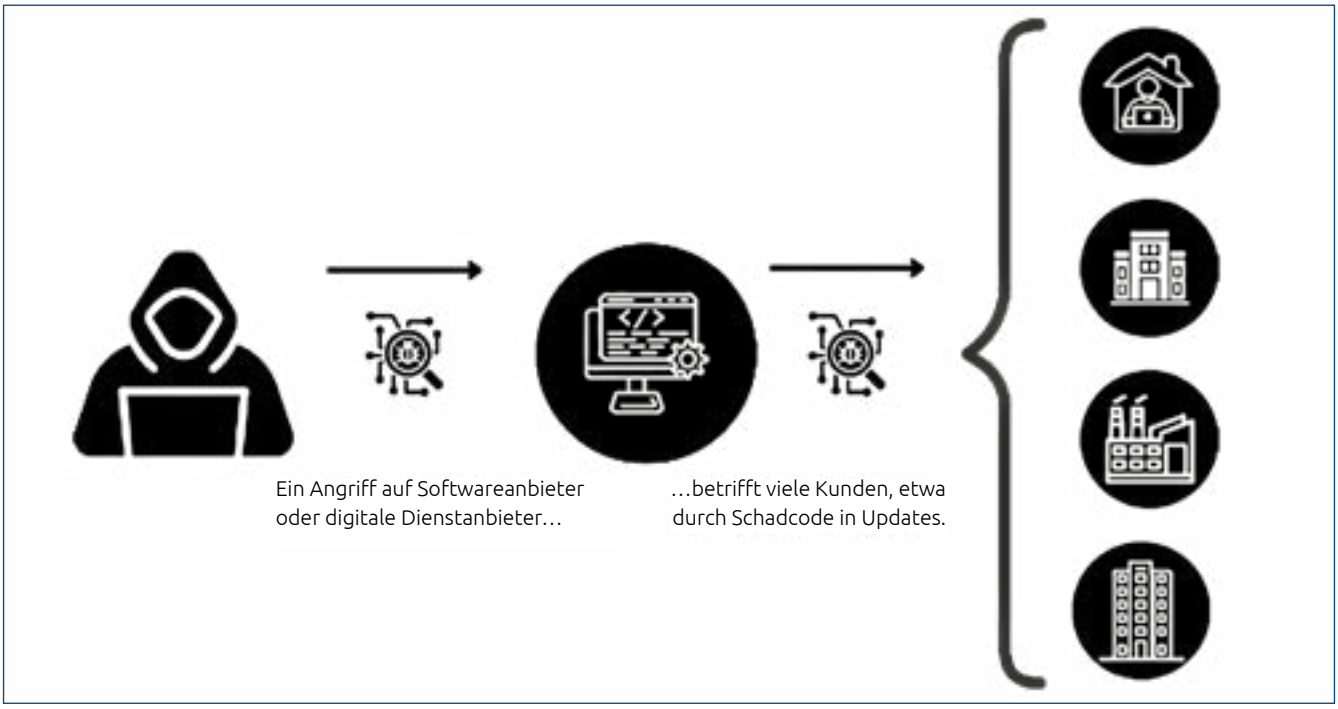
Bei Lieferkettenangriffen versuchen Angreifer häufig, genau diese Zusammenarbeit und das Vertrauen zwischen den Partnern auszunutzen. Dabei lassen sich zwei typische Vorgehensweisen beobachten:

Weg 1: Angriff über Software oder digitale Dienste

Eine Variante besteht darin, Softwareanbieter oder digitale Dienste anzugreifen, die von vielen Unternehmen – oder den gewünschten Zielunternehmen – genutzt werden. Gelingt es Angreifern, etwa Schadcode in ein Programm oder ein Softwareupdate einzuschleusen, kann sich dieser Angriff schnell auf viele Organisationen auswirken.

Ein bekanntes Beispiel ist der Angriff auf den Softwareanbieter SolarWinds, bei dem manipulierte Updates verteilt wurden. Auch Sicherheitslücken in weit verbreiteten Programmen – etwa der Dateiübertragungssoftware MOVEit – haben in der Vergangenheit zahlreiche Unternehmen gleichzeitig betroffen. Selbst scheinbar einfache Programme können dabei eine Rolle spielen. Viele Administratoren oder Entwickler nutzen etwa Programme wie Notepad++, um Konfigurationsdateien oder Skripte zu bearbeiten. Anfang 2026 wurde bekannt, dass Angreifer über den Update-Mechanismus rund um Notepad++ Schadsoftware verbreiten konnten.

Welche Unternehmen, Behörden oder Personen durch den Angriff im Anschluss betroffen sind, hängt vom jeweiligen Softwareanbieter bzw. -dienstleister ab. >



Supply Chain Attack via Software-/Diensteanbieter

> Während einige Anwendungen – wie Notepad++ – vom Selbstständigen bis hin zu Mitarbeitern in einer IT-Abteilung im Konzern genutzt werden, sind andere Angebote auf bestimmte Branchen oder Unternehmensgrößen ausgerichtet.

Weg 2: Angriff über kleinere Partner oder Zulieferer

Eine zweite Variante besteht darin, gezielt Unternehmen innerhalb der Lieferkette anzugreifen, um über diese Zugang zu einem eigentlichen Ziel zu erhalten.

Dabei konzentrieren sich Angreifer häufig auf kleinere Dienstleister oder Zulieferer des gewünschten Zielunternehmens. Der Grund ist einfach: Das oftmals größere Zielunternehmen verfügt meistens über umfangreiche Sicherheitsmaßnahmen, während die kleineren Partner oftmals weniger Ressourcen für IT-Sicherheit haben.

Wenn Angreifer es schaffen, einen solchen Partner erfolgreich anzugreifen, können sie

- Zugangsdaten stehlen,
- Wartungszugänge missbrauchen oder
- über gemeinsame Systeme in das Netzwerk des eigentlichen Zielunternehmens gelangen.

Solche Angriffe richten sich also nicht gegen das erste Opfer selbst, sondern gegen dessen Kunden oder Geschäftspartner.

Warum Lieferkettenangriffe so gefährlich sind

Lieferkettenangriffe gelten als besonders riskant, weil sie Vertrauen ausnutzen. Softwareupdates, Wartungszugriffe oder Datenübertragungen zwischen Partnern gehören zum normalen Geschäftsalltag und wirken zunächst unauffällig.

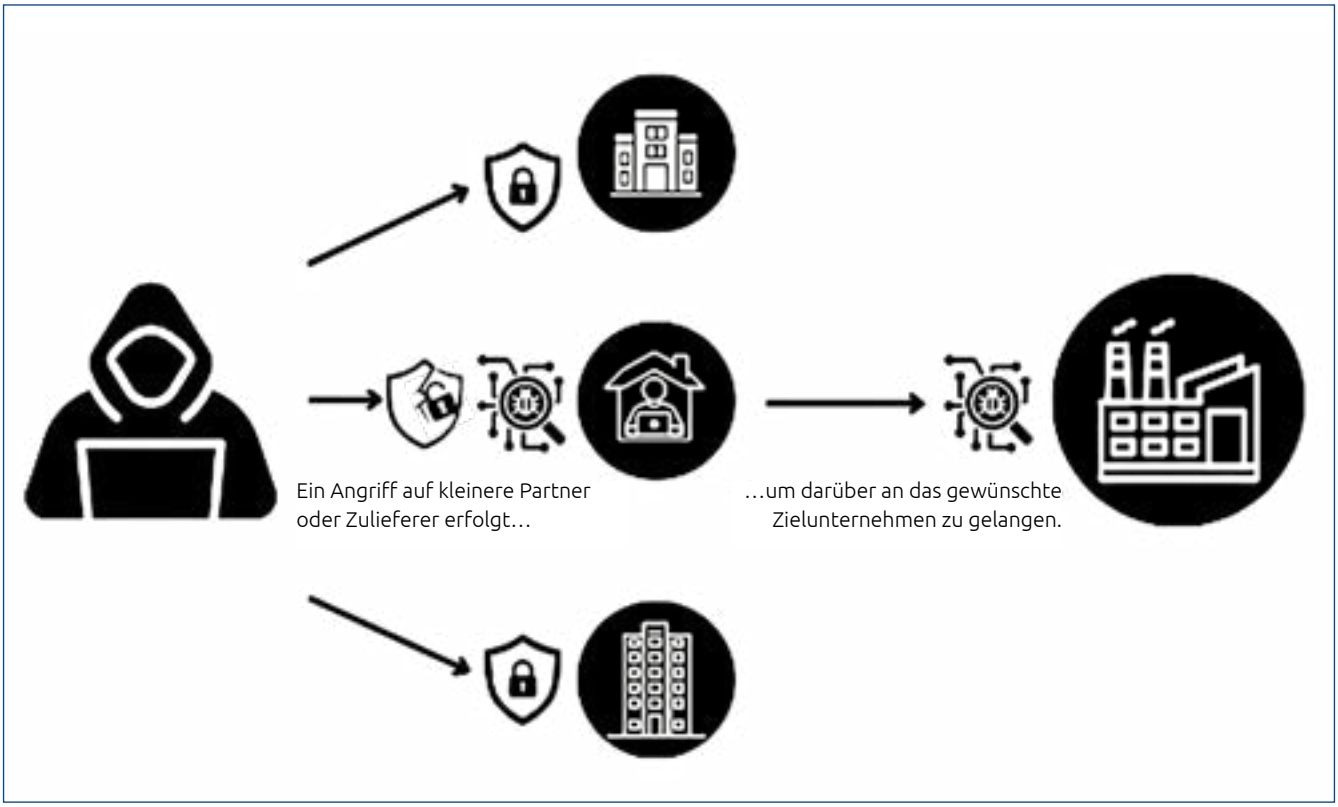
Die möglichen Folgen können jedoch erheblich sein:

- Zugriff auf interne Systeme
- Diebstahl vertraulicher Daten
- Einschleusen von Schadsoftware
- Verschlüsselung von Daten (Ransomware)
- Unterbrechung von Geschäftsprozessen

Sind dabei personenbezogene Daten betroffen, können zusätzlich Meldepflichten nach der Datenschutz-Grundverordnung entstehen.

Lieferkettensicherheit betrifft auch Geschäftspartner

Das Thema Lieferkettensicherheit betrifft nahezu alle Unternehmen. Deshalb sehen die Gesetzgeber in den



Supply Chain Attack via Zulieferer/Dienstleister

unterschiedlichsten Ländern vor, dass etwa Unternehmen bei der IT-Sicherheit auch die Lieferkette betrachten müssen.

In der EU findet sich diese Vorgabe etwa in der NIS2-Richtlinie, die in Deutschland ca. rund 30.000 Unternehmen direkt einhalten müssen. Die Erfüllung der Vorgabe – die Sicherheit in der Lieferkette zu beachten – kann in der Praxis dazu führen, dass kleinere Geschäftspartner etwa durch vertragliche Vereinbarungen verpflichtet werden, gewisse Sicherheitsanforderungen einzuhalten.

Die Auswirkungen auf Unternehmen

- **Auswirkung 1:** Für die Unternehmen haben Lieferkettenangriffe drei wesentliche Auswirkungen: Auswirkung 1: Einerseits können alle Unternehmen, die Software oder Onlinedienste nutzen, Opfer von Angriffen werden, wenn die Anbieter der Software oder des Onlinedienstes erfolgreich „gehackt" werden. Auch wenn keine weiteren Geschäftspartner infolge des Angriffs betroffen sind, kann ein solcher Angriff dazu führen, dass Kriminelle etwa Daten stehlen und verschlüsseln oder die Systeme für weiterführende Angriffe nutzen.
- **Auswirkung 2:** Ist ein Unternehmen Lieferant oder Dienstleister für ein größeres und „besser" abgesichertes Unternehmen, besteht das Risiko, dass Kriminelle das Unternehmen angreifen, um an die Daten oder Systeme des größeren Unternehmens zu gelangen.

Zudem ist es möglich, dass Kunden des Unternehmens die Sicherheit der Lieferkette gewährleisten müssen und dazu entsprechende Anforderungen stellen oder entsprechende Überprüfungen durchführen.

- **Auswirkung 3:** Nutzt man selbst die Leistungen von kleineren und eventuell schlechter abgesicherten Unternehmen, besteht das Risiko, dass Kriminelle diese Geschäftspartner angreifen, um an die Daten oder Systeme des Unternehmens zu gelangen.

Bitte nicht übersehen: Unternehmen können mehrere Rollen einnehmen – als potenzielles Ziel, als Teil der Lieferkette und als möglicher Angriffsweg für andere.

Was Unternehmen dagegen tun können

Unternehmen versuchen, das Risiko von Lieferkettenangriffen durch verschiedene Maßnahmen zu reduzieren. Dazu gehören unter anderem:

- sorgfältige Auswahl und Prüfung von Dienstleistern
- Sicherheitsanforderungen in Verträgen
- regelmäßige Updates und Sicherheitsprüfungen
- eingeschränkte Zugriffsrechte für externe Partner
- Segmentierung des Netzwerks bzw. der Systeme
- Überwachung von Systemen und Netzwerken
- Festlegung von Ansprechpartnern zur Klärung von Auffälligkeiten

Doch Technik allein reicht nicht aus – auch das Verhalten der Beschäftigten spielt eine wichtige Rolle.

Was Beschäftigte beachten sollten

Kriminelle haben nicht nur das Ziel, technische Schwachstellen, sondern auch Menschen auszunutzen. Die Angreifer versuchen dann via „Social Engineering", Beschäftigte zu überzeugen, etwa

- sensible Daten oder Zugangsdaten zu übermitteln,
- Dateien zu öffnen und auszuführen, oder
- einen Fernwartungszugang zu öffnen.

Je nach Situation geben sich die Angreifer dann etwa als Mitarbeiter des Kunden oder auch als Support-Mitarbeiter bzw. Techniker eines involvierten Unternehmens aus. Wie auch bei direkten Angriffen wird Druck aufgebaut und teilweise mit dramatischen Konsequenzen gedroht, wenn man der Aufforderung nicht nachkommt.

Um solche Angriffe abzuwehren, sollten Sie

- sich an die internen Vorgaben zur IT-Sicherheit halten,
- im Bedarfsfall über einen anderen, bekannten Kanal Rücksprache mit vertrauten Ansprechpartnern, etwa des Kunden oder IT-Anbieters, halten,
- die zuständigen Stellen im Unternehmen informieren, wenn Ihnen ungewöhnliche Aktivitäten, wie entsprechende Kontaktaufnahmen oder auch Dateien beim Datenaustausch, auffallen.

Sicherheit endet nicht am eigenen Netzwerk

Die Digitalisierung hat Unternehmen enger miteinander vernetzt als je zuvor. Daten, Software und Systeme werden heute über viele organisatorische Grenzen hinweg genutzt.

Wer aufmerksam bleibt und ungewöhnliche Situationen frühzeitig meldet, kann dazu beitragen, Schäden zu vermeiden. Denn manchmal kommt der Angriff nicht direkt von außen – sondern über die „Hintertür" der Lieferkette. (ST)

EINMAL SCANNEN, BITTE – UND SCHON SIND IHRE DATEN WEG

Stellen Sie sich vor: Sie kommen morgens ins Büro und sehen am Schwarzen Brett einen Aushang. „Neues WLAN im Konferenzraum – bitte QR-Code scannen und Zugangsdaten aktualisieren." Klingt nach IT. Klingt nach Routine. Klingt legitim.

Es scheint legitim, aber darin liegt das Problem

QR-Codes sind aus unserem Alltag nicht mehr wegzudenken. Restaurantspeisekarten, Parkscheinautomaten, Paketbenachrichtigungen – wir scannen sie, ohne groß nachzudenken. Das wissen auch Angreifer. Und sie nutzen dieses Vertrauen gezielt aus.

Was ist Quishing? Und warum ist es so gefährlich?

Der Begriff setzt sich zusammen aus QR-Code und Phishing. Das Prinzip ist dasselbe wie bei einer Betrugs-Mail. Sie werden auf eine gefälschte Webseite gelockt, um dort Ihre Zugangsdaten oder persönliche Informationen einzugeben. Der entscheidende Unterschied liegt im Weg dorthin.

Beim klassischen Phishing sehen Sie noch eine URL. Vielleicht fällt Ihnen auf, dass statt „sparkasse.de" da „sparkasse-sicherheit.net" steht. Beim QR-Code sehen Sie gar nichts. Sie scannen, Ihr Smartphone ruft die Adresse auf und erst dann landen Sie auf der gefälschten Seite. Die Prüfmöglichkeit, die bei einer URL noch existiert, fehlt hier völlig.

Mein Tipp:

Behandeln Sie jeden QR-Code wie einen unbekannten Link in einer E-Mail. Sie würden auch nicht blind auf einen Link klicken, dessen Ziel Sie nicht kennen. Beim QR-Code gilt dasselbe.

Wo begegnen Ihnen gefälschte QR-Codes im Arbeitsalltag?

Angreifer wissen genau, wo wir QR-Codes erwarten. Deshalb tauchen gefälschte Codes gezielt dort auf:

- **In E-Mails und Aushängen:** In einer scheinbar internen Nachricht werden Sie gebeten, einen Prozess per QR-Code zu bestätigen. Oder jemand hat schlicht einen Aufkleber mit einem anderen Code über den echten am Drucker geklebt.
- **Auf Paketzetteln:** Sie erhalten eine angebliche Zustellbenachrichtigung. Ein Scan führt Sie direkt auf eine gefälschte Paketdienstseite, die nach Adress- und Zahlungsdaten fragt.
- **In externen Dokumenten:** Ein QR-Code im Anhang eines Angebots führt angeblich zur Vertragsunterlage oder in Bewerbungsunterlagen vermeintlich zum Portfolio des Bewerbers.

Mein Tipp:

Fragen Sie sich bei jedem QR-Code, wer ihn dort platziert hat und warum. Fehlen ein Briefkopf, ein Name, ein Kontext? Dann ist Vorsicht angesagt.

Das Datenschutzproblem, das viele übersehen

Quishing ist nicht nur ein IT-Sicherheitsthema. Es ist auch ein Datenschutzthema. Und zwar aus einem Grund, der leicht übersehen wird.

Als Mitarbeitende haben Sie Zugang zu Kundendaten, Personalinformationen oder internen Finanzdaten. Werden Ihre Zugangsdaten gestohlen, ist damit auch der Weg zu diesen Informationen offen. Das ist eine Datenpanne im Sinne der Datenschutz-Grundverordnung. Für unser Unternehmen entsteht eine Meldepflicht gegenüber der Datenschutzaufsichtsbehörde. Und für betroffene Kunden kann ein erheblicher Schaden verursacht werden – ihre Daten könnten missbraucht oder verkauft werden.

Erschwerend kommt hinzu, dass Angreifer beim Scan Ihres Smartphones zusätzliche Informationen sammeln können: Gerätetyp, Betriebssystem, manchmal sogar Ihren ungefähren Standort. All das passiert im Hintergrund.

Mein Tipp:

Wenn Sie bemerken, auf einen gefälschten QR-Code hereingefallen zu sein, informieren Sie sofort die IT und mich als Datenschutzbeauftragten. Wir haben gesetzliche Fristen, innerhalb derer wir handeln müssen. Keine Panik – aber keine Zeit verlieren.

Wie erkenne ich einen gefährlichen QR-Code?

Eine 100%ig sichere Erkennungsmethode gibt es nicht – aber klare Warnsignale:

- Prüfen Sie nach dem Scannen zuerst die angezeigte URL, bevor Sie irgendwas antippen. Die meisten Smartphones zeigen kurz die Zieladresse an. Nehmen Sie sich diese zwei Sekunden. Passt die Adresse zum erwarteten Absender? Oder erscheint da etwas völlig Unbekanntes?
- Seien Sie besonders misstrauisch, wenn die aufgerufene Seite nach Zugangsdaten oder Passwörtern fragt. Eine legitime interne Seite wird Sie niemals via QR-Code zur Passworteingabe auffordern.
- Und wenn ein QR-Code auf einem Aufkleber abgebildet ist, der offensichtlich über etwas anderem sitzt – lassen Sie die Finger davon.

Mein Tipp:

Im Zweifelsfall einfach kurz anrufen. Kommt der Code angeblich von der IT? Rufen Sie die IT an. Ein Anruf kostet 30 Sekunden. Ein Datenverlust kann Wochen kosten.

Was tun, wenn ich doch gescannt habe?

Ruhig bleiben. Und dann zügig handeln.

Wenn Sie Zugangsdaten eingegeben haben, ändern Sie Ihr Passwort sofort. Informieren Sie die IT-Abteilung. Die können prüfen, ob der Account bereits kompromittiert wurde. Und informieren Sie mich, damit wir gemeinsam beurteilen können, ob ein meldepflichtiger Datenschutzvorfall vorliegt.

Vor allem gilt: nichts verheimlichen. Je länger ein Angreifer Zeit hat, desto mehr Schaden richtet er an. Frühes Melden ist kein Fehler. Es ist das Richtige.

Ihre Checkliste gegen Quishing: 6 Maßnahmen, die Sie beachten müssen

1. Scannen Sie QR-Codes nur, wenn Sie die Quelle eindeutig kennen.
2. Prüfen Sie nach dem Scannen immer die angezeigte URL, bevor Sie die Seite öffnen.
3. Geben Sie niemals Zugangsdaten auf einer Seite ein, die Sie über einen QR-Code erreicht haben, ohne die URL geprüft zu haben.
4. Melden Sie unbekannte QR-Codes an Aushängen oder auf Geräten sofort der IT.
5. Scannen Sie auf Dienstgeräten keine QR-Codes aus privaten oder unbekannten Quellen.
6. Bei Verdacht oder Vorfall: IT und Datenschutzbeauftragten sofort informieren.

Fazit: 2 Sekunden, die alles verändern

QR-Codes sind praktisch. Das bleibt so. Aber praktisch bedeutet nicht automatisch sicher. Es reicht, kurz innezuhalten. Zwei Sekunden Prüfung statt blindem Scan. Eine kurze Rückfrage statt sofortiger Aktion. Datensicherheit und Datenschutz hängen hier unmittelbar zusammen – denn Ihre Zugangsdaten sind der Schlüssel zu unseren Kundendaten.

Ihr Datenschutzbeauftragter (AH)

WUSSTEN SIE SCHON?

QR-Code-Angriffe haben seit 2023 massiv zugenommen. Das Bundesamt für Sicherheit in der Informationstechnik warnt ausdrücklich vor der wachsenden Verbreitung von Quishing in Deutschland. Besonders betroffen sind Unternehmen, deren Mitarbeitende regelmäßig mit externen Dienstleistern oder Paketlieferungen zu tun haben.

Ein häufig unterschätzter Faktor ist das Smartphone selbst. Auf dem Mobilgerät ist die vollständige URL nach dem Scan schwerer zu erkennen als auf einem Desktop-Computer. Angreifer wissen das und optimieren ihre gefälschten Seiten gezielt für die mobile Ansicht.

Die einfachste Schutzmaßnahme, die kaum jemand kennt: Viele Smartphones erlauben es, die URL-Vorschau nach dem Scan anzuzeigen, bevor die Seite geöffnet wird. Prüfen Sie in Ihren Geräteeinstellungen, ob diese Funktion bei Ihnen aktiv ist. Zwei Sekunden Einrichtungsaufwand. Dauerhafter Schutz. (AH)

PRIVATSPHÄRE & SICHERHEIT IN SOCIAL MEDIA

In diesem Video geht es um ein Thema, welches viele vermutlich eher als „privat“ einordnen – aber welches dennoch erhebliche Auswirkungen auf das Unternehmen haben kann: **die Nutzung von Social Media.** Privatsphäre & Sicherheit in Social Media – kleine Postings – große Wirkung.

Ich habe die Ausgabe von Privacy@Work gelesen:

Name, Vorname, Abteilung	Unterschrift

Bei Fragen im Bereich Datenschutz wenden Sie sich bitte an Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten!

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autoren: Andreas Hessel, Sebastian Tausch, Produktmanagement: Lisa Suchy, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte S. 1: Tithi – AdobeStock.com, S. 3+4: Sebastian Tausch, Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 16-mal pro Jahr; Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier