BLACKVEIL
CYBER SECURITY

Dark Web Leaks in the DACH Mid-Market

Systematic Analysis of 1,976 Companies across Germany, Austria, and Switzerland

STUDY Q1 2026

Blackveil Cybersecurity GmbH
Marcus Henschel, CEO
April 2026

The Key Numbers at a Glance

Based on the analysis of 1,976 DACH companies — Q1 2026

68,1%	9.390	Ø 7	3.411
COMPANIES AFFECTED	CREDENTIAL RECORDS	LEAKS PER COMPANY	EMAILS EXPOSED

> "The question is no longer whether a company has credentials on the dark web — but whether it knows about them and how many there are."
>
> — Marcus Henschel, CEO Blackveil Cybersecurity GmbH

How We Analyzed 1,976 Companies

For this study, we systematically examined mid-market companies across the DACH region — all with more than 50 employees.

- **Strict Search Criteria: Only Complete Credentials**
  Only complete combinations of URL + username + password were counted as findings. Partial results were deliberately excluded.
- **Only Leaks from the Last 3 Months — No Historical Archives**
  The scan period was deliberately limited to recent findings. A leak rate of 68.1% under this restriction means: freshly compromised, potentially still active credentials.
- **The Actual Leak Rate Is Likely Even Higher**
  By excluding partial findings and historical data, our numbers represent a conservative lower bound.

68% Is Not an Outlier — It Is the New Normal

Of the 1,976 companies analyzed, 1,344 had at least one confirmed dark web leak

1,344 out of 1,976 companies affected — that is 68.1%

Only 629 companies (31.9%) showed no findings under our strict criteria. More than two-thirds have complete credentials on the dark web.

An average of 7 separate leaked credential records per company

These are not isolated incidents from a single data breach. In many cases, they are recent leaks from multiple sources — infostealer malware, phishing campaigns, or third-party data breaches.

3,411 corporate email addresses found in leak datasets

Direct attack surfaces for targeted phishing, account takeovers, and Business Email Compromise (BEC) attacks.

What Kind of Data Ends Up on the Dark Web?

The spectrum of exposed corporate data extends far beyond passwords

Infostealer Logs

Malware on employee devices extracts all saved browser passwords, session cookies, and autofill data — including VPN access, email accounts, and internal tools.

Third-Party Data Breaches

Employees reuse passwords across multiple services. When a SaaS tool is breached, corporate credentials go with it.

Ransomware Leak Sites

Ransomware groups steal and publish data before encrypting it. Internal documents, contracts, and credentials become publicly accessible.

Paste Sites and Telegram Channels

Credentials are shared and sold in real time on Telegram leak groups and paste sites.

Which Industries Are Most Affected?

Some sectors are significantly overrepresented on the dark web

	INDUSTRY	AFFECTED COMPANIES
1	Business Services	170
2	Manufacturing	96
3	IT & Dienstleistungen	70
4	Beratung & Engineering	64
5	Maschinenbau & Anlagenbau	58
6	Real Estate	48
7	Elektronik & Elektrotechnik	43
8	Construction	42
9	Wholesale Trade	41
10	Chemie & Pharma	40

Notable: No industry in our dataset had a leak rate below 50% — the impact is cross-industry. Business Services leads the list — a sector with high employee turnover, strong reliance on third-party platforms, and frequent cross-company data exchange.

Why Most Companies Are Unaware

The vast majority of affected companies have no idea that their credentials are circulating on the dark web

1 **No Monitoring in Place**
Most mid-market companies do not actively monitor dark web sources. Without continuous scanning, leaks remain undetected.

2 **Leaks Surface Months or Years Later**
Data stolen today often does not appear on dark web markets until 6–18 months later.

3 **Leaked Data Spreads Across Multiple Sources**
A single credential record appears across dozens of leak databases, Telegram groups, and paste sites.

4 **Attackers Are Patient**
Stolen credentials are collected, validated, and deployed months later — for ransomware or as an initial access point.

Transparent Approach

For Reliable Results

DATA SOURCE

Dark Web Monitoring Infrastructure

Continuous scanning of hacker forums, Telegram leak channels, paste sites, and ransomware leak sites for exposed corporate credentials.

SCOPE

DACH Region

1,976 companies from Germany, Austria, and Switzerland. Mid-market companies with 50+ employees.

TIMEFRAME

Last 3 Months

Only recent leaks — no historical legacy data. This ensures the results reflect a real, active threat.

CRITERIA

Complete Credentials

Only records containing URL + username + password. No hashes, no incomplete entries. The actual rate is even higher.

Note: This study is based on publicly available data from the dark web. No systems were actively tested or compromised. The analysis serves exclusively for awareness and prevention purposes.

Conclusion

The Numbers Speak for Themselves

- **68.1% of audited DACH companies have active credentials on the dark web**
  Under strict search criteria and using exclusively current data from the last 3 months.
- **The threat is cross-industry and affects the entire mid-market**
  No industry falls below a 50% leak rate. Business Services, Manufacturing, and IT lead the list.
- **Without monitoring, leaks remain undetected indefinitely**
  The vast majority of affected companies do not know that their credentials have been compromised.

> “BlackVeil enables companies to detect signs of potential cyberattacks up to 4 months before they occur and to take proactive action.”
>
> — Marcus Henschel, CEO Blackveil Cybersecurity GmbH

What IT Leaders Should Do Now

The measures with the greatest immediate impact

1

Establish Visibility First

You cannot respond to threats you cannot see. A one-time dark web assessment — or ideally continuous monitoring — reveals which employees and systems are exposed.

2

Prioritize Corporate Email Addresses

Every leaked corporate email address is a direct phishing attack surface. Affected accounts should immediately enable multi-factor authentication and reset passwords.

3

Do Not Wait for Breach Notifications

Most dark web leaks never generate a public notification — the responsibility to discover them lies with the company itself.

4

Monitor Continuously, Not Just Once

A snapshot is a starting point, not a solution. New leaks emerge daily. Only continuous monitoring ensures you are notified as soon as your data surfaces.

5

Include Employees, Not Just Domains

Many credential leaks originate from personal email addresses that employees used for business services. A robust approach covers both corporate domains and key personnel.

Is Your Company Affected?

We check free of charge and without obligation whether your company's credentials are currently available on the dark web.

Request Free Initial Analysis

Blackveil Cybersecurity GmbH

Ottenser Hauptstraße 2-6

22765 Hamburg

info@blackveil.de

www.blackveil.com

Dark Web Monitoring & Threat Intelligence