Baobab
Risk Solutions

Data Breach Report

Der Mittelstand als leichtes Ziel

Einleitung

Als Assekuradeur für digitale Risiken bewerten wir bei Baobab kontinuierlich beide Dimensionen des Risikos: Die technische Schwachstelle vor dem Angriff und den finanziellen Schaden danach. Unsere Datenauswertung offenbart: Es zieht sich ein Riss durch die Sicherheitslandschaft.

Während Großunternehmen ihre digitalen Türen zunehmend verriegeln, stehen sie im Mittelstand oft noch weit offen.

Doch unsere Daten zeigen auch Hoffnung: Die meisten Angriffe sind nicht hochkomplex, sondern opportunistisch.
Das bedeutet: Unternehmen sind dem Risiko nicht hilflos ausgeliefert. Mit den richtigen Maßnahmen lässt sich die Gefahr drastisch reduzieren.

Unsere Erkenntnisse basieren auf der kontinuierlichen Analyse von Deep Scans und Quotierungsdaten aus Angebotsprozessen. Auch wenn dieser Datensatz keinen Anspruch auf eine vollständige statistische Repräsentativität für den gesamten Markt erhebt, lassen die schiere Masse der untersuchten Fälle und die Langzeitbeobachtung klare, belastbare Trends erkennen.

Inhalt

Datenlage

>10.000 Angriffsoberflächenscans ausgewertet

57.660 geleakte Datensätze aus 5.000 Quellen analysiert

>100 reale Schadensfälle kategorisiert

>100 externe Ransomwarefälle untersucht

Zusammenfassung

88,7% der geleakten Daten wiederholen sich

Hacker müssen das Rad nicht neu erfinden. Die Mehrheit der im Darknet gefundenen Zugangsdaten stammt aus massiven, historischen Aggregationen. Wer einmal im Netz der Info-Stealer landet, bleibt dort über Jahre als Ziel markiert, da Daten systematisch neu verpackt und automatisiert gegen Netzwerke eingesetzt werden.

Passwörter reichen nicht als Schutzwall

Die Komplexität eines Passworts ist zweitrangig, wenn es im Klartext (Plaintext) in Datenbanken zum Verkauf steht. Unsere Analyse zeigt: Ohne Multi-Faktor-Authentifizierung (MFA) bleibt der initiale Zugang trivial. Angreifer brechen nicht ein, sie melden sich einfach mit validen, billig erworbenen Credentials an.

75% aller Gefahren sind konzentriert

Der externe Angriffsfokus liegt überwiegend auf Netzwerk-Perimeter (VPNs/Firewalls) und Kollaborationstools (E-Mail). Diese beiden Kategorien machen rund drei Viertel der gesamten Bedrohungslage aus und decken nahezu alle Zero-Day-Signale ab. Entsprechend liegt die Priorität auf der Absicherung internetexponierter Systeme, da Angriffe hier besonders häufig sind.

Datenreichtum schlägt Umsatzgröße

Der Irrglaube „Wir sind zu klein, um ein Ziel zu sein“ ist lebensgefährlich. Hacker messen Attraktivität nicht am Umsatz, sondern an der Menge personenbezogener Daten (PII). Schon bei Unternehmen unter 5 Mio. € Umsatz verwalten 31 % mehr als 10.000 Datensätze – ein perfektes Ziel für Angriffe.

Statt einbrechen, einfach anmelden

Es ist ein häufiger Irrglaube, dass Cyberkriminelle hochkomplexen Code entwickeln müssen, um Firewalls zu überwinden. Die Realität ist deutlich banaler und wirtschaftlicher: Warum mühsam einbrechen, wenn man den Schlüssel für wenige Euro im Darknet kaufen kann? Kompromittierte Identitäten sind heute die billigste und effektivste Waffe im Arsenal der Angreifer.

Das Archiv des Schreckens

Unsere Analyse zeigt, dass Hacker nur selten komplexe Verschlüsselungen umgehen müssen. Die Mehrheit der im Darknet gefundenen Zugangsdaten liegt im Klartext (Plaintext) vor – sie sind sofort lesbar und einsatzbereit.

91% der analysierten Leaks enthalten Klartext-Passwörter. Das macht den initialen Zugriff für Angreifer trivial und kosteneffizient.

Diese einfache Verfügbarkeit von Passwörtern macht Cyberkriminalität nicht nur einfach, sondern auch höchst lukrativ. Ein Beispiel aus einem von uns analysierten Telegramkanal verdeutlicht das Geschäftsmodell: Über ein einfaches Abonnement erhalten Käufer dort wöchentlich Zugriff auf mindestens 5.000 Datensätze.

Beispiel eines Darknet-Angebots

Quelle: Darknet-Telegram-Channel

Angebot

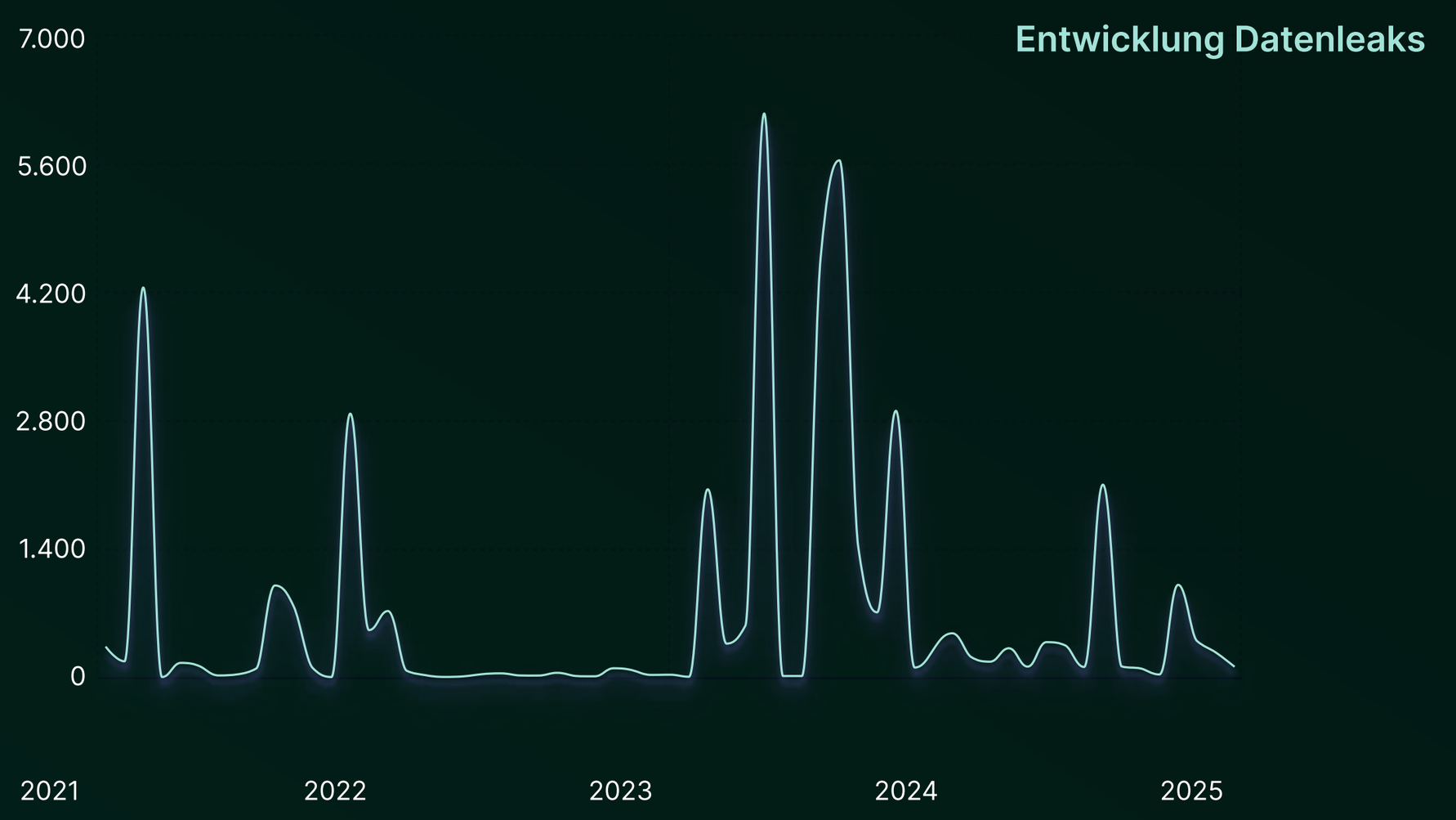
- Zugang zum exklusiven Kanal
- Täglich 5.000 - 15.000 gestohlene Daten
- Monatsabonnement inklusive Transfer von 45.000 Logs

Preise

- Eine Woche: 75$
- Zwei Wochen: 150$
- Ein Monat: 250$
- Drei Monate: 600$

Mega-Breaches zu Info-Stealern

Während in der Vergangenheit Einzeldiebstähle bei Konzernen wie Adobe oder LinkedIn die Schlagzeilen dominierten, sehen wir aktuell eine Verschiebung hin zu Info-Stealer-Logs.



Was sind Info-Stealer?

Hierbei handelt es sich um Schadsoftware, die sich unbemerkt auf Endgeräten einnistet und dort Zugangsdaten direkt aus dem Browser, aus Passwort-Managern oder aus aktiven Sitzungen (Session-Cookies) extrahiert.

Diese Logs sind besonders gefährlich, da sie oft aktuelle Passwörter enthalten und einmal geleakte Daten bleiben im Umlauf. Unsere Daten belegen eine Duplikationsrate von rund 88,7 % – das bedeutet, dieselben gestohlenen Daten tauchen immer wieder in verschiedenen Datensammlungen auf.

Chandan Raj Nivanda
Cyber Security Researcher

"Wir beobachten eine deutliche Verschiebung in der Angriffsstrategie: weg von singulären, massiven Server-Hacks hin zur Skalierung durch tausende kleine Info-Stealer-Infektionen."

Das Ausmaß der Sicherheitslücke

Viele Unternehmen glauben, dass ein Datenleck nur ein oder zwei einzelne Konten betrifft. Unsere Analyse offenbart jedoch ein weitaus systemischeres Risiko: Für das Durchschnittsunternehmen ist die Gefährdung kein kleiner Flüchtigkeitsfehler, sondern ein massives Problem, das eine Vielzahl kompromittierter Passwörter umfasst.

Mehrfach-Leaks

Unsere Analyse identifizierte **durchschnittlich 18 Zugangsdatensätze pro Unternehmen.**

Hohe Gefahr

In einigen Unternehmen ist das Risiko besonders hoch: Bei 23 Unternehmen wurden zwischen 100 und 400 individuelle Passwörter im Darknet gefunden.

Dauerhaftes Risiko

Wenn eine Domain wiederholt in diesen Datensätzen auftaucht, ist dies oft ein Zeichen dafür, dass Sicherheitslücken über Jahre hinweg ungelöst blieben. So häufen sich gestohlene Daten kontinuierlich an.

Das Passwort-Paradox

Trotz ständiger Warnungen von Systemanbietern vor unsicheren Passwörtern dominieren nach wie vor erschreckend vorhersehbare Muster. Unsere Analyse zeigt, dass die große Mehrheit der kompromittierten Zugangsdaten immer noch auf einfachen Zahlenfolgen basiert – wobei 123 der am häufigsten genutzte Startpunkt ist.

Typische Muster

Auch Vornamen wie Hannah und Michael oder Begriffe wie Backend, Klingel und Star Wars tauchen häufig auf.

Die häufigsten Passwörter

Rank 1	12345678
Rank 2	123456

Analysierte Muster

Kurze Wörter · Filmtitel · Städte · Namen · Nummern

Das Risiko

Ob einfache Zahlenfolgen wie 123456 oder triviale Begriffe wie Starwars – die Nutzung schwacher Passwörter bleibt ein hohes Risiko. Zwar werden solche Passwörter vermehrt im privaten Kontext genutzt, wie beispielsweise für die digitale Essenbestellung.

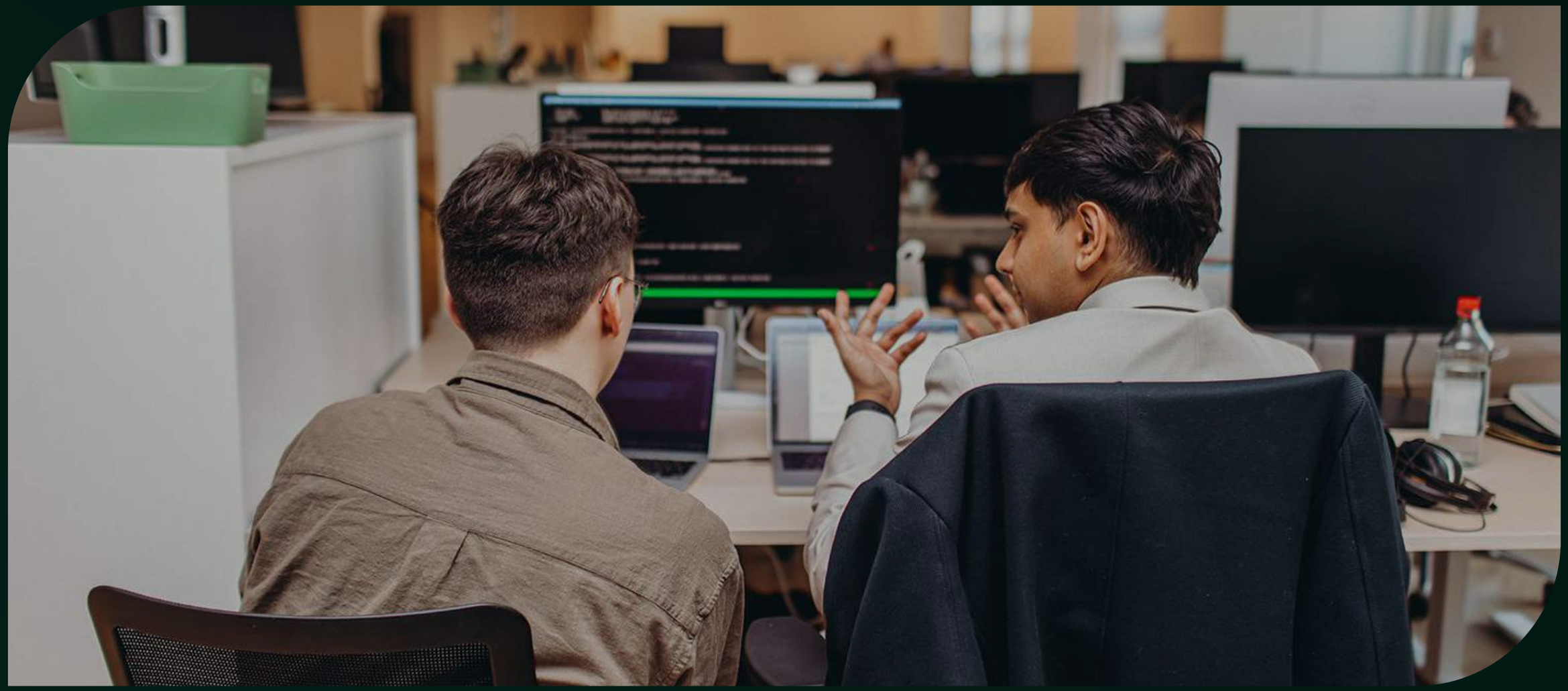
Doch die Gefahr reicht tiefer: Unsere Analyse zeigt, dass selbst komplexe, zufällig generierte Zeichenfolgen massenhaft in Leaks auftauchen.

Andrew Saula
Head of Cybersecurity

"Kriminelle Gruppierungen machen sich heute nicht mehr die Mühe, Passwörter mühsam zu knacken; sie fügen kompromittierte Zugangsdaten direkt in automatisierte Tools ein (Credential Stuffing). Ohne zusätzliche Faktoren wie Multi-Faktor-Authentifizierung(MFA) bleibt der initiale Zugang zur Unternehmensarchitektur trivial, völlig ungeachtet der Passwortkomplexität."

Die Angriffsfläche

Während kompromittierte Passwörter die primäre Zugangskontrolle umgehen, verhalten sich Software-Schwachstellen wie unsichtbare Risse im Fundament der IT-Architektur. Um diese Risiken zu identifizieren, durchleuchtet unsere Deep-Scan-Technologie die IT-Infrastruktur unserer Kunden und prüft diese bei jedem Durchlauf auf 10.355 Schwachstellen (CVEs).



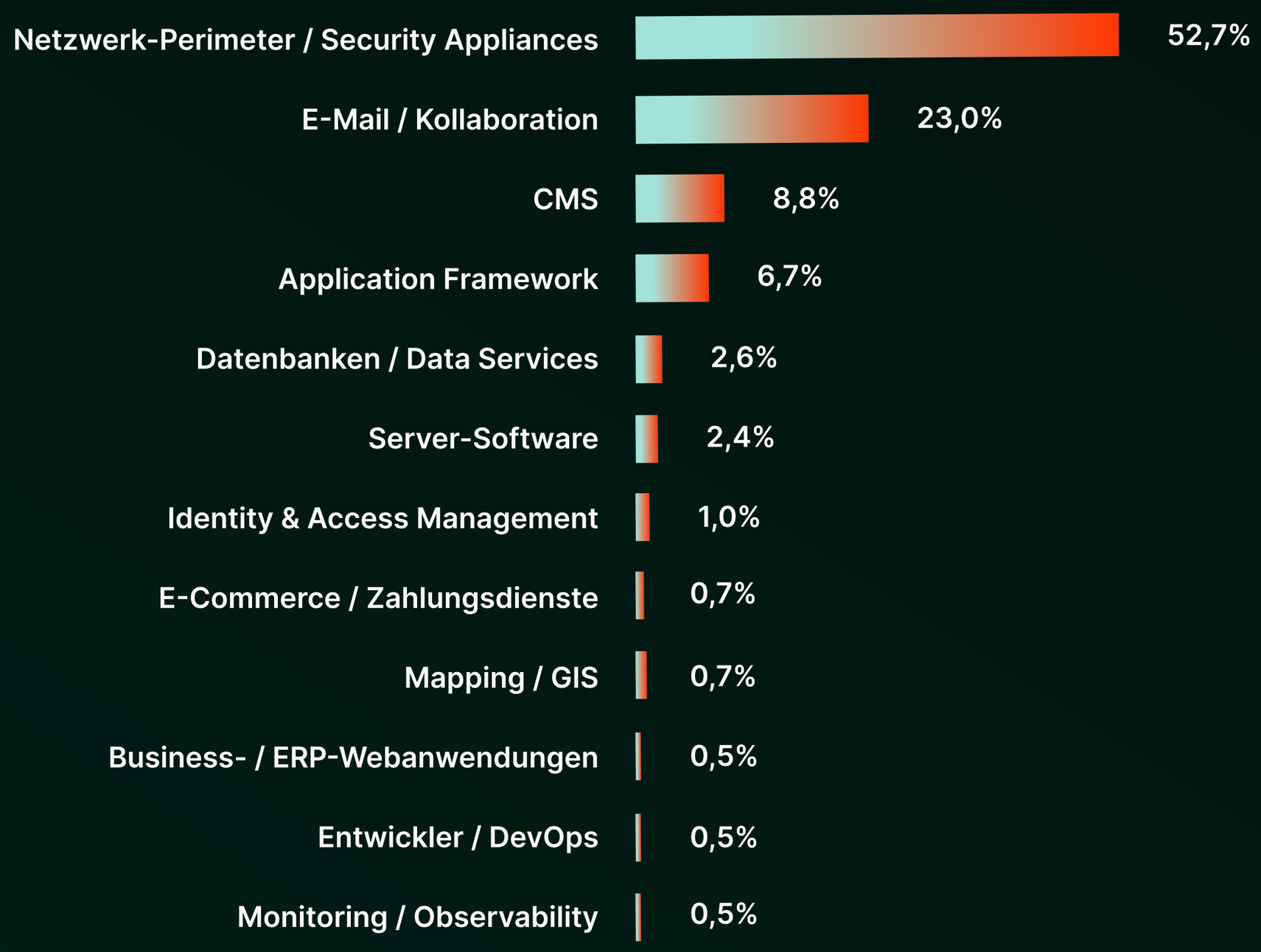
Die unterschätzten Lücken

Bei Cyberbedrohungen ist die Gefahr nicht gleichmäßig verteilt, sondern konzentriert. Der externe Angriffsfokus im Mittelstand liegt fast ausschließlich auf dem Network Edge (Netzwerk-Peripherie) und Kollaborations-Technologien. Diese beiden Kategorien machen drei Viertel der gesamten Bedrohungslage aus und decken fast alle aktiven oder Zero-Day-Signale ab. CMS und Application-Frameworks bleiben zwar relevant, rangieren jedoch deutlich hinter dieser ersten Risikostufe.

Für Unternehmen ist die Priorität bei der Verteidigung damit klar: Sichern Sie zuerst die zum Internet hin exponierten Ebenen. Hier sind Angriffe am hartnäckigsten und die potenziellen Schäden am größten.

75% aller kritischen Bedrohungsaktivitäten konzentrieren sich auf zwei Bereiche: den Network Edge (VPNs/ Firewalls) und Kollaboration-Tools (E-Mail).

Häufigsten Angriffsziele nach Technologie



Kleine Unternehmen, große Chancen

Unsere Daten zeigen eine klare Korrelation zwischen Unternehmensgröße und Patch-Disziplin. Während Großunternehmen meist über spezialisierte Teams für das IT-Sicherheit verfügen, hängen kleinere Organisationen hier häufig hinterher:

12,7%

kritische Schwachstellen weisen Unternehmen mit weniger als 1 Mio. € Umsatz auf.

6,23%

kritische Schwachstellen weisen Unternehmen mit mehr als 100 Mio. € Umsatz auf.

Veraltete Software

Je kleiner das Unternehmen, desto älter ist oft die Software. Veraltete VPN-Gateways oder ungepatchte Exchange-Server sind wie offene Fenster im Erdgeschoss – eine Einladung für Ransomware-Gruppen.

Während die Systemwartung in Konzernen von dedizierten IT-Abteilungen gesteuert wird, wird sie in KMUs mangels Personal oft nur reaktiv oder nebenbei erledigt. Genau dieses Fehlen fester Ressourcen erklärt, warum sich die kritische Schwachstellen bei Unternehmen ab 100 Mio. € Umsatz fast halbiert.

Klein im Umsatz, groß im Risiko

Ein gefährlicher Irrglaube hält sich hartnäckig in der Geschäftsführung kleinerer Unternehmen: „Wir sind zu klein, um ein Ziel zu sein.“ Der Trugschluss basiert auf der Annahme, Angreifer würden ihre Ziele manuell auswählen. Die heutige Realität wird jedoch von massenhafter Automatisierung dominiert. Tätergruppierungen scannen das gesamte Internet im Sekundentakt nach offenen Schwachstellen und ungeschützten Schnittstellen ab. Ein automatisierter Bot-Scan sucht lediglich nach dem Weg des geringsten Widerstands. Wer eine Schwachstelle aufweist, wird zum Ziel.

Unsere Analyse zeigt: Die Attraktivität für Hacker wird nicht am Umsatz gemessen, sondern an den Daten.

Der versteckte Schatz

Wir haben Unternehmen mit weniger als 5 Mio. € Jahresumsatz analysiert. Das Ergebnis widerlegt den Mythos der Unwichtigkeit:

31% aller Kleinunternehmen verwalten mehr als 10.000 PII-Datensätze.

PII-Preise

Ein einzelner gestohlener Datensatz kostet im Durchschnitt etwa 134€. Verliert ein Unternehmen 10.000 Datensätze, liegt der theoretische Gesamtschaden schnell bei 1,34 Mio. €. Für ein Unternehmen mit weniger als 5 Mio. € Jahresumsatz ist das existenzbedrohend.

11% aller Kleinunternehmen verwalten zwischen 100.000 und sogar 500.000 Datensätze.

Für einen Angreifer ist ein solches Unternehmen eine Goldgrube. Ein Datensatz ist auf dem Schwarzmarkt bares Geld wert – der Umsatz ist dem Hacker dabei egal. Selbst wenn der Hacker die Daten nicht weiterverkauft, sind sie extrem wertvoll. Bei modernen Ransomware-Angriffen wie Double Extortion werden die Systeme nicht mehr nur verschlüsselt, sondern die Daten vorher unbemerkt kopiert und exfiltriert.

Der Hacker droht dem Unternehmen dann: „Wenn du kein Lösegeld zahlst, veröffentliche ich die Daten deiner Kunden.“ Die Angst vor empfindlichen DSGVO-Strafen, Klagen der Kunden und einem Reputationsverlust zwingt das Unternehmen oft zur Zahlung. Die eigenen Daten werden so zur perfekten Geisel.

Das fehlende Schutzschild

Trotz dieses Risikos fehlt oft der wichtigste Schutz: Die Multi-Faktor-Authentifizierung (MFA). Unsere Daten zeigen: erst ab 50 Mio. € Umsatz gehört MFA zum Standard in der IT-Sicherheit.

Statistik: Unternehmen ohne MFA

Gefährliche Lücke

Fatih Kenar
Cyber Security Analyst

"Kleine Unternehmen haben so wichtige Daten wie Konzerne, verzichten aber auf wichtige Sicherheitsstandards. Dabei könnte MFA diese Lücke einfach schließen. Sie stellt sicher, dass ein Login nur dann erfolgreich ist, wenn neben dem Passwort ein zweiter, persönlicher Beweis wie ein Code auf dem Firmenhandy erbracht wird. Selbst wenn Hacker ein gestohlenes Passwort besitzen, scheitern sie an dieser entscheidenden Hürde."

MFA als NIS2-Anforderung

Mit der NIS2-Richtlinie ist MFA nun europaweit zur gesetzlichen Pflicht geworden. Das bedeutet: Für Unternehmen innerhalb der EU ist das Fehlen von MFA kein bloßes Sicherheitsversäumnis mehr, sondern ein regulatorisches Haftungsrisiko, das zu erheblichen Bußgeldern und rechtlichen Konsequenzen führen kann.

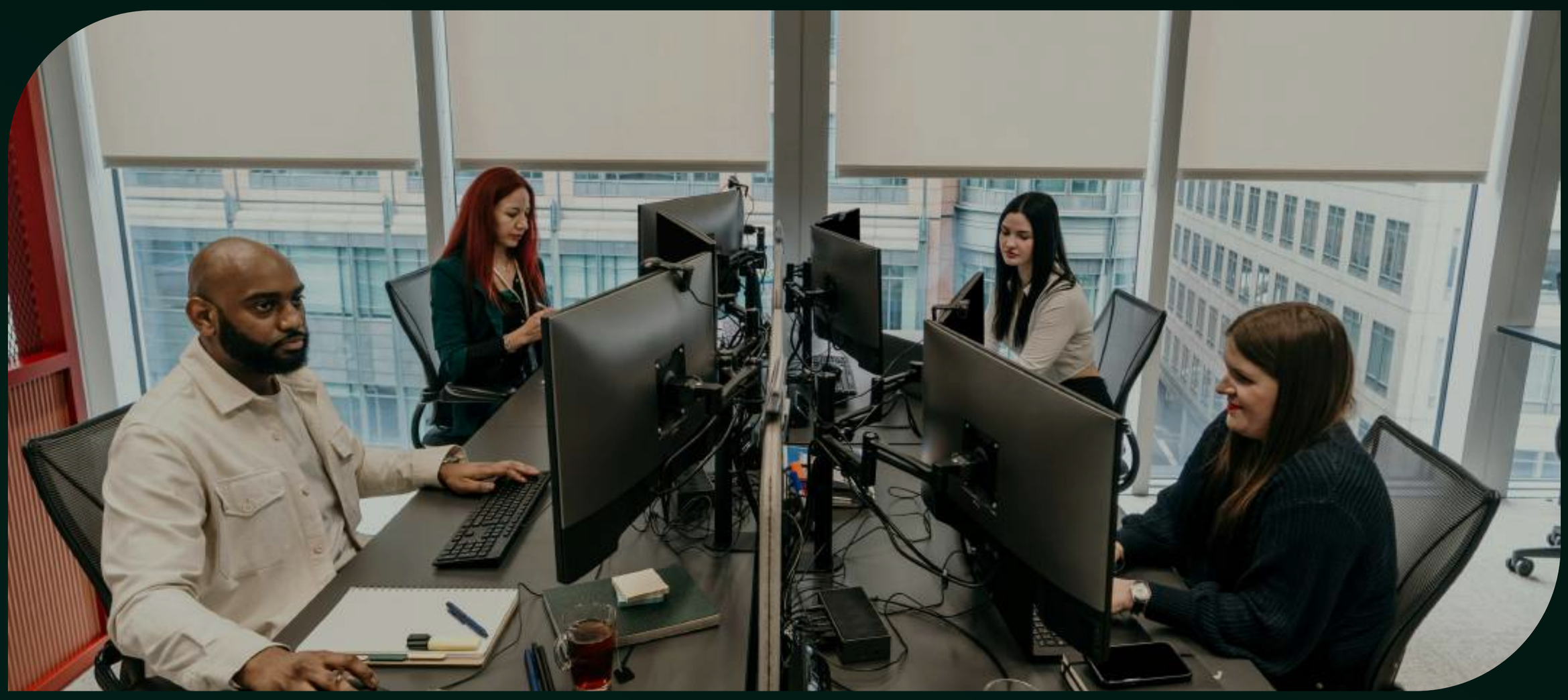
6.12.2025 markiert das Datum, an dem die NIS2-Richtlinie für betroffene Unternehmen in Deutschland rechtsverbindlich wurde.

Frederik Schwarz
Cyber Security Analyst

„Die NIS2-Richtlinie ist ein wichtiger Schritt für die europäische Cybersicherheit und schafft die dringend benötigte Verbindlichkeit für Unternehmen. Die eigentliche Herausforderung liegt jedoch in der Umsetzung: Der gesetzliche Druck ist hoch, während interne Ressourcen oft knapp sind. Entscheidend ist daher nicht mehr, ob Sicherheit verbessert wird, sondern wie schnell diese Lücke geschlossen werden kann.“

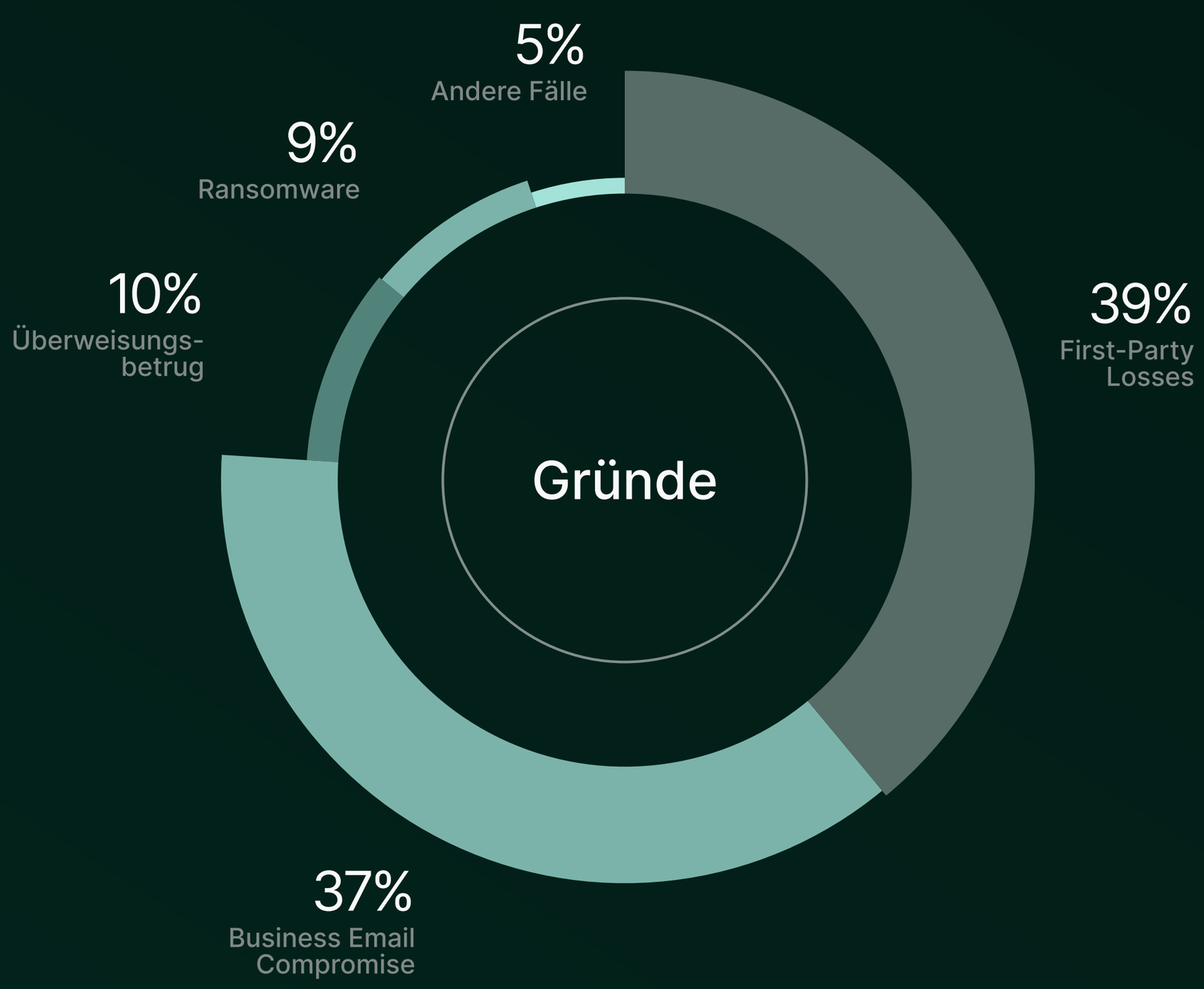
Die Kunst der Schadensbegrenzung

Wenn die Prävention versagt, greift das Krisenmanagement. Unsere Schadendaten geben einen nüchternen Einblick in die Realität während und nach dem Angriff.



Ursachen für finanzielle Schäden

Technische Hacks sind seltener Grund für finanzielle Schäden. In den meisten Fällen spielt der Mensch die entscheidende Rolle. Die häufigsten Gründe für finanzielle Schäden sind:



Awareness-Schulungen

Quelle: ENISA Threat Landscape 2025

Da First-Party Losses (wie Phishing) mit 39% das größte Risiko darstellt, wäre eine flächendeckende Sensibilisierung der Belegschaft wichtig.

Doch die Realität ist anders: Unsere Daten zeigen, dass 46 % der großen Unternehmen (über 100 Mio. € Umsatz) keine Phishing-Simulationen durchführen. Dass nahezu die Hälfte dieser ressourcenstarken Unternehmen solche Standards vernachlässigt, offenbart eine Schwachstelle.

Besonders da bereits 2025 80 %* der Social-Engineering-Angriffe durch Künstliche Intelligenz durchgeführt wurden. Ohne regelmäßiges Training sind solche Phishing-Mails von echten Nachrichten kaum noch zu unterscheiden.

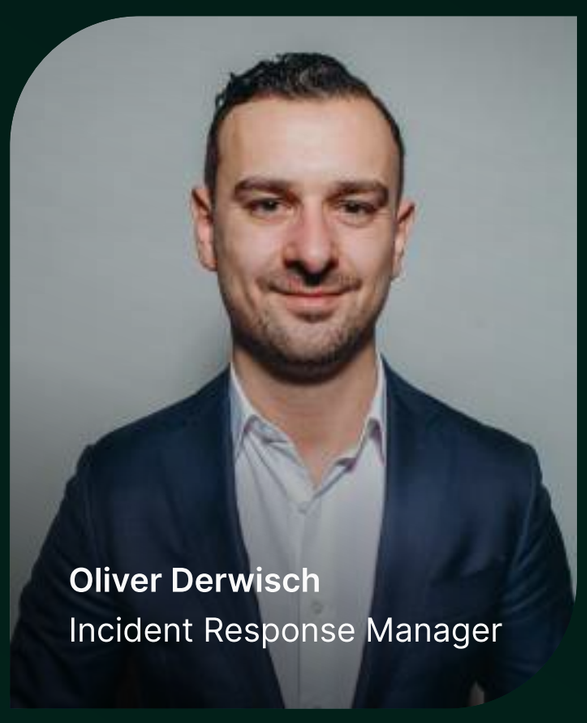
Der Preis der Erpressung

Ransomware bleibt ein teures Risiko. Unsere Analyse von 245 realen Ransomware-Fällen zeigt: Die Erstforderungen (Initial Demands) liegen teilweise sogar bei 2,59 Mio. $. Während sich die Mehrheit der Forderungen im Bereich zwischen 100.000 $ und 500.000 $ bewegt, übersteigen fast 30 % der Forderungen die Millionen-Dollar-Marke.

Verhandeln lohnt sich

Entgegen der Panikreaktion vieler Betroffener ist die erste Forderung so gut wie nie der Endpreis. Professionelle Unterstützung hilft dabei, den finanziellen Schaden zu begrenzen.

51% durchschnittliche Preisreduzierung durch Verhandlung mit einem Incident-Response-Experten.



Oliver Derwisch
Incident Response Manager

„Lösegeldzahlungen sind selten die richtige Lösung. Wahre Resilienz entsteht durch Vorbereitung und ein strukturiertes Incident Response Management – indem der Schaden begrenzt, die Wiederherstellung ermöglicht und eine Zahlung in den meisten Fällen überflüssig gemacht wird.“

Verhandlungs-beispiel

Quelle: Ransomware.live

260.000 $ wenn Sie heute zahlen.

Wir können heute 155.000 $ zahlen.

220.000 $ heute. Hier ist unsere BTC-Wallet. Geben Sie Bescheid, wenn Sie bereit zur Zahlung sind.

Nicht einfach zahlen

Trotz dieser Verhandlungsergebnisse empfiehlt es sich, Erpressern kein Geld auszuzahlen. Denn in der überwiegenden Mehrheit der Fälle blieben Angreifer erfolglos. Warum? Weil die Backups funktionierten und Incident-Response-Experten eingriffen.

Rund 77 % der betroffenen Unternehmen zahlten kein Lösegeld.

Die Backup-Illusion

Doch ein funktionierendes Backup ist keine Selbstverständlichkeit. Unsere Daten offenbaren einen Leichtsinn bei Konzernen:

21 % der Großunternehmen (über 100 Mio. € Umsatz) testen ihre vollständige Wiederherstellung nicht regelmäßig.

Ohne regelmäßige Validierung der Wiederherstellungsprozesse bieten Backups im Ernstfall keine operative Sicherheit, sondern ein unkalkulierbares Restrisiko.

Widerstandsfähigkeit statt Panik

IT-Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Die gute Nachricht: Es muss keine digitale Festung sein. Für KMU ist die Etablierung ausgewählter Schutzmechanismen der entscheidende Hebel. Drei konkrete Praktiken genügen, um die Resilienz zu steigern.

1. Digitale Identitäten mit MFA absichern

Eine strikte Multi-Faktor-Authentifizierung (MFA) sollte über die gesamte IT-Infrastruktur implementiert werden – für alle internen Mitarbeiter, externen Dienstleister und sämtliche Zugangspunkte (VPN, Cloud-Dienste, E-Mail-Tenants). MFA ist der beste Mechanismus zum Schutz bei kompromittierten Zugangsdaten und gestohlener Passwörter.

2. Angreifer einfach blockieren

KI-gestütztes Phishing macht Täuschungen zunehmend realitätsnah. Für echte Resilienz braucht es daher technische Schutzmechanismen statt reiner Sensibilisierung. Phishing-Simulationen fördern zwar das Bewusstsein, entscheidend ist jedoch der Einsatz von Managed Detection and Response (MDR). In Kombination mit Zero Trust und 24/7-Überwachung werden Bedrohungen in Echtzeit erkannt und neutralisiert – selbst wenn schädliche Links geklickt werden.

3. Operative Resilienz mit verifizierten Backups sichern

Ein ungetestetes Backup ist keine Sicherheitsmaßnahme, sondern nur eine vage Hoffnung. Viele Großunternehmen machen den Fehler, sich auf automatisierte Speicherroutinen zu verlassen. Mindestens einmal jährlich sollte ein vollständiger Disaster-Recovery-Test (Wiederherstellungstest) durchgeführt werden. Eine verifizierte, offline verfügbare Datensicherung bleibt das stärkste und einzige verlässliche Instrument gegen Double-Extortion-Ransomware.

Wir schließen die Lücke

Baobab Risk Solutions ist einer der führenden europäischen Anbieter für die Absicherung von digitalen Risiken. Als spezialisierter Managing General Agent (MGA) versteht Baobab digitale Risiken durch tiefgreifende, datenbasierte Analysen und bietet proaktiven Schutz als elementaren Bestandteil der Versicherungspolice.

Das Unternehmen arbeitet mit exzellent bewerteten Lloyd's-Syndikaten sowie Zurich und Liberty Specialty Markets zusammen, die als Kapazitätsgeber fungieren. Etablierte Venture-Capital-Geber – wie Viola FinTech oder eCapital – sorgen für langfristige finanzielle Stabilität.

Seit 2022 bietet Baobab die Cyberversicherung Cyber Safe am Markt an. Die Vertrauensschadenversicherung Crime und die IT-Haftpflichtversicherung oneIT-protect komplementieren das Produktportfolio.

Baobab Risk Solutions mit Hauptsitz in Deutschland ist außerdem in Österreich und den Benelux-Staaten tätig.

Baobab Risk Solutions
Cyber-, Versicherungs- und Underwriting-Experten

BRS arbeitet mit etablierten Kapazitätsgebern zusammen

Baobab
Risk Solutions

baobab.io