Hinter den Kulissen:

Cybersicherheit für KMU

Wie digitale Banditen Ihr Unternehmen stilllegen – und wie Sie sich ohne eigene IT-Abteilung wirksam schützen



PRAXISHANDBUCH FÜR DEN MITTELSTAND

Hinter den Kulissen: Cybersicherheit für KMU

Wie digitale Banditen Ihr Unternehmen stilllegen – und wie Sie sich ohne eigene IT-Abteilung wirksam schützen

Harald de Vries

linkedin.com/in/harald-de-vries

CEO KMU.NETWORK & Strategic Advisor der
BFC - Bundesvereinigung für Cybersicherheit e.V.
(www.bfc.foundation)

Das Buch entstand mit Unterstützung von Klaus-Dieter Rommeiss und Sebastian Bing, Mitglieder des Vorstandes der BFC e.V.
und Wolfgang Röhr

KMU.BIBLIOTHEK

© Copyright 2027 - Harald de Vries - Alle Rechte vorbehalten.
VR-Publishing House Ltd.
27 Old Gloucester Street
London, UK
WC1N 3AX
Telefon: +44 845 891 0231

Lektorat: Mary Vaughan
Redaktion: Torsten Windmill
Korrektor: Christin Kirsch
Covergestaltung: VR-Cover - London
Covermotiv: © NUN3H
Alle Cartoons: © NUN3H
1. Auflage Januar 2027

Copyright Hinweis

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne ausdrückliche Zustimmung des Autors nicht zulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Einspeicherung und Verarbeitung in elektronischen Systemen. Dieses Buch entstand unter Nutzung moderner digitaler Werkzeuge zur Recherche, Strukturierung, Illustration und redaktionellen Ausarbeitung. Die Auswahl, inhaltliche Verantwortung, redaktionelle Prüfung und finale Gestaltung liegen vollständig beim Autor.

Haftungsausschluss

Dieses Buch wurde mit größtmöglicher Sorgfalt erstellt. Dennoch übernehmen die Autoren keinerlei Gewähr für die Aktualität, Richtigkeit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, welche durch die Nutzung oder Nichtnutzung der dargebotenen Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens der Autoren kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.

Die im Buch beschriebenen Technologien, Vorgehensweisen und Empfehlungen stellen keine verbindliche Beratung oder rechtliche Auskunft dar. Leserinnen und Leser werden ausdrücklich dazu aufgefordert, vor Umsetzung der beschriebenen Maßnahmen gegebenenfalls fachlichen Rat einzuholen und eigenverantwortlich zu handeln.Die Verwendung der im Buch genannten Marken- und Produktnamen dient ausschließlich der Veranschaulichung und stellt keine Markenrechtsverletzung dar. Alle genannten Marken- und Warenzeichen gehören ihren jeweiligen Eigentümern.

Inhaltsverzeichnis

Vorwort: Montag, 7:42 Uhr – Der Betrieb steht (Und warum dieses Buch Ihr Unternehmen retten kann)

Wenn im Großhandel die Lkw auf dem Hof bleiben und der Handwerksbetrieb an keinen Kundenauftrag mehr herankommt • Der gefährlichste Irrtum im Mittelstand: „Wer will schon in unsere kleine Firma?“ • Ein Wort aus der Praxis

TEIL 1: Die Trickbetrüger an der Vordertür (Psychologie, Täuschung & E-Mail-Fallen)

Kapitel 1: Phishing – Wenn die Mail aussieht wie immer (Der Wolf im Schafspelz)

Wie modernes Phishing funktioniert • Gefährliche Anhänge und gefälschte Anmeldelinks • Aus der Praxis: Steuerbüro und Autohaus • Was passiert eigentlich, wenn ich nur ganz kurz auf den Link klicke?

Kapitel 2: „Der falsche Chef kennt Ihren Namen. Das nennt man Social Engineering.“

Social Engineering einfach erklärt • Ausspähung (Reconnaissance & OSINT) • Pretexting (Die erfundene Geschichte) • Aus der Praxis: Der falsche IT-Helfer und der perfekte Bewerber • Was passiert eigentlich mit unserem Organigramm auf der Webseite?

Kapitel 3: Bitte heute noch überweisen! – CEO-Fraud, manipulierte Rechnungen & KI-Stimmen

CEO-Fraud (Die Chef-Masche) • Falsche Bankverbindungen (Man-in-the-Middle) • Deepfakes und KI-Stimmen am Telefon • Aus der Praxis: Baustoffhändler und Tagungshotel • Was passiert eigentlich, wenn ein Betrüger heimlich im Postfach mitliest?

TEIL 2: Die Einbrecher an der Hintertür (Technik, Erpresser-Industrie, Geräte & Vernetzung)

Kapitel 4: Wer hat hier eigentlich einen Schlüssel? – Passwörter, Zugänge & der zweite Riegel

Warum „Sommer2026!“ kein Tresor ist • Gefahr von Sammel-Logins und alten Mitarbeiter-Zugängen • Passwort-Manager & Zwei-Faktor-Authentifizierung (2FA) • Aus der Praxis: Arztpraxis und Maschinenbauer • Was passiert eigentlich bei einem Datenleck im Darknet?

Kapitel 5: Ransomware – Digitale Geiselnahme und das gekidnappte Firmennetzwerk

Erpressungstrojaner einfach erklärt • Doppelte Erpressung und Erpressung ohne Verschlüsselung • Aus der Praxis: Nischenzulieferer und Logistikbetrieb • Was passiert eigentlich in den ersten 60 Sekunden nach der Infektion?

Kapitel 6: Die dunkle Industrie – Pranger-Webseiten, faule Bluffs und warum die KI niemals schläft

Verbrechen als Franchise-System (Ransomware-as-a-Service) • Am digitalen Pranger (Dedicated Leak Sites) • Einschüchterung & Bluff erkennen • Warum die KI niemals schläft • Aus der Praxis: Zulieferer-Schreck und Countdown-Bluff

Kapitel 7: Das Update, das immer „morgen“ kommt – und wenn der Büro-PC die Werkhalle mitreißt

Warum Software-Updates frischer Beton für Risse im Fundament sind • Vergessene Fernwartungszugänge • Wenn Büro und Werkhalle ungetrennt verbunden sind • Aus der Praxis: Bauunternehmen, Möbelhändler und Metallbetrieb

Kapitel 8: Der Laptop sitzt noch im Zug – Homeoffice, Privatgeräte & offene Cloud-Links

Verlorene Notebooks und Festplattenverschlüsselung • Das Risiko von Privatgeräten und Schatten-IT • Offene Scheunentore in der Cloud • Aus der Praxis: Personalberatung, Werbeagentur und Architekturbüro

TEIL 3: Das Schutzschild für Ihren Betrieb (Mensch, Schulung, Backup & Dienstleister)

Kapitel 9: Die menschliche Firewall – Monatliche Mitarbeiterschulung & saubere Dokumentation

Warum die Einmal-Belehrung verpufft • Das 15-Minuten-Prinzip • Dokumentationspflicht für Geschäftsführer, DSGVO und Versicherung • Aus der Praxis: Reisebüro und Elektrobetrieb

Kapitel 10: „Gut, dass Sie angerufen haben!“ – Fehlerkultur im Ernstfall

Warum Scham der beste Freund des Hackers ist • Die „Keine-Strafe-bei-Sofortmeldung“-Regel • Aus der Praxis: Der Lehrling im Elektrohandwerk • Was passiert eigentlich in 24 Stunden Schweigen im Netzwerk?

Kapitel 11: Ein Backup ist erst beim Zurückholen etwas wert – Ihre digitale Zeitmaschine

Warum eine angesteckte Festplatte mitverschlüsselt wird • Die 3-2-1-Regel • Der Wiederherstellungs-Test mit der Stoppuhr • Aus der Praxis: Druckerei und Onlinehändler

Kapitel 12: Was macht eigentlich unser IT-Dienstleister? – Und wann zahlt die Cyber-Versicherung?

Zuruf-Feuerwehr vs. Sicherheitsvertrag • Cyber-Versicherungen im Klartext • Aus der Praxis: Pflegedienst und Spedition am Wochenende

TEIL 4: Wenn es ernst wird – Krisenmanagement & der 90-Tage-Fahrplan

Kapitel 13: Die ersten 60 Minuten – Der rote Notfallknopf, die Kundenkommunikation und der Wiederanlauf

Isolieren statt Ausschalten • Die Kunden-Erstmeldung und die 72-Stunden-DSGVO-Frist • Reihenfolge für den Wiederanlauf • Soforthilfe über die Bundesvereinigung für Cybersicherheit e.V.

Kapitel 14: Was schaffen wir in 90 Tagen? – Ihr machbarer Schutz-Fahrplan ohne IT-Abteilung

Das 80/20-Prinzip • Der konkrete Stufenplan für 30, 60 und 90 Tage • Die 60-Minuten-Trockenübung am Dienstagmittag

TEIL 5: Der große Praxis-Werkzeugkasten & Anhang

Anhang A: Das „Kein-IT-Chinesisch“-Glossar

Anhang B: Die Sammel-Checklisten zum Abhaken

Anhang C: Kopiervorlagen & Arbeitshilfen zum Ausfüllen

Anhang D: Die ultimative KMU-Tool-Liste (nach Aufgaben sortiert)

Nachwort: Warum sich der nächste Notfall am besten an einem ganz normalen Dienstag üben lässt

Danksagung • Über den Autor: Harald de Vries • Kontakt, Anlaufstellen & Notfall-Ressourcen



Vorwort: Montag, 7:42 Uhr – Der Betrieb steht (Und warum dieses Buch Ihr Unternehmen retten kann)

Montagmorgen, 7:42 Uhr. Die Kaffeemaschine im Aufenthaltsraum gibt ihr gewohntes, leicht asthmatisches Röcheln von sich. Draußen auf dem Hof rangiert bereits der erste Sattelzug rückwärts an die Laderampe, und das Piepen des Rückwärtsgangs mischt sich mit dem Geräusch von klappernden Kaffeetassen. Es verspricht eine gute, produktive Woche zu werden.

Dann ruft der Lagerleiter aus dem Erdgeschoss nach oben: „Du, Chef? Der Drucker an der Rampe spuckt nichts aus. Ich kriege die Lieferscheine für die Frühschicht nicht raus."

Sie seufzen innerlich, nehmen einen Schluck Kaffee und gehen an Ihren eigenen Schreibtisch, um kurz im System nachzusehen. Wahrscheinlich hängt nur wieder die Warteschlange vom Netzwerkdrucker. Sie bewegen die Maus. Der Bildschirm erwacht aus dem Standby – doch statt Ihrer gewohnten Auftragsübersicht blickt Ihnen ein grelles, rotschwarzes Textfenster entgegen. Darin steht in holprigem, aber unmissverständlichem Englisch, dass sämtliche Dateien Ihres Unternehmens militärisch verschlüsselt wurden. Darunter tickt ein digitaler Countdown rückwärts: 71 Stunden, 58 Minuten, 12 Sekunden.

Ab diesem Moment ist Ihr Arbeitstag vorbei. Genauer gesagt: Ihr regulärer Geschäftsbetrieb ist vorbei.

Fallbeispiel 1: Wenn 40 Tonnen Stahl an einem Blatt Papier scheitern

Schauen wir uns an, wie das in der echten Welt aussieht. Vor einiger Zeit traf es einen mittelständischen Großhändler für Gastronomie- und Gebäudebedarf. Ein grundsolider Betrieb: 38 Mitarbeitende, sechs eigene Lkw, ein Hochregallager voller Paletten und ein Chef, der sein Geschäft von der Pike auf gelernt hatte.

An jenem Montagmorgen standen die Lkw abfahrbereit auf dem Hof. Die Ware war da, die Fahrer saßen im Führerhaus, der Diesel war bezahlt und die Kunden warteten auf ihre Lieferungen. Doch die Lkw bewegten sich keinen Millimeter vom Fleck. Warum? Weil das Lagerprogramm gesperrt war. Niemand wusste, auf welchem Regalplatz welche Palette lag, welche Bestellungen überhaupt kommissioniert werden mussten und – selbst wenn man die Kartons blind aufgeladen hätte – niemand konnte einen Lieferschein oder ein Frachtpapier drucken. Ohne Lieferschein nimmt aber kein größerer Kunde an seiner Rampe Ware an.

Der Fehler: Der Unternehmer hatte jahrelang gedacht, ein Ausfall der Computer bedeute lediglich, dass die Buchhaltung eben mal zwei Tage lang keine Rechnungen schreiben könne. Er hatte übersehen, dass seine gesamte physische Logistik an einem einzigen zentralen Server hing, von dem es zwar eine Datensicherung gab – diese steckte aber dauerhaft per Kabel am selben Server und wurde von den Erpressern gleich mitverschlüsselt.

Die Lösung: Erst nach vier schmerzhaften Tagen Stillstand, in denen ein eilig gerufener Notfall-Experte das System komplett neu aufsetzen musste und die Mitarbeiter mit Klemmbrettern, Kulis und telefonischen Zurufen improvisierten, rollten die ersten Lkw wieder. Heute hat dieser Betrieb nicht nur ein vom Netzwerk getrenntes Backup, sondern im Schrank des Lagerleiters liegt eine wasserfeste Box. Darin: Ein USB-Stick (und ein ausgedruckter Ordner) mit den Standard-Tourenplänen der wichtigsten Stammkunden und ein Block Blanko-Lieferscheine mit Durchschlag. Wenn heute der Server ausfällt, rollen die Lkw um 8:00 Uhr trotzdem vom Hof.

Fallbeispiel 2: Drei volle Auftragsbücher, aber kein einziger Straßenname

Ein zweites Beispiel zeigt, dass man keine große Lagerhalle braucht, um kalt erwischt zu werden. Ein kleiner Handwerksbetrieb für Sanitär- und Heizungstechnik mit neun Beschäftigten hatte über Monate hinweg vorbildlich auf „digital“ umgestellt. Weg mit der Zettelwirtschaft! Alle Kundentermine, Ersatzteillisten, Wartungsprotokolle und Anfahrtsadressen liefen über eine Cloud-App direkt auf die Tablets der Monteure.

An einem Dienstagmorgen wollten sich die sechs Gesellen auf den Weg zu den Baustellen machen, doch ihre App verlangte plötzlich ein neues Passwort. Auch im Büro kam die Chefin nicht mehr in das Verwaltungskonto hinein. Der Grund: Jemand hatte auf eine täuschend echt aussehende E-Mail des Software-Anbieters geklickt und dort gutgläubig die Zugangsdaten eingegeben. Die Angreifer hatten das Konto übernommen, das Passwort geändert und verlangten nun Geld für die Freigabe.

Der Betrieb erreichte zwar seine Monteure noch über deren Handys, kam aber an keinen einzigen Kundenauftrag mehr heran. Die Gesellen saßen in ihren vollgepackten Transportern und wussten schlichtweg nicht, zu welchen Kunden sie an diesem Tag fahren sollten.

Der Fehler: Das gesamte Wissen über die laufende Woche befand sich an einem einzigen digitalen Ort, der nur durch ein simples Passwort geschützt war – ohne zweiten Sicherheitsriegel (Zwei-Faktor-Authentifizierung).

Die Lösung: Mithilfe des Software-Herstellers und einer Identitätsprüfung per Personalausweis konnte der Zugang nach anderthalb Tagen zwar zurückerobert werden, aber sechs Monteure anderthalb Tage lang fürs Däumchendrehen im Transporter zu bezahlen, tut weh. Heute ist das Konto durch einen zweiten Code auf dem Handy der Chefin gesichert, und jeden Freitagnachmittag um 15:00 Uhr wird der Wochenplan für die kommende Woche einmal automatisch als PDF gespeichert und zweimal ausgedruckt an das Schwarze Brett in der Werkstatt geheftet. Kostet drei Cent Papier und rettet im Ernstfall die ganze Woche.

Der gefährlichste Satz im deutschen Mittelstand

Wenn ich als Strategic Advisor der BFC - Bundesvereinigung für Cybersicherheit e.V. oder im Rahmen meiner Arbeit bei KMU.NETWORK mit Unternehmerinnen und Unternehmern spreche, höre ich in den ersten fünf Minuten fast immer denselben Satz. Er wird meist mit einem entspannten Lächeln vorgetragen und lautet:

> *„Ach, Herr de Vries, wir sind ein kleiner Betrieb mit zwölf Leuten auf dem platten Land. Wer will denn schon in unsere Firma? Bei uns gibt es doch keine Staatsgeheimnisse zu holen!“*

Dieser Satz ist menschlich absolut verständlich. Er beruht auf unserer Erfahrung aus der echten, greifbaren Welt: Ein Einbrecher mit Brechstange und Sturmhaube überlegt sich vorher genau, in welches Haus er einsteigt. Er beobachtet die Nachbarschaft, schaut, wo der Porsche in der Einfahrt steht, und wägt ab, ob sich das Risiko lohnt, für Opas alte Kuckucksuhr im Gefängnis zu landen. Für Ihre kleine Werkstatt oder Ihr Büro im Gewerbegebiet reist kein Meisterdieb extra aus Osteuropa oder Übersee an.

Im Internet gelten jedoch völlig andere Naturgesetze.

Stellen Sie sich Cyberkriminelle nicht wie Einbrecher mit einer Brechstange vor, die nachts gezielt vor Ihrem Hoftor stehen. Stellen Sie sich Cyberkriminelle wie industrielle Schleppnetzfischer auf dem offenen Ozean vor.

Einem Schleppnetzfischer ist es völlig egal, wie Sie heißen, wie viele Mitarbeiter Sie haben oder ob Sie Schrauben, Brötchen oder Steuererklärungen produzieren. Er lässt ein zehn Kilometer breites, vollautomatisches Netz ins Wasser und zieht es einmal komplett durch das digitale Meer. Dieses Netz besteht aus Millionen automatisierter E-Mails und kleiner Suchprogramme, die rund um die Uhr Milliarden von Internetanschlüssen abklopfen – völlig kostenlos und ohne dass ein Mensch dafür auch nur eine Taste drücken muss.

Wenn Ihr Betrieb ein offenes Kellerfenster hat (zum Beispiel ein schwaches Passwort oder ein vergessenes Update) oder ein Mitarbeiter im Alltagsstress nach dem glitzernden Köder schnappt, hängen Sie im Netz. Erst nachdem Sie im Netz zappeln, schaut ein Programm – oder ein Handlanger der Bande – kurz nach, wer da eigentlich gefangen wurde: „Aha, ein mittelständisches Ingenieurbüro mit sieben Beschäftigten. Jahresumsatz geschätzt eine Million Euro. Wunderbar, von denen verlangen wir 25.000 Euro Lösegeld."

Für die Angreifer sind gerade kleine und mittlere Unternehmen (KMU) die perfekte Beute:

1. **Sie haben genug Geld (oder eine Existenz zu verlieren):** Anders als eine Privatperson, die für ihre Urlaubsfotos keine 15.000 Euro zahlt, steht bei Ihnen sofort der Betrieb still. Jeder Tag ohne Kasse, ohne Produktion und ohne Aufträge kostet Sie bares Geld.
2. **Sie haben keine eigene IT-Abteilung:** Konzerne wie die Deutsche Bank oder Siemens beschäftigen ganze Hundertschaften von Sicherheitsexperten, die 24 Stunden am Tag auf blinkende Monitore starren. Sie hingegen haben wahrscheinlich einen externen IT-Dienstleister, der kommt, wenn der Server raucht, oder einen technikaffinen Mitarbeiter, der „das mit den Computern" nebenbei mitmacht.

Was passiert eigentlich, wenn … ein Angriff heute gar nicht mehr von einem Menschen ausgeführt wird?

Vielleicht haben Sie im Kino schon einmal gesehen, wie ein Hacker dargestellt wird: Ein blasser Teenager im Kapuzenpullover sitzt in einem abgedunkelten Keller, trinkt Energy-Drinks und hämmert wie besessen grüne Buchstabenkolonnen in eine schwarze Konsole, bis auf dem Bildschirm „Zugang gewährt“ blinkt.

Vergessen Sie dieses Bild. Wenn ein Krimineller heute von Hand tippen müsste, um in Ihre Firma einzubrechen, wären Sie ziemlich sicher.

Was tatsächlich passiert, wenn Ihre Firmen-E-Mail-Adresse oder Ihr Firmenserver im Internet sichtbar ist: Vollautomatische Software-Roboter (sogenannte Bots), die heute zunehmend mit Künstlicher Intelligenz gefüttert werden, prüfen Ihre digitale Haustür im Millisekundentakt. Während Sie und Ihre Belegschaft am Freitagabend um 18:00 Uhr verdient ins Wochenende gehen, das Licht ausschalten und den Grill anwerfen, schläft die Software der Angreifer nicht.

Sie probiert an einem einzigen Wochenende völlig geräuschlos zehntausende gestohlene Passwort-Kombinationen an Ihrem E-Mail-Postfach oder Ihrem Fernwartungszugang aus. Findet das Programm am Samstagmorgen um 3:14 Uhr eine offene Tür, schlägt es nicht sofort Krach. Es setzt einen kleinen digitalen Fuß in den Türspalt, schaut sich in aller Ruhe um, sucht nach Ihren Datensicherungen, kopiert Ihre wichtigsten Kunden- und Konstruktionsdaten auf einen fremden Server – und dreht erst am Montagmorgen um 7:30 Uhr, kurz bevor Ihre Frühschicht den Hof betritt, alle Schlösser

Warum dieses Buch anders ist (Das „Kein-IT-Chinesisch“-Versprechen)

Wenn Sie bisher versucht haben, sich über Cybersicherheit zu informieren, sind Sie vermutlich nach zehn Minuten entnervt ausgestiegen. Meistens wirft man Ihnen dort Begriffe wie Zero-Day-Exploit, Asymmetrische Ende-zu-Ende-Kryptografie, DNS-Spoofing oder Endpoint Detection and Response an den Kopf – garniert mit dem Vorwurf, Sie seien selbst schuld, wenn Sie das nicht längst eingerichtet haben.

Ich mache Ihnen heute ein Versprechen: **In diesem Buch gibt es kein theoretisches IT-Kauderwelsch.**

Sie müssen kein Kfz-Mechatroniker sein und nicht wissen, wie das Einspritzventil eines Dieselmotors im Detail berechnet wird, um sicher Auto zu fahren, den Sicherheitsgurt anzulegen und im Winter rechtzeitig Winterreifen aufzuziehen. Genauso wenig müssen Sie Informatik studiert haben, um Ihr Unternehmen vor 95 Prozent aller digitalen Banditen zu schützen.

Als Unternehmer und Strategic Advisor der Bundesvereinigung für Cybersicherheit e.V. erlebe ich jeden Tag beide Seiten: Ich sehe die Betriebe, die nach einem Angriff vor dem Nichts stehen, weil einfachste Grundregeln fehlten. Und ich sehe die Betriebe, bei denen die Angreifer sich die Zähne ausbeißen und frustriert weiterziehen – nicht etwa, weil diese Firmen Millionen für Weltraum-Technik ausgegeben hätten, sondern weil der Chef oder die Chefin ein paar glasklare, bodenständige Regeln im Alltag verankert hat.

Genau darum geht es auf den nächsten Seiten:

Wie die Trickbetrüger heute wirklich arbeiten: Wir schauen uns gemeinsam an, wie Angriffe von der gefälschten Rechnung und dem falschen Anruf im Büro über geknackte Passwörter bis hin zur großen Erpresser-Industrie im Darknet ablaufen.

Echte Geschichten aus dem Betriebsalltag: Sie lesen in jedem Kapitel konkrete Fallbeispiele von Handwerkern, Händlern, Praxen, Dienstleistern und Produzenten – inklusive der Fehler, die dort passiert sind, und wie sie pragmatisch gelöst wurden.

Werkzeuge, die im echten Leben funktionieren: Sie erfahren, wie Sie Ihre Mitarbeiter mindestens einmal im Monat in nur 15 Minuten so schulen, dass niemand mehr auf faule Tricks hereinfällt (und wie Sie das sauber dokumentieren, damit Ihnen im Ernstfall weder das Gesetz noch Ihre Versicherung einen Strick daraus dreht).

Sie brauchen für dieses Buch keinen Schraubenzieher und kein Programmierhandbuch. Ein Textmarker, ein Kugelschreiber und Ihr gesunder Menschenverstand als Unternehmer reichen völlig aus.

Bevor wir gleich in Kapitel 1 den ersten Trickbetrüger an Ihrer digitalen Vordertür entlarven, lade ich Sie ein, direkt hier die erste, vielleicht wichtigste Übung dieses Buches zu machen. Sie dauert keine fünf Minuten.

Herzlichst,

Harald de Vries

CEO KMU.NETWORK | Strategic Advisor der BFC - Bundesvereinigung für Cybersicherheit e.V.

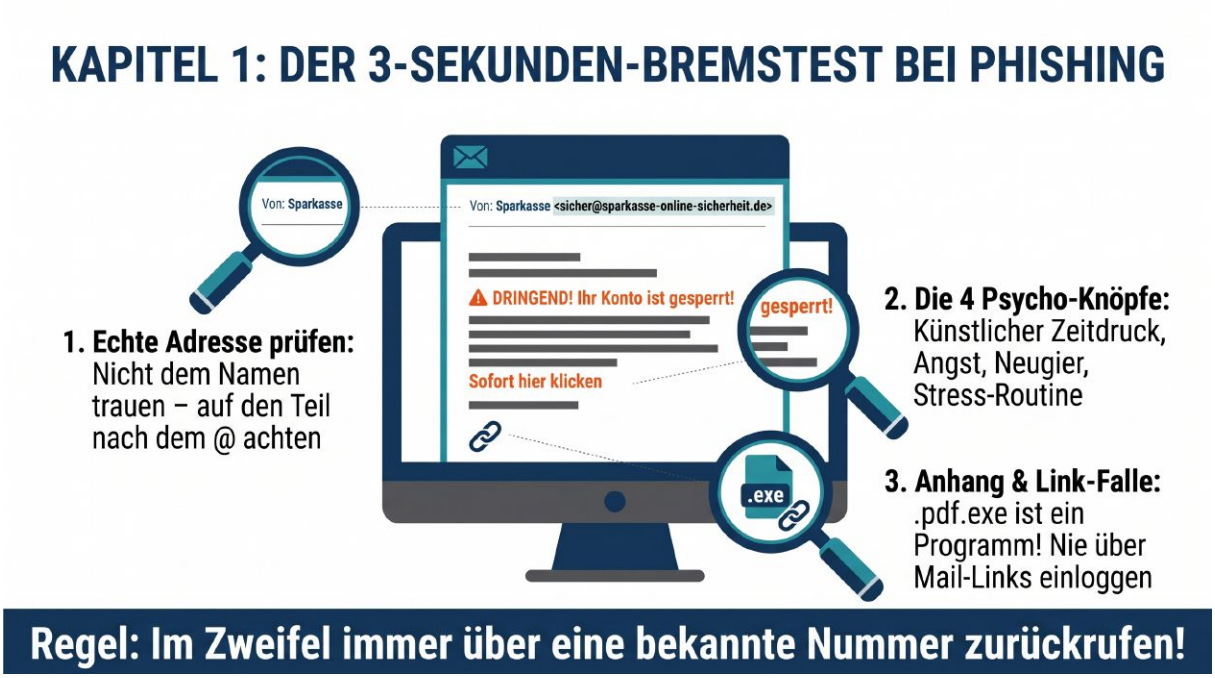
Checkliste & Aufgabe für Ihren Betrieb (Zum direkten Abhaken vor Kapitel 1)

Nehmen Sie sich einen Stift oder ein Blatt Papier und beantworten Sie ehrlich diese drei kurzen Punkte für Ihr Unternehmen, bevor Sie weiterblättern:

- ☐ **Die 3 Überlebens-Abläufe notieren:** Schreiben Sie die drei konkreten Abläufe in Ihrem Betrieb auf, die am Montagmorgen um 8:00 Uhr unter allen Umständen zuerst weiterlaufen müssen, damit Sie arbeitsfähig sind (z. B. 1. Lieferscheine/Versand im Lager, 2. Zugriff auf den Terminkalender der Monteure, 3. Kasse/Telefonanlage).
- ☐ **Das Preisschild eines Ausfalltages berechnen:** Überschlagen Sie einmal grob auf der Rückseite eines Briefumschlags, was Sie ein einziger Tag kompletter Stillstand kostet (laufende Löhne ohne Umsatz + verärgerte Kunden + Nacharbeitskosten + Vertragsstrafen). Multiplizieren Sie diese Zahl mit 5 (der durchschnittlichen Dauer kleinerer Ausfälle). Diese Summe ist der Grund, warum sich jede Minute Lesezeit in diesem Buch für Sie bezahlt macht.
- ☐ **Die „Chef-Frage“ klären:** Wissen Sie heute spontan, wen Sie am Samstagabend um 21:00 Uhr anrufen können, wenn auf Ihrem Firmenrechner plötzlich gar nichts mehr geht – und haben Sie diese Telefonnummer irgendwo auf echtem Papier stehen (nicht nur im Computer gespeichert)?

TEIL 1: Die Trickbetrüger an der Vordertür

Psychologie, Täuschung & E-Mail-Fallen



Kapitel 1: Phishing – Wenn die Mail aussieht wie immer (Der Wolf im Schafspelz)

Wenn vor zwanzig Jahren ein Betrüger versuchte, Ihnen per E-Mail das Geld aus der Tasche zu ziehen, war das meistens recht unterhaltsam. Sie bekamen eine Nachricht von einem angeblichen nigerianischen Prinzen oder einem schwerreichen Onkel aus Übersee, der dringend 45 Millionen Dollar außer Landes schaffen musste und ausgerechnet Ihr Firmenkonto als Zwischenlager auserkoren hatte. Geschrieben war das Ganze in einem Deutsch, als hätte jemand ein englisches Wörterbuch in einen Mixer geworfen. Niemand bei klarem Verstand hat darauf geklickt. Wir haben darüber geschmunzelt, auf „Löschen“ gedrückt und uns sicher gefühlt.

Das Problem ist: Viele Unternehmer glauben insgeheim immer noch, dass betrügerische E-Mails – in der Fachsprache Phishing (abgeleitet vom englischen Wort Fishing, also dem „Angeln“ nach Passwörtern und Daten mit einem falschen Köder) genannt – so aussehen.

In der Realität haben die digitalen Banditen inzwischen Deutsch gelernt. Mehr noch: Sie nutzen heute dieselben Programme für Künstliche Intelligenz wie moderne Werbeagenturen. Eine heutige Phishing-Mail enthält keine Rechtschreibfehler mehr. Sie trägt das gestochen scharfe Logo Ihres Paketdienstes, Ihrer Hausbank, der Deutschen Telekom oder Ihres Steuerberaters. Sie verwendet exakt die gewohnte Schriftart, die richtige Grußformel und kommt genau in dem Moment, in dem Sie ohnehin auf eine Lieferung oder eine Abrechnung warten. Die Mail sieht aus wie immer. Und genau deshalb ist sie heute das gefährlichste Einfallstor für den gesamten Mittelstand.