INCIDENT-PLAYBOOKS FÜR KMU

# Der IT-Notfallplan für Mitarbeitende

Stand: September 2026 · 18 Playbooks

Pro Vorfall eine Seite: Situation, Sofortmaßnahmen, Meldeweg, häufige Fehler und was danach passiert. Ergänzend gehört das Incident-Kontaktblatt mit euren eigenen Meldewegen dazu. Alle Playbooks sind online unter wermescher.com/tools/it-notfallplan abrufbar.



**Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.**

Erstgespräch vereinbaren: https://cal.com/mein.termin/mit.herwart-allgemein-30min

wermescher.com/tools/it-notfallplan

INCIDENT-PLAYBOOK DEV-03

# Privates Gerät für Firmendaten verwendet

Geräte & Datenträger

Unternehmensdaten sind auf einem privaten Gerät oder in einem privaten Konto gelandet. Manchmal bewusst, weil es schneller ging. Oft unbemerkt, weil eine Synchronisierung im Hintergrund lief.

- Firmendokument am eigenen Laptop bearbeitet
- Dienstliche Mail ans private Postfach weitergeleitet
- Foto von Unterlagen am privaten Handy
- Firmendaten in privatem Cloud-Speicher abgelegt

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts löschen. Was jetzt verschwindet, fehlt später bei der Frage, welche Daten überhaupt betroffen waren.

02 Keine weiteren Kopien anlegen, nichts weiterleiten, nicht weiterbearbeiten.

03 Automatische Synchronisierung pausieren, wenn eine läuft: Cloud-Backup, Fotomediathek, Messenger-Sicherung.

04 Kurz notieren, welche Daten es sind, wann sie auf das Gerät kamen und über welchen Weg.

05 Den Vorgang melden, auch wenn nichts Schlimmes passiert ist. Die Bewertung übernimmt die IT.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die direkte Führungskraft. Bei personenbezogenen Daten zusätzlich die Datenschutz-Ansprechperson.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, im Zweifel telefonisch. Für die Meldung ein dienstliches Gerät verwenden.

WAS BEREITHALTEN

- Um welches private Gerät oder Konto es geht
- Welche Daten betroffen sind und ungefähr wie viele
- Seit wann die Daten dort liegen
- Ob personenbezogene Daten dabei sind
- Ob weitere Personen Zugriff auf das Gerät haben

## Nicht tun

HÄUFIGE FEHLER

- × Die Daten eigenmächtig löschen, bevor der Vorgang aufgenommen ist.
- × Den Vorgang verschweigen, weil er unangenehm ist. Eine späte Meldung kostet immer mehr als eine unangenehme.
- × Zur Bereinigung weitere Kopien auf andere private Geräte oder Konten ziehen.
- × Screenshots der Daten an Kolleginnen und Kollegen schicken, um die Lage zu erklären.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT klärt den Umfang, prüft eine nachweisbare Löschung und entscheidet, ob das Gerät bereinigt werden muss.
- → Bei personenbezogenen Daten bewertet die Datenschutz-Ansprechperson, ob eine meldepflichtige Datenschutzverletzung vorliegt.
- → Gibt es einen echten fachlichen Bedarf, richtet die IT einen freigegebenen Weg ein: sicherer Zugriff oder ein verwaltetes Gerät.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK ACC-01

# Passwort oder Zugangsdaten preisgegeben

Konto & Identität

Ein Passwort ist in fremde Hände geraten. Es wurde auf einer nachgebauten Seite eingetippt, am Telefon genannt, in einem Chat geteilt oder lag sichtbar für andere zugänglich. Ob damit schon jemand angemeldet ist, weißt du nicht.

- Passwort auf einer gefälschten Anmeldeseite eingegeben
- Zugangsdaten am Telefon weitergegeben
- Passwort per Chat oder Mail verschickt
- Notierte Zugangsdaten sind abhandengekommen

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort sofort ändern, von einem Gerät aus, das nicht Teil des Vorfalls ist.

02 In den Kontoeinstellungen alle aktiven Sitzungen abmelden. Sonst bleibt eine fremde Anmeldung trotz neuem Passwort bestehen.

03 Prüfen, wo dasselbe Passwort noch verwendet wird, und auch dort wechseln.

04 Melden, auch wenn du das Passwort bereits geändert hast. Die IT prüft, ob in der Zwischenzeit zugegriffen wurde.

05 Wenn möglich Multi-Faktor-Authentifizierung für das Konto aktivieren.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, zeitnah. Bei Konten mit Zahlungs- oder Personaldaten zusätzlich die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Nicht über das betroffene Konto selbst.

WAS BEREITHALTEN

- Um welches Konto und welchen Dienst es geht
- Wie und wann die Daten preisgegeben wurden
- Ob das Passwort bereits geändert wurde
- Wo dasselbe Passwort sonst noch im Einsatz war
- Ob das Konto Multi-Faktor-Authentifizierung hat

## Nicht tun

HÄUFIGE FEHLER

× Nur das Passwort ändern und die aktiven Sitzungen unangetastet lassen.
× Eine leichte Abwandlung des alten Passworts wählen. Angreifer probieren genau diese Varianten durch.
× Den Fall für erledigt halten, weil sich nichts Auffälliges zeigt. Zugänge werden oft erst Wochen später genutzt.
× Aus Scham abwarten. Der Zeitvorsprung ist das Einzige, was in diesem Fall hilft.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

→ Die IT prüft die Anmeldeprotokolle des Kontos auf fremde Zugriffe und ungewöhnliche Standorte.
→ Postfachregeln, Weiterleitungen und verknüpfte Anwendungen werden auf nachträgliche Änderungen kontrolliert.
→ Bei Konten mit Zugriff auf personenbezogene Daten folgt die Bewertung durch Datenschutz-Ansprechperson und Geschäftsführung.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Phishing-Link angeklickt (PHI-02) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK ACC-02

# MFA-Gerät verloren oder gewechselt

Konto & Identität

Das Gerät mit der Authenticator-App oder dem Sicherheitsschlüssel ist weg, defekt oder wurde getauscht. Anmeldungen, die einen zweiten Faktor verlangen, sind damit blockiert. Bei Verlust oder Diebstahl kommt hinzu, dass ein Fremder das Gerät in der Hand hält.

- Diensthandy verloren oder gestohlen
- Neues Handy ohne übertragene Authenticator-App
- Sicherheitsschlüssel nicht mehr auffindbar
- Gerät defekt und nicht mehr startfähig

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Bei Verlust oder Diebstahl sofort melden. Das ist ein Sicherheitsvorfall, keine reine Nutzerhilfe.

02 Ist das Gerät fremdverwaltet, die IT das Gerät sperren und die Fernlöschung auslösen lassen.

03 Beim geplanten Gerätewechsel die Übertragung durchführen, bevor das alte Gerät zurückgesetzt oder entsorgt wird.

04 Den zweiten Faktor für das alte Gerät in den Kontoeinstellungen entfernen lassen, sobald der neue eingerichtet ist.

05 Wiederherstellungscodes nicht auf demselben Gerät und nicht ungeschützt ablegen.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei Diebstahl zusätzlich die Geschäftsführung, bei Diensthandys auch wegen der enthaltenen Daten.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, wenn das Gerät verloren oder gestohlen wurde. Beim geplanten Wechsel über den normalen Meldeweg.

WAS BEREITHALTEN

- Um welches Gerät es geht und ob es dienstlich oder privat war
- Ob es verloren, gestohlen, defekt oder getauscht wurde
- Wann es zuletzt in deinem Besitz war
- Für welche Konten es als zweiter Faktor diente
- Ob das Gerät mit Code oder Biometrie gesperrt war

## Nicht tun

HÄUFIGE FEHLER

- × Das alte Gerät zurücksetzen oder entsorgen, bevor die hinterlegten Faktoren übertragen und entfernt sind.
- × Den Verlust als reines Ausstattungsthema behandeln und nur ein neues Gerät anfordern.
- × Wiederherstellungscodes im Postfach oder in einer Notiz-App auf demselben Gerät speichern.
- × Die Multi-Faktor-Authentifizierung vorübergehend abschalten, um weiterarbeiten zu können.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT entfernt die auf dem alten Gerät hinterlegten Faktoren aus allen betroffenen Konten.
- → Anmeldeprotokolle werden auf Zugriffe nach dem Verlustzeitpunkt geprüft.
- → Der neue zweite Faktor wird eingerichtet und neue Wiederherstellungscodes werden ausgegeben.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Privates Handy dienstlich genutzt (DEV-03) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK ACC-03

# Verdacht auf Kontoübernahme

Konto & Identität

Es gibt Anzeichen, dass jemand anderes Zugriff auf ein dienstliches Konto hat. Typisch sind Anmeldungen zu ungewöhnlichen Zeiten, Nachrichten, die du nie geschrieben hast, oder Einstellungen, die sich von selbst geändert haben.

- Anmeldung aus einem fremden Land gemeldet
- Gesendete Mails, die du nicht geschrieben hast
- Neue Weiterleitungsregel im Postfach
- Passwort funktioniert plötzlich nicht mehr

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort sofort ändern, von einem anderen, sauberen Gerät aus. Funktioniert das nicht mehr, direkt zur Meldung übergehen.

02 In den Kontoeinstellungen alle aktiven Sitzungen abmelden, damit fremde Zugriffe unterbrochen werden.

03 Postfachregeln und Weiterleitungen prüfen und auffällige Einträge notieren, bevor du sie entfernst.

04 Prüfen, ob dasselbe Passwort noch anderswo im Einsatz ist, und diese Konten ebenfalls ändern.

05 Sofort melden, auch wenn du den Zugriff schon unterbrochen hast.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei Konten mit Zahlungsfreigabe zusätzlich die Geschäftsführung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über das betroffene Konto, weil Angreifer dort mitlesen können.

WAS BEREITHALTEN

- Um welches Konto und welchen Dienst es geht
- Woran du den fremden Zugriff bemerkt hast
- Seit wann die Auffälligkeiten bestehen
- Welche Weiterleitungen oder Regeln du gefunden hast
- Ob das Passwort auch für andere Dienste genutzt wurde

## Nicht tun

HÄUFIGE FEHLER

- × Über das verdächtige Konto selbst melden oder dort über den Vorfall schreiben.
- × Gefundene Weiterleitungsregeln löschen, ohne sie vorher festzuhalten. Sie sind ein wichtiger Hinweis auf das Vorgehen.
- × Abwarten, ob sich das Problem von selbst erledigt.
- × Kundinnen und Kunden auf eigene Faust warnen, bevor das Vorgehen abgestimmt ist.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT sperrt das Konto vorübergehend, setzt die Anmeldedaten neu auf und richtet die Multi-Faktor-Authentifizierung neu ein.
- → Anhand der Anmeldeprotokolle wird geprüft, welche Daten eingesehen und welche Nachrichten versendet wurden.
- → Sind personenbezogene Daten oder Zahlungsvorgänge betroffen, folgt die Bewertung durch Datenschutz-Ansprechperson und Geschäftsführung.

**Verweise:** Incident-Kontaktblatt (PDF) · Cloud-Konto kompromittiert (CLD-01) · Verdacht auf Datenschutzverletzung (DAT-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK ACC-04

# Unerwartete MFA-Anfragen

Konto & Identität

Auf dem Handy erscheint eine Bestätigungsanfrage für eine Anmeldung, die du nicht ausgelöst hast. Manchmal einmal, manchmal in Serie und mitten in der Nacht. Jede dieser Anfragen bedeutet, dass jemand dein Passwort bereits kennt.

- Push-Anfrage ohne eigene Anmeldung
- Mehrere Anfragen kurz hintereinander
- Anfrage nachts oder im Urlaub
- SMS-Code, den niemand angefordert hat

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Anfrage ablehnen. Niemals bestätigen, um die Serie zu beenden.

02 Passwort des betroffenen Kontos sofort ändern. Die Anfragen belegen, dass es bekannt ist.

03 Alle aktiven Sitzungen des Kontos abmelden.

04 Sofort melden, auch wenn du nichts bestätigt hast. Die IT braucht den Zeitpunkt der Versuche.

05 Hast du versehentlich bestätigt: telefonisch melden, das ist der dringende Fall.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei versehentlicher Bestätigung sofort telefonisch.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, bei bestätigter Anfrage telefonisch.

WAS BEREITHALTEN

- Für welches Konto die Anfragen kamen
- Wie viele Anfragen und zu welchen Uhrzeiten
- Ob eine Anfrage bestätigt wurde
- Ob das Passwort bereits geändert wurde
- Ob parallel Anrufe oder Nachrichten dazu kamen

## Nicht tun

HÄUFIGE FEHLER

- × Eine Anfrage bestätigen, damit endlich Ruhe ist. Genau darauf zielt die Wiederholung.
- × Die Anfragen wegwischen und nichts weiter tun. Das Passwort bleibt in fremder Hand.
- × Einem Anrufer glauben, der sich als IT ausgibt und um Bestätigung der Anfrage bittet.
- × Bis zum nächsten Werktag warten, weil die Anfragen nachts kommen.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Anmeldeprotokolle auf Herkunft und Zeitpunkt der Versuche und setzt die Anmeldedaten neu auf.
- → Der zweite Faktor wird bei Bedarf auf ein Verfahren mit Nummernabgleich oder Sicherheitsschlüssel umgestellt.
- → Ist eine Bestätigung erfolgt, werden Postfachregeln, Weiterleitungen und verknüpfte Anwendungen kontrolliert.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Verdächtiger Anruf (PHI-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-01

# Verdächtige Nachricht erhalten

Phishing & Social Engineering

Eine Mail oder Chat-Nachricht wirkt nicht echt. Sie drängt zur Eile, kommt von einem unerwarteten Absender oder verlangt eine Anmeldung, eine Zahlung oder die Weitergabe von Daten. Du hast noch nichts angeklickt und nichts eingegeben.

- Angebliche Sperrung eines Kontos mit Frist von 24 Stunden
- Rechnung von einem Absender, der nie Rechnungen schickt
- Bitte um Freigabe eines geteilten Dokuments
- Nachricht der Geschäftsführung über einen fremden Kanal

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts anklicken, nichts herunterladen, nicht antworten. Solange die Nachricht nur im Postfach liegt, ist nichts passiert.

02 Absenderadresse vollständig anzeigen lassen und mit der echten Adresse vergleichen. Der angezeigte Name sagt nichts aus.

03 Bei angeblich internen Absendern über einen bekannten Weg rückfragen, nie über die Kontaktdaten aus der Nachricht.

04 Melden, auch wenn du sicher bist, dass es Phishing ist. Die IT braucht die Info, um andere Empfänger zu schützen.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei Nachrichten mit Zahlungsbezug zusätzlich die Buchhaltung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Falls vorhanden, den Melde-Button im Mail-Programm nutzen.

WAS BEREITHALTEN

- Vollständige Absenderadresse, nicht nur der angezeigte Name
- Betreff und Eingangszeitpunkt der Nachricht
- Worum die Nachricht bittet
- Ob du etwas angeklickt oder geantwortet hast
- Ob Kolleginnen und Kollegen dieselbe Nachricht bekommen haben

## Nicht tun

HÄUFIGE FEHLER

- × Die Nachricht an Kolleginnen und Kollegen weiterleiten, um zu warnen. Wer den Link dort öffnet, ist im selben Fall.
- × Auf Abmelden oder Kein Interesse klicken. Auch diese Links bestätigen, dass die Adresse aktiv gelesen wird.
- × Die Nachricht einfach löschen. Ohne Meldung erfährt die IT nichts von der laufenden Welle.
- × Den Absender anrufen, um nachzufragen, wenn die Nummer aus der Nachricht selbst stammt.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, wie viele Postfächer die Nachricht erreicht hat, und entfernt sie zentral aus allen betroffenen Konten.
- → Absender und Zieladresse werden gesperrt, damit Folgewellen aus derselben Quelle nicht mehr durchkommen.
- → Häufen sich gleichartige Nachrichten, folgt eine kurze Information ans Team mit den konkreten Erkennungsmerkmalen.

**Verweise:** Incident-Kontaktblatt (PDF) · Phishing-Link angeklickt (PHI-02) · CEO-Fraud oder Rechnungsbetrug (PHI-04) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-02

# Phishing-Link angeklickt

Phishing & Social Engineering

Du hast einen Link aus einer Nachricht geöffnet und erst danach gemerkt, dass etwas nicht stimmt. Die Seite verlangt eine Anmeldung, einen Bestätigungscode oder einen Download. Vielleicht hast du schon etwas eingetippt.

- Anmeldeseite, die der internen Anmeldung nachgebaut ist
- Seite fragt nach dem Code aus der Authenticator-App
- Download startet ohne Zutun
- Adresszeile zeigt eine fremde Domain

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Seite sofort schließen. Wurde nichts eingegeben, ist in den meisten Fällen nichts abgeflossen.

02 Hast du Zugangsdaten eingegeben: Passwort von einem anderen Gerät aus ändern und alle aktiven Sitzungen abmelden.

03 Hast du einen MFA-Code bestätigt: sofort telefonisch melden. Der Zugriff kann in diesem Moment bereits laufen.

04 Wurde etwas heruntergeladen oder installiert: Gerät vom Netz trennen und die IT anrufen, bevor du weiterarbeitest.

05 Screenshot der Seite und die vollständige Adresse aus der Adresszeile sichern.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei bestätigtem MFA-Code sofort telefonisch.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, wenn Zugangsdaten oder ein Code betroffen sind. Sonst über den internen Meldeweg.

WAS BEREITHALTEN

- Welche Adresse in der Adresszeile stand
- Ob du Zugangsdaten eingegeben hast und für welchen Dienst
- Ob du eine MFA-Anfrage bestätigt hast
- Ob ein Download gestartet oder etwas installiert wurde
- Uhrzeit des Klicks, so genau wie möglich

## Nicht tun

HÄUFIGE FEHLER

- × Abwarten und beobachten, ob etwas passiert. Bei abgeflossenen Zugangsdaten zählt jede Minute.
- × Das neue Passwort auf demselben Gerät setzen, wenn ein Download gelaufen ist.
- × Die Seite noch einmal öffnen, um nachzusehen, wie sie aussah. Der Screenshot genügt.
- × Den Vorfall verschweigen, weil er unangenehm ist. Gemeldete Fälle sind in Minuten eingedämmt.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Anmeldeprotokolle des betroffenen Kontos auf fremde Zugriffe und setzt die Anmeldedaten neu auf.
- → Bei bestätigtem MFA-Code werden zusätzlich die hinterlegten Geräte und Wiederherstellungsoptionen kontrolliert.
- → Wurde etwas ausgeführt, wird das Gerät untersucht und im Zweifel neu aufgesetzt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Verdächtigen Anhang geöffnet (PHI-03) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-03

# Verdächtigen Anhang geöffnet

Phishing & Social Engineering

Du hast einen Anhang geöffnet und danach stimmt etwas nicht. Das Dokument verlangt, den Bearbeitungsschutz aufzuheben oder Inhalte zu aktivieren, es öffnet ein Fenster, das nach Zugangsdaten fragt, oder es bleibt leer, obwohl eine Rechnung angekündigt war.

- Word- oder Excel-Datei bittet, Inhalte zu aktivieren
- Angebliche Rechnung öffnet eine Anmeldemaske
- ZIP-Archiv mit einer Datei, die wie ein Dokument aussieht
- Dokument ist leer oder unleserlich

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Datei und Programm schließen. Hast du Inhalte oder Makros aktiviert, das Gerät sofort vom Netzwerk und WLAN trennen.

02 Gerät eingeschaltet lassen. Ein Neustart kann Spuren vernichten, die für die Aufklärung gebraucht werden.

03 Die IT anrufen, nicht mailen. Bei aktivierten Makros gilt das Gerät bis zur Prüfung als nicht vertrauenswürdig.

04 Hast du in einem Fenster Zugangsdaten eingegeben: Passwort von einem anderen Gerät aus ändern.

05 Die Ursprungsnachricht samt Absender und Dateiname festhalten, ohne sie weiterzuleiten.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei Dateien aus dem Rechnungsumlauf zusätzlich die Buchhaltung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, weil das betroffene Gerät für die Meldung nicht genutzt werden soll.

WAS BEREITHALTEN

- Dateiname und Dateityp des Anhangs
- Ob du Inhalte, Makros oder den Bearbeitungsschutz freigegeben hast
- Was nach dem Öffnen auf dem Bildschirm passiert ist
- Absender und Betreff der Nachricht
- Ob das Gerät noch am Netz hängt

## Nicht tun

HÄUFIGE FEHLER

- × Den Rechner neu starten oder herunterfahren, bevor die IT den Fall aufgenommen hat.
- × Die Datei zur Prüfung an jemanden weiterleiten. Der nächste Empfänger öffnet sie im Zweifel ebenfalls.
- × Selbst einen Virenscan starten und das Ergebnis abwarten, statt zu melden.
- × Weiterarbeiten, weil scheinbar nichts passiert ist. Schadsoftware arbeitet in der Regel unauffällig.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT untersucht das Gerät, prüft Netzwerkverbindungen und offene Prozesse und entscheidet über Bereinigung oder Neuaufsetzen.
- → Erreichbare Netzlaufwerke und Cloud-Ordner werden auf Veränderungen und Verschlüsselung geprüft.
- → Dieselbe Datei wird in allen Postfächern gesucht und dort zentral entfernt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Phishing-Link angeklickt (PHI-02) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-04

# CEO-Fraud oder Rechnungsbetrug

Phishing & Social Engineering

Eine Zahlung soll ausgelöst oder eine Bankverbindung geändert werden. Die Anweisung kommt scheinbar von der Geschäftsführung oder von einem bekannten Lieferanten, wirkt dringend und bittet um Vertraulichkeit oder darum, den üblichen Weg abzukürzen.

- Geschäftsführung bittet um eine eilige Überweisung
- Lieferant meldet eine neue Kontonummer
- Rechnung mit geänderter IBAN bei bekanntem Betrag
- Bitte um Gutscheinkauf oder Barauslage

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Zahlung anhalten. Nichts freigeben und nichts vorbereiten, solange die Anweisung nicht über einen zweiten Weg bestätigt ist.

02 Bei bekannter Rufnummer aus dem eigenen Verzeichnis rückfragen, nie über Kontaktdaten aus der Nachricht oder der Rechnung.

03 Ist die Überweisung schon draußen: sofort die Bank anrufen und den Rückruf der Zahlung verlangen. Das ist zeitkritisch.

04 Geschäftsführung und Buchhaltung unmittelbar informieren, auch wenn der Betrug nur vermutet wird.

05 Nachricht, Rechnung und Kontodaten unverändert sichern, inklusive vollständigem Absender.

## Melden

SOFORT

WEN

Geschäftsführung und Buchhaltung sofort, parallel die IT-Verantwortlichen. Bei erfolgter Zahlung zusätzlich die Hausbank.

WIE

Telefonisch, nicht per Mail. Läuft der Betrug über ein übernommenes Postfach, lesen die Täter mit.

WAS BEREITHALTEN

- Betrag, Empfängerbank und IBAN der verlangten Zahlung
- Über welchen Kanal die Anweisung kam
- Ob die Zahlung bereits freigegeben oder ausgeführt wurde
- Wer im Haus sonst noch kontaktiert wurde
- Welche Frist oder Begründung genannt wurde

## Nicht tun

HÄUFIGE FEHLER

- × Auf die Bitte um Vertraulichkeit eingehen. Sie dient allein dazu, die Vier-Augen-Kontrolle auszuhebeln.
- × Über den Kanal der Anweisung rückfragen, auch nicht auf eine mitgeschickte Telefonnummer.
- × Die geänderte Bankverbindung im Lieferantenstamm speichern, bevor sie telefonisch bestätigt ist.
- × Aus Zeitdruck teilweise zahlen oder eine Anzahlung leisten.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Geschäftsführung entscheidet über Anzeige bei der Polizei und die Einbindung der Versicherung. Beides ist zeitkritisch.
- → Die IT prüft, ob ein Postfach im Haus oder beim Lieferanten übernommen wurde und seit wann mitgelesen wird.
- → Der Freigabeprozess für Zahlungen und Stammdatenänderungen wird überprüft und wo nötig nachgeschärft.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Lieferant wurde gehackt (SUP-01) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-05

# Verdächtiger Anruf oder Identitätsbetrug

Phishing & Social Engineering

Jemand ruft an und gibt sich als IT-Support, Bank, Behörde, Lieferant oder Kollege aus. Verlangt werden Zugangsdaten, ein Bestätigungscode, eine Fernwartungssitzung oder Auskunft über interne Abläufe. Der Anruf kommt unerwartet und drängt zur Eile.

- Angeblicher Support will per Fernwartung auf den Rechner
- Anrufer fragt nach dem Code aus der Authenticator-App
- Bank meldet einen Sicherheitsvorfall und braucht Daten
- Neuer Kollege fragt nach internen Abläufen

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine Zugangsdaten und keine Codes nennen. Kein seriöser Anrufer fragt danach, auch die eigene IT nicht.

02 Keine Fernwartung zulassen und keine Software installieren, die am Telefon verlangt wird.

03 Gespräch beenden. Du brauchst keine Begründung und schuldest keine Höflichkeit.

04 Läuft bereits eine Fernwartung: Gerät vom Netz trennen und die IT über ein anderes Gerät anrufen.

05 Selbst zurückrufen, über eine Nummer aus dem internen Verzeichnis oder von der offiziellen Website.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei angeblichen Bank- oder Behördenanrufen zusätzlich Buchhaltung und Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Lief eine Fernwartung, telefonisch und von einem anderen Gerät.

WAS BEREITHALTEN

- Rufnummer und Zeitpunkt des Anrufs
- Als wer sich die Person ausgegeben hat
- Was konkret verlangt wurde
- Ob du etwas genannt, installiert oder freigegeben hast
- Ob Namen oder interne Details bekannt waren

## Nicht tun

HÄUFIGE FEHLER

- × Zur Prüfung eine Nummer zurückrufen, die der Anrufer selbst genannt hat.
- × Aus Höflichkeit im Gespräch bleiben und nur Kleinigkeiten bestätigen. Auch Namen und Abläufe sind verwertbar.
- × Einen Code vorlesen, weil der Anrufer ihn angeblich zur Verifizierung braucht.
- × Den Anruf als erledigt betrachten, weil du nichts verraten hast. Die IT braucht die Info trotzdem.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, ob im selben Zeitraum Anmeldeversuche oder MFA-Anfragen auf dein Konto liefen.
- → Wurde eine Fernwartung zugelassen, wird das Gerät untersucht und im Zweifel neu aufgesetzt.
- → Häufen sich Anrufe, wird das Team informiert, welche Rollen und Nummern gerade angesprochen werden.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · CEO-Fraud oder Rechnungsbetrug (PHI-04) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK PHI-06

# Verdächtiger QR-Code oder SMS-Link

Phishing & Social Engineering

Ein QR-Code oder eine SMS führt auf eine Seite, die Zugangsdaten, eine Zahlung oder eine App-Installation verlangt. Beide Wege umgehen den Mail-Schutz des Unternehmens, weil sie am Handy und außerhalb des Postfachs ankommen.

- QR-Code-Aufkleber über dem Original am Parkautomaten
- SMS zu einer angeblich fehlgeschlagenen Paketzustellung
- QR-Code in einer Mail statt eines Links
- SMS von der angeblichen Bank mit Bestätigungslink

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nichts eingeben und die Seite schließen. Solange keine Daten eingetippt sind, ist meist nichts passiert.

02 Wurde bereits etwas eingegeben: sofort das betroffene Passwort ändern und alle aktiven Sitzungen abmelden.

03 Wurde eine App oder ein Profil installiert: Gerät vom WLAN und Mobilfunk trennen und die IT anrufen, bevor du weiter tippst.

04 Screenshot der Nachricht oder Foto des QR-Codes machen, samt Absendernummer.

05 Melden, auch wenn du nichts eingegeben hast. Der Fund selbst ist die nützliche Information.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei QR-Codes im eigenen Gebäude zusätzlich Empfang oder Facility-Verantwortliche.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Bei installierter App oder Profil telefonisch, nicht schriftlich vom betroffenen Gerät.

WAS BEREITHALTEN

- Wo der QR-Code hing oder von welcher Nummer die SMS kam
- Wie die Zielseite ausgesehen und was sie verlangt hat
- Ob du etwas eingegeben oder installiert hast
- Ob es ein dienstliches oder privates Gerät war
- Wann genau du den Code gescannt oder den Link geöffnet hast

## Nicht tun

HÄUFIGE FEHLER

× Den Code ein zweites Mal scannen, um ihn Kolleginnen und Kollegen zu zeigen.
× Den Link zur Warnung an andere weiterleiten. Wer ihn öffnet, landet auf derselben Seite.
× Auf die SMS antworten, auch nicht mit einer Absage. Eine Antwort bestätigt, dass die Nummer aktiv ist.
× Verdächtige QR-Aufkleber entfernen, bevor jemand sie fotografiert hat.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

→ Die IT prüft, ob weitere Personen dieselbe Nachricht erhalten haben, und sperrt die Zieladresse.
→ Bei eingegebenen Zugangsdaten werden Konto und Anmeldeprotokolle geprüft und die Anmeldedaten neu aufgesetzt.
→ Bei installierten Apps oder Konfigurationsprofilen wird das Gerät untersucht und im Zweifel neu aufgesetzt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK DAT-05

# Verdacht auf Datenschutzverletzung

Daten & Datenschutz

Personenbezogene Daten sind möglicherweise verloren gegangen, an Unbefugte gelangt, verändert worden oder nicht mehr verfügbar. Der Verdacht genügt für die Meldung. Die Bewertung übernehmen andere.

- Kundenliste an den falschen Empfänger geschickt
- Ordner mit Personaldaten offen freigegeben
- Unterlagen mit Kundendaten verloren
- Bewerbungsunterlagen im falschen Postfach gelandet

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Sofort melden. Die gesetzliche Frist des Unternehmens beginnt mit dem Moment, in dem es Kenntnis erlangt, also mit deiner Meldung.

02 Den Zustand einfrieren: nichts löschen, nichts überschreiben, keine Freigabe stillschweigend zurückziehen.

03 Belege sichern: Screenshot der Freigabe, Kopie der gesendeten Nachricht, Notiz zur Uhrzeit.

04 Notieren, welche Personengruppen und welche Datenarten betroffen sein könnten und wie viele Personen es ungefähr sind.

05 Ist die Ursache noch aktiv, etwa ein offener Link, das der IT beim Melden ausdrücklich sagen.

## Melden

SOFORT

WEN

Datenschutz-Ansprechperson und IT-Verantwortliche gemeinsam. Fehlt eine benannte Datenschutz-Ansprechperson, geht die Meldung an die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, ohne Umweg über Zwischenstationen. Bei Unsicherheit telefonisch.

WAS BEREITHALTEN

- Was passiert ist und wann du es bemerkt hast
- Welche Datenarten betroffen sind
- Wie viele Personen ungefähr betroffen sind
- Wer die Daten erhalten haben könnte
- Ob die Ursache noch besteht

## Nicht tun

HÄUFIGE FEHLER

- × Erst selbst prüfen, ob es wirklich schlimm ist. Die Bewertung ist Aufgabe der Datenschutz-Ansprechperson.
- × Betroffene Personen auf eigene Faust informieren, bevor das Vorgehen abgestimmt ist.
- × Empfänger bitten, die Nachricht einfach zu löschen, und den Fall damit für erledigt halten.
- × Belege löschen, um die Sache unauffällig zu bereinigen.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Datenschutz-Ansprechperson bewertet, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und welches Risiko für die betroffenen Personen entsteht.
- → Ergibt die Bewertung ein Risiko, meldet das Unternehmen unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die Datenschutzbehörde (Art. 33 DSGVO).
- → Bei voraussichtlich hohem Risiko werden zusätzlich die betroffenen Personen unverzüglich benachrichtigt (Art. 34 DSGVO).
- → Auch Verletzungen ohne Meldepflicht werden intern dokumentiert. Die Dokumentation ist selbst eine gesetzliche Pflicht.

**Verweise:** Incident-Kontaktblatt (PDF) · Gesetze und Regulierung im Wissensbereich · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK MAL-01

# Virenmeldung oder Sicherheitswarnung

Malware & verdächtiges Verhalten

Auf dem Bildschirm erscheint eine Warnung über einen Virus, eine Bedrohung oder ein Sicherheitsproblem. Unklar ist, ob die Meldung vom installierten Schutzprogramm stammt oder von einer Website, die eine Warnung nur nachbaut.

- Warnfenster im Browser mit Telefonnummer zum Support
- Meldung des Virenscanners über eine blockierte Datei
- Aufforderung, ein Reinigungsprogramm zu installieren
- Dauerhafter Warnton mit Vollbildmeldung

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Prüfen, wo die Meldung steht. Alles innerhalb eines Browserfensters ist keine Meldung deines Schutzprogramms.

02 Keine Telefonnummer aus der Meldung anrufen und keine angebotene Software installieren.

03 Browserfenster oder Tab schließen. Lässt es sich nicht schließen, den Browser über den Task-Manager beenden.

04 Kommt die Meldung nachweislich vom Schutzprogramm: nichts wegklicken, Screenshot machen und melden.

05 Wurde bereits etwas installiert oder eine Nummer angerufen: Gerät vom Netz trennen und die IT anrufen.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister. Bei echter Scanner-Meldung zeitnah, bei installierter Fremdsoftware sofort.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Wurde etwas installiert, telefonisch und von einem anderen Gerät.

WAS BEREITHALTEN

- Wortlaut der Meldung, am besten als Screenshot
- Ob sie im Browser oder ausserhalb erschienen ist
- Welcher Dateiname oder Bedrohungsname genannt wurde
- Was du unmittelbar davor geöffnet hast
- Ob du etwas installiert oder angerufen hast

## Nicht tun

HÄUFIGE FEHLER

- × Die angezeigte Support-Nummer anrufen. Sie führt zu den Urhebern der Meldung.
- × Ein empfohlenes Reinigungs- oder Optimierungsprogramm installieren.
- × Eine echte Scanner-Meldung wegklicken und weiterarbeiten, ohne sie zu melden.
- × Die blockierte Datei erneut öffnen oder aus der Quarantäne holen.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft die Protokolle des Schutzprogramms und ordnet ein, ob es sich um einen Einzelfund oder eine Welle handelt.
- → Bei installierter Fremdsoftware wird das Gerät untersucht und im Zweifel neu aufgesetzt.
- → Häufen sich gefälschte Warnfenster, werden die auslösenden Adressen zentral gesperrt.

**Verweise:** Incident-Kontaktblatt (PDF) · Rechner verhält sich ungewöhnlich (MAL-02) · Verdächtiger Anruf (PHI-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK MAL-02

# Rechner verhält sich ungewöhnlich

Malware & verdächtiges Verhalten

Das Gerät reagiert anders als sonst. Es wird ohne erkennbaren Grund langsam, der Lüfter läuft dauerhaft, Fenster öffnen sich von selbst, der Mauszeiger bewegt sich eigenständig oder Programme starten und beenden sich ohne Zutun.

- Mauszeiger bewegt sich ohne Zutun
- Dauerhaft hohe Auslastung ohne laufendes Programm
- Unbekannte Programme im Autostart
- Dateien sind umbenannt oder verschwunden

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät vom Netzwerk und WLAN trennen. Das unterbricht Fernzugriff und den Zugang zu Netzlaufwerken.

02 Gerät eingeschaltet lassen und nicht neu starten. Ein Neustart löscht Spuren, die für die Aufklärung gebraucht werden.

03 Nicht weiterarbeiten und keine Zugangsdaten mehr eintippen. Eingaben können mitgelesen werden.

04 Die IT von einem anderen Gerät oder telefonisch verständigen.

05 Notieren, was genau auffällt und seit wann, solange die Beobachtung frisch ist.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister, unverzüglich. Bei fremdgesteuertem Mauszeiger sofort telefonisch.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt, nicht vom betroffenen Gerät aus.

WAS BEREITHALTEN

- Welche Auffälligkeiten konkret auftreten
- Seit wann das Verhalten besteht
- Was du zuletzt geöffnet oder installiert hast
- Ob das Gerät noch am Netz hängt
- Ob auf Netzlaufwerke zugegriffen wurde

## Nicht tun

HÄUFIGE FEHLER

- × Neu starten oder herunterfahren in der Hoffnung, dass es sich damit erledigt.
- × Selbst Programme deinstallieren oder Autostart-Einträge löschen, bevor die IT den Stand gesehen hat.
- × Weiterarbeiten und sich in andere Dienste einloggen.
- × Externe Datenträger anstecken, um schnell noch Dateien zu sichern.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT untersucht laufende Prozesse, Autostart und ausgehende Verbindungen und entscheidet über Bereinigung oder Neuaufsetzen.
- → Erreichbare Netzlaufwerke und Cloud-Ordner werden auf Veränderungen geprüft.
- → Anmeldedaten der auf dem Gerät genutzten Konten werden vorsorglich neu aufgesetzt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Verdächtigen Anhang geöffnet (PHI-03) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK MAL-03

# Verdacht auf Ransomware

Malware & verdächtiges Verhalten

Dateien lassen sich nicht mehr öffnen, tragen plötzlich fremde Endungen oder es erscheint eine Erpressungsnachricht. Jede Minute zählt, weil die Verschlüsselung weiterläuft, solange das Gerät im Netzwerk hängt.

- Dateinamen mit unbekannter Endung versehen
- Textdatei mit Lösegeldforderung in jedem Ordner
- Office-Dateien lassen sich nicht mehr öffnen
- Netzlaufwerke verändern sich vor den Augen

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät sofort vom Netzwerk trennen: Netzwerkkabel ziehen und WLAN ausschalten. Das stoppt die Ausbreitung auf Server und Kolleginnen.

02 Gerät eingeschaltet lassen und nicht neu starten. Im Arbeitsspeicher liegen Spuren, die für die Aufklärung und manchmal für die Entschlüsselung entscheidend sind.

03 Angeschlossene Datenträger und Backup-Festplatten physisch abstecken.

04 Foto der Erpressungsnachricht mit dem Handy machen, bevor irgendetwas verändert wird.

05 Sofort telefonisch melden. Nicht per Mail vom betroffenen Gerät.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister sofort, parallel die Geschäftsführung. Bei laufender Ausbreitung gilt das als Notfall zu jeder Tageszeit.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Wenn niemand erreichbar ist, die nächste Eskalationsstufe anrufen.

WAS BEREITHALTEN

- Welches Gerät betroffen ist und wo es steht
- Woran du es bemerkt hast und wann
- Ob Netzlaufwerke oder Cloud-Ordner betroffen sind
- Was auf der Erpressungsnachricht steht
- Was du zuletzt geöffnet oder installiert hast

## Nicht tun

HÄUFIGE FEHLER

- × Das Gerät herunterfahren oder neu starten, solange die IT nichts anderes sagt.
- × Auf eigene Faust ein Entschlüsselungswerkzeug aus dem Internet herunterladen und ausführen.
- × Kontakt zu den Erpressern aufnehmen oder zahlen. Beides entscheidet ausschließlich die Geschäftsführung.
- × Dateien aus einem Backup zurückspielen, bevor klar ist, dass das Netzwerk sauber ist.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT isoliert betroffene Systeme, sucht nach weiteren befallenen Geräten und sichert Spuren für die Aufklärung.
- → Die Geschäftsführung entscheidet über Krisenkommunikation, Anzeige bei der Polizei und Einbindung der Cyber-Versicherung.
- → Sind personenbezogene Daten betroffen, läuft parallel die Bewertung nach Art. 33 DSGVO mit der 72-Stunden-Frist.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen zusätzlich die Berichtspflichten nach § 34: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden an das zuständige Computer-Notfallteam.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Bin ich von NIS2 betroffen? · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK MAL-04

# Lösegeldforderung am Bildschirm

Malware & verdächtiges Verhalten

Auf dem Bildschirm steht eine Forderung nach Zahlung, damit Dateien wieder zugänglich werden oder angeblich gestohlene Daten nicht veröffentlicht werden. Oft nennt sie eine Frist und einen Kontaktweg für die Verhandlung.

- Vollbildmeldung mit Countdown und Zahlungsadresse
- Textdatei in jedem Ordner mit Zahlungsanweisung
- Mail mit der Drohung, Daten zu veröffentlichen
- Dateien tragen plötzlich eine fremde Endung

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Gerät sofort vom Netzwerk und WLAN trennen, damit die Verschlüsselung nicht auf Netzlaufwerke weiterläuft.

02 Gerät eingeschaltet lassen und nicht neu starten.

03 Geschäftsführung und IT unverzüglich telefonisch verständigen. Das ist ein Führungsthema, kein IT-Detail.

04 Foto oder Screenshot der Forderung samt Frist und Kontaktweg sichern, am besten mit dem Handy.

05 Auf nichts antworten und nichts anklicken, auch nicht auf den angebotenen Entschlüsselungstest.

## Melden

SOFORT

WEN

Geschäftsführung und IT-Verantwortliche sofort, gemeinsam. Die Entscheidung über das weitere Vorgehen liegt bei der Leitung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über Mail oder Chat, die möglicherweise mitgelesen werden.

WAS BEREITHALTEN

- Wortlaut der Forderung und genannte Frist
- Welche Laufwerke und Ordner betroffen sind
- Seit wann die Dateien nicht mehr lesbar sind
- Ob weitere Geräte im Haus Auffälligkeiten zeigen
- Ob das Gerät noch am Netz hing, als es bemerkt wurde

## Nicht tun

HÄUFIGE FEHLER

- × Auf die Forderung antworten oder in Verhandlungen treten. Das entscheidet ausschließlich die Geschäftsführung.
- × Zahlen. Es gibt keine Zusicherung, dass Daten zurückkommen oder unveröffentlicht bleiben.
- × Betroffene Dateien löschen oder mit Wiederherstellungsprogrammen experimentieren.
- × Eine Sicherung einspielen, bevor geklärt ist, ob der Zugang der Täter noch besteht.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Geschäftsführung entscheidet über Anzeige, Einbindung der Versicherung und externe Unterstützung bei der Aufarbeitung.
- → Sind personenbezogene Daten betroffen, läuft parallel die Frist für die Meldung an die Datenschutzbehörde.
- → Fällt das Unternehmen unter NIS2, prüft die Leitung die Meldepflicht nach dem NISG 2026: Frühwarnung binnen 24 Stunden.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Ransomware (MAL-03) · Verdacht auf Datenschutzverletzung (DAT-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK CLD-01

# Verdacht auf kompromittiertes Cloud-Konto

Cloud & Zusammenarbeit

In einem Cloud-Dienst wie Microsoft 365 oder Google Workspace passieren Dinge, die niemand veranlasst hat. Anders als bei einem einzelnen Postfach hängen daran Dateien, Freigaben und verbundene Anwendungen des gesamten Unternehmens.

- Dateien in SharePoint oder Drive plötzlich geändert oder verschwunden
- Unbekannte App hat Zugriff auf das Konto erhalten
- Neue Freigabelinks für Ordner, die niemand erstellt hat
- Anmeldung aus einem Land ohne Standort des Unternehmens

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Passwort von einem anderen, sauberen Gerät aus ändern und alle aktiven Sitzungen im Konto abmelden.

02 In den Kontoeinstellungen die verbundenen Apps und erteilten Berechtigungen ansehen und Auffälliges notieren.

03 Neu entstandene Freigabelinks und Zugriffsrechte notieren, bevor sie entfernt werden.

04 Die lokale Synchronisierung pausieren, damit Änderungen aus der Cloud nicht weiter auf die Geräte gespielt werden.

05 Unverzüglich melden. Cloud-Vorfälle betreffen fast nie nur ein Konto.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister mit Administrationsrechten für den Cloud-Dienst. Bei Administratorkonten zusätzlich die Geschäftsführung.

WIE

Telefonisch über den Notfallkontakt aus dem Kontaktblatt. Nicht über den betroffenen Cloud-Dienst, also weder per Mail noch per Chat darin.

WAS BEREITHALTEN

- Welcher Dienst und welches Konto betroffen sind
- Welche Auffälligkeit dir zuerst begegnet ist und wann
- Welche verbundenen Apps du gefunden hast
- Welche Ordner oder Dateien betroffen scheinen
- Ob das Konto Administrationsrechte hat

## Nicht tun

HÄUFIGE FEHLER

- × Über den betroffenen Dienst selbst melden oder dort über den Vorfall chatten.
- × Verbundene Apps und Freigaben löschen, bevor sie festgehalten sind.
- × Dateien aus dem lokalen Ordner in die Cloud zurückspielen, um Änderungen zu reparieren.
- × Externe Empfänger von Freigabelinks eigenständig kontaktieren.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Administration prüft die Anmelde- und Aktivitätsprotokolle des Mandanten und grenzt ein, welche Konten betroffen sind.
- → Erteilte App-Berechtigungen werden entzogen, Freigaben zurückgenommen und Anmeldedaten samt Multi-Faktor-Authentifizierung neu aufgesetzt.
- → Anhand der Protokolle wird bewertet, ob Daten abgeflossen sind und ob daraus eine Meldepflicht folgt.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Kontoübernahme (ACC-03) · Verdacht auf Datenschutzverletzung (DAT-05) · Interne Kontakte siehe Incident-Kontaktblatt

INCIDENT-PLAYBOOK SUP-01

# Verdacht auf kompromittierten Lieferanten

Lieferanten & Softwareentwicklung

Ein Lieferant, Dienstleister oder Softwareanbieter meldet einen Sicherheitsvorfall, oder seine Kommunikation wirkt plötzlich auffällig. Der Angriff trifft ein anderes Unternehmen, die Auswirkungen landen trotzdem im eigenen Betrieb.

- Lieferant informiert über einen Sicherheitsvorfall
- Bekannter Ansprechpartner schickt plötzlich seltsame Anhänge
- Mail mit geänderten Bankdaten eines Lieferanten
- Softwareanbieter warnt vor manipuliertem Update

## Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine Zahlung freigeben und keine Stammdaten ändern, solange der Vorfall nicht geklärt ist.

02 Aktuelle Mails und Anhänge dieses Lieferanten nicht öffnen und nichts installieren, was von dort kam.

03 Rückfragen ausschließlich über eine bekannte Telefonnummer aus dem eigenen System, nie über Kontaktdaten aus der verdächtigen Nachricht.

04 Festhalten, welche Zugänge dieser Lieferant zu internen Systemen hat, etwa Fernwartung, Portal oder Schnittstelle.

05 Sofort melden, auch wenn der Vorfall beim anderen Unternehmen passiert ist.

## Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die für den Lieferanten zuständige Fachabteilung. Bei Zahlungsbezug zusätzlich Buchhaltung und Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Verdächtige Nachrichten als Anhang weitergeben, nicht als Weiterleitung mit anklickbaren Links.

WAS BEREITHALTEN

- Um welchen Lieferanten es geht
- Woher die Information über den Vorfall stammt
- Welche Zugänge oder Schnittstellen bestehen
- Ob offene Zahlungen oder Bestellungen laufen
- Ob zuletzt Software oder Updates von dort kamen

## Nicht tun

HÄUFIGE FEHLER

- × Geänderte Bankdaten übernehmen, weil die Mail vom bekannten Ansprechpartner kommt.
- × Die Rückfrage über die Kontaktdaten aus der verdächtigen Nachricht stellen.
- × Den Fernwartungszugang des Lieferanten stillschweigend offen lassen, bis sich jemand meldet.
- × Andere Kunden oder Partner des Lieferanten eigenständig warnen.

## Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT sperrt oder beschränkt die Zugänge des Lieferanten und prüft die Protokolle auf Zugriffe über diesen Weg.
- → Die Fachabteilung klärt über einen gesicherten Kanal, welche Daten und Prozesse betroffen sind, und dokumentiert die Antworten.
- → Sind eigene personenbezogene Daten betroffen, folgt die Bewertung nach Art. 33 DSGVO durch die Datenschutz-Ansprechperson.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen, ob daraus ein erheblicher Cybersicherheitsvorfall im eigenen Haus wird, der nach § 34 zu melden ist.

**Verweise:** Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Insights zu Drittparteien und Lieferkette · Interne Kontakte siehe Incident-Kontaktblatt