BLACKVEIL
CYBER SECURITY

Dark Web Leaks im DACH-Mittelstand

Systematische Analyse von 1.976 Unternehmen aus Deutschland, Österreich und der Schweiz

STUDIE Q1 2026

Blackveil Cybersecurity GmbH
Marcus Henschel, CEO
April 2026

Die wichtigsten Zahlen auf einen Blick

Basierend auf der Analyse von 1.976 DACH-Unternehmen — Q1 2026

68,1%
UNTERNEHMEN BETROFFEN

9.390
CREDENTIAL-DATENSÄTZE

Ø 7
LEAKS PRO FIRMA

3.411
E-MAILS EXPONIERT

> „Die Frage ist nicht mehr, ob ein Unternehmen Credentials im Dark Web hat — sondern ob es davon weiß und wie viele."
>
> — Marcus Henschel, CEO Blackveil Cybersecurity GmbH

Wie wir 1.976 Unternehmen analysiert haben

Für diese Studie haben wir systematisch mittelständische Unternehmen aus dem DACH-Raum geprüft — alle mit mehr als 50 Mitarbeitern.

- **Strenge Suchkriterien: Nur vollständige Credentials**
  Als Fund zählen ausschließlich vollständige Kombinationen aus URL + Benutzername + Passwort. Teilbefunde wurden bewusst ausgeschlossen.
- **Nur Leaks der letzten 3 Monate — keine historischen Archive**
  Der Scan-Zeitraum war bewusst auf aktuelle Funde begrenzt. Eine Leak-Quote von 68,1% unter dieser Einschränkung bedeutet: frisch kompromittierte, potenziell noch aktive Zugangsdaten.
- **Die tatsächliche Leak-Rate liegt wahrscheinlich noch höher**
  Durch den Ausschluss von Teilbefunden und historischen Daten bilden unsere Zahlen eine konservative Untergrenze.

68% ist kein Ausreißer — es ist der Normalzustand

Von den 1.976 analysierten Unternehmen wiesen 1.344 mindestens einen bestätigten Dark Web Leak auf

1.344 von 1.976 Unternehmen betroffen — das sind 68,1%

Nur 629 Unternehmen (31,9%) zeigten nach unseren strengen Kriterien keine Funde. Mehr als zwei Drittel haben vollständige Zugangsdaten im Dark Web.

Durchschnittlich 7 separate geleakte Credential-Datensätze pro Firma

Das sind keine Einzelvorfälle aus einem einmaligen Datenleck. In vielen Fällen handelt es sich um aktuelle Leaks aus mehreren Quellen — Infostealer-Malware, Phishing-Kampagnen oder Datenpannen bei Drittanbietern.

3.411 Unternehmens-E-Mail-Adressen in Leak-Datensätzen

Direkte Angriffsflächen für gezieltes Phishing, Account-Übernahmen und Business Email Compromise (BEC)-Angriffe.

Welche Daten landen im Dark Web?

Das Spektrum exponierter Unternehmensdaten geht weit über Passwörter hinaus

Infostealer-Logs

Malware auf Mitarbeiter-Geräten extrahiert alle gespeicherten Browser-Passwörter, Session-Cookies und Autofill-Daten — einschließlich VPN-Zugängen, E-Mail-Konten und internen Tools.

Drittanbieter-Datenpannen

Mitarbeiter verwenden Passwörter über mehrere Dienste hinweg. Wird ein SaaS-Tool gehackt, gehen die Unternehmens-Credentials mit.

Ransomware-Leak-Seiten

Ransomware-Gruppen stehlen und veröffentlichen Daten, bevor sie diese verschlüsseln. Interne Dokumente, Verträge und Zugangsdaten werden öffentlich zugänglich.

Paste-Sites und Telegram-Kanäle

Zugangsdaten werden in Echtzeit in Telegram-Leakgruppen und auf Paste-Sites geteilt und verkauft.

Welche Branchen sind am stärksten betroffen?

Einige Sektoren sind im Dark Web deutlich überrepräsentiert

	BRANCHE	BETROFFENE UNTERNEHMEN
1	Business Services	170
2	Maschinenbau	96
3	IT & Dienstleistungen	70
4	Beratung & Engineering	64
5	Maschinenbau & Anlagenbau	58
6	Immobilien	48
7	Elektronik & Elektrotechnik	43
8	Baugewerbe	42
9	Großhandel	41
10	Chemie & Pharma	40

Auffällig: Keine Branche in unserem Datensatz lag unter einer Leak-Rate von 50% — die Betroffenheit ist branchenübergreifend. Business Services führt die Liste an — ein Sektor mit hoher Mitarbeiterfluktuation, starker Abhängigkeit von Drittanbieter-Plattformen und häufigem unternehmensübergreifendem Datenaustausch.

Warum die meisten Unternehmen nichts davon wissen

Die große Mehrheit der betroffenen Unternehmen hat keine Ahnung, dass ihre Zugangsdaten im Dark Web kursieren

1 **Kein Monitoring vorhanden**
Die meisten mittelständischen Unternehmen überwachen Dark Web-Quellen nicht aktiv. Ohne kontinuierliches Scanning bleiben Leaks unentdeckt.

2 **Leaks tauchen Monate oder Jahre später auf**
Daten, die heute gestohlen werden, erscheinen oft erst 6–18 Monate später auf Dark Web-Märkten.

3 **Geleakte Daten verbreiten sich über viele Quellen**
Ein einzelner Credential-Datensatz taucht in Dutzenden Leak-Datenbanken, Telegram-Gruppen und Paste-Sites auf.

4 **Angreifer sind geduldig**
Gestohlene Zugangsdaten werden gesammelt, validiert und Monate später eingesetzt — für Ransomware oder als Einstiegspunkt.

Transparente Vorgehensweise

Für belastbare Ergebnisse

DATENQUELLE

Dark Web Monitoring Infrastruktur

Kontinuierliche Durchsuchung von Hacker-Foren, Telegram-Leakkanälen, Paste-Sites und Ransomware-Leak-Seiten nach exponierten Unternehmens-Zugangsdaten.

SCOPE

DACH-Raum

1.976 Unternehmen aus Deutschland, Österreich und der Schweiz. Mittelstand ab 50 Mitarbeitern.

ZEITRAUM

Letzte 3 Monate

Nur aktuelle Leaks — keine historischen Altdaten. Das stellt sicher, dass die Ergebnisse eine reale, aktive Bedrohung widerspiegeln.

KRITERIEN

Vollständige Credentials

Nur Datensätze mit URL + Benutzername + Passwort. Keine Hashes, keine unvollständigen Einträge. Die tatsächliche Rate liegt noch höher.

Hinweis: Diese Studie basiert auf öffentlich im Dark Web verfügbaren Daten. Es wurden keine Systeme aktiv getestet oder kompromittiert. Die Analyse dient ausschließlich der Sensibilisierung und Prävention.

Fazit

Die Zahlen sprechen für sich

- **68,1% der geprüften DACH-Unternehmen haben aktive Credentials im Dark Web**
  Unter strengen Suchkriterien und ausschließlich aktuellen Daten der letzten 3 Monate.
- **Die Bedrohung ist branchenübergreifend und betrifft den gesamten Mittelstand**
  Keine Branche liegt unter 50% Leak-Rate. Business Services, Maschinenbau und IT führen die Liste an.
- **Ohne Monitoring bleiben Leaks auf unbestimmte Zeit unentdeckt**
  Die große Mehrheit der betroffenen Unternehmen weiß nicht, dass ihre Zugangsdaten kompromittiert sind.

> „BlackVeil ermöglicht es Unternehmen, Anzeichen für potenzielle Cyberangriffe bereits bis zu 4 Monate vor ihrem Eintreten zu erkennen und proaktiv zu handeln."
>
> — Marcus Henschel, CEO Blackveil Cybersecurity GmbH

Was IT-Verantwortliche jetzt tun sollten

Die Maßnahmen mit der größten unmittelbaren Wirkung

1 **Erst Sichtbarkeit herstellen**

Man kann nicht auf Bedrohungen reagieren, die man nicht sieht. Eine einmalige Dark Web-Prüfung — oder idealerweise ein kontinuierliches Monitoring — zeigt, welche Mitarbeiter und Systeme exponiert sind.

2 **Unternehmens-E-Mail-Adressen priorisieren**

Jede geleakte Unternehmens-E-Mail-Adresse ist eine direkte Phishing-Angriffsfläche. Betroffene Konten sollten sofort Multi-Faktor-Authentifizierung aktivieren und Passwörter zurücksetzen.

3 **Nicht auf Breach-Benachrichtigungen warten**

Die meisten Dark Web-Leaks erzeugen nie eine öffentliche Benachrichtigung — die Verantwortung, sie zu entdecken, liegt beim Unternehmen selbst.

4 **Kontinuierlich monitoren, nicht nur einmalig**

Eine Momentaufnahme ist ein Anfang, keine Lösung. Täglich entstehen neue Leaks. Nur kontinuierliches Monitoring stellt sicher, dass man benachrichtigt wird, sobald eigene Daten auftauchen.

5 **Mitarbeiter einbeziehen, nicht nur Domains**

Viele Credential Leaks entstehen über private E-Mail-Adressen, die Mitarbeiter für berufliche Dienste verwendet haben. Ein robuster Ansatz deckt sowohl Unternehmensdomains als auch Schlüsselpersonen ab.

Ist Ihr Unternehmen betroffen?

Wir prüfen kostenlos und unverbindlich, ob Zugangsdaten Ihres Unternehmens aktuell im Dark Web verfügbar sind.

Kostenlose Erstanalyse anfordern

Blackveil Cybersecurity GmbH

Ottenser Hauptstraße 2-6

22765 Hamburg

info@blackveil.de

www.blackveil.com

Dark Web Monitoring & Threat Intelligence