Sehen, wer Sie bereits im Visier hat –

Threat Intelligence, die Entscheidungen verändert



Agenda

Über Group-IB	01
Bedrohungslage Deutschland 2025/26	02
Wie Angreifer vorgehen	03
Warum der Überblick oft fehlt	04
Was ASM bewirkt	05
Fazit & nächste Schritte	06

Über Group-IB

Seit 2003

Group-IB entwickelt Technologien zur Bekämpfung von Cyberkriminalität – Hauptsitz in Singapur, Kunden weltweit.

Quelle: group-ib.com

1.550+ Ermittlungen

Erfolgreich abgeschlossene Cyber-Ermittlungen in über 60 Ländern, in Zusammenarbeit mit Interpol und Europol.

Quelle: group-ib.com, 2026

Marktführer

Von Gartner als Leader im ersten Magic Quadrant für Cyber Threat Intelligence ausgezeichnet.

Quelle: Gartner, Mai 2026

02

Die Bedrohungslage in Deutschland 2025/26

Deutschland im Visier: Zahlen 2025/26

Registrierte Bedrohungsberichte mit Bezug zu Deutschland, Oktober 2025 bis Oktober 2026 · Quelle: Group-IB Threat Intelligence

1.426

Angriffe mit Bezug zu Deutschland wurden in den letzten zwölf Monaten registriert.

988

Datenleaks: Unternehmensdaten werden abgezogen, veröffentlicht oder im Untergrund verkauft.

602

Ransomware-Vorfälle trafen deutsche Organisationen – meist mit doppelter Erpressung.

289

hacktivistische Aktionen, vor allem DDoS-Angriffe prorussischer Gruppen.

Am stärksten betroffene Branchen

Registrierte Vorfälle Oktober 2025 bis Oktober 2026 · Anteil an allen Bedrohungsberichten zu Deutschland

Industrie & Produktion



Vorfälle · 15,6 % aller Berichte

- Hauptziel von Ransomware-Gruppen wie SafePay und Qilin
- Betroffen u. a. ein Halbleiterhersteller und ein Bauunternehmen

Transport & Logistik



Vorfälle · 15,0 % aller Berichte

- Im Visier von Ransomware- und Hacktivisten-Gruppen
- Angriffe u. a. auf einen deutschen Verkehrsflughafen

Behörden & Militär



Vorfälle · 14,1 % aller Berichte

- DDoS-Kampagnen von NoName057(16) gegen Bund und Kommunen
- Ziele u. a. Polizeiportale und Sicherheitsbehörden

03

Ihre Angriffsfläche im Visier

Wie Angreifer externe Assets nutzen

Viele Bedrohungsberichte zu Deutschland zeigen Techniken, die ASM frühzeitig sichtbar macht.



1 Aufspüren

Angreifer scannen automatisiert öffentlich sichtbare Systeme wie Webseiten, Server oder Subdomains – auch solche, von denen das Unternehmen selbst nichts mehr weiß.

Grundlage: alles, was aus dem Internet erreichbar ist



2 Ausnutzen

Veraltete Software, offene Ports oder falsch konfigurierte Systeme dienen als Einstiegspunkt in die IT-Umgebung.

Deutschland: 45+ Vorfälle über exponierte Internet-Dienste (T1190, T1133)



3 Eindringen

Von dort verschaffen sich Angreifer Zugriff auf interne Systeme, Daten oder Zahlungsvorgänge – oft über Wochen unbemerkt.

Deutschland: 91 Vorfälle über Phishing und gültige Zugangsdaten (T1566, T1078)

Change Healthcare, 2024

Ein öffentlich dokumentierter Fall aus den USA – das Muster trifft deutsche Unternehmen genauso.

12. Feb. 2024

Zugang über Fernzugriffsportal

Angreifer nutzen gestohlene Zugangsdaten für ein Citrix-Portal ohne Multi-Faktor-Authentifizierung.

12.–21. Feb. 2024

9 Tage unbemerkt

Die Angreifer bewegen sich unentdeckt durchs Netzwerk und entwenden Unternehmens- und Patientendaten.

21. Feb. 2024

Ransomware & Systemausfall

Die Verschlüsselung legt zentrale Abrechnungs- und Verordnungsprozesse im US-Gesundheitswesen lahm.

Mai 2024

Offenlegung & Anhörung

Der CEO bestätigt vor dem US-Kongress die fehlende MFA, eine Lösegeldzahlung und das Ausmaß des Datendiebstahls.

190 Mio.
betroffene Personen

3,09 Mrd. USD
Gesamtkosten (2024)

Quelle: UnitedHealth Group (SEC 10-K 2024), Kongress-Anhörung Mai 2024

Pilz GmbH & Co. KG, 2019

Ein Fall aus Deutschland: kompromittierte Zugangsdaten statt offener Schwachstelle – ebenfalls Teil der Angriffsfläche.

Mai 2019 (vermutet)

Erste Infektion

Eine Phishing-Mail mit Schadanhang schleust den Dridex-Trojaner ins Netzwerk ein – monatelang unbemerkt.

13. Okt. 2019

Ransomware aktiviert

Über ein kompromittiertes Konto breitet sich die Ransomware BitPaymer im Netzwerk aus und verschlüsselt Daten.

13.–21. Okt. 2019

Weltweite Notabschaltung

Pilz trennt vorsorglich alle Server, Arbeitsplätze und Kommunikationssysteme in 76 Ländern vom Netz.

Ende Okt. 2019

Schrittweise Wiederherstellung

E-Mail nach rund einer Woche wieder verfügbar; Bestell- und Liefersysteme erst nach acht Tagen teilweise.

76 Länder
ohne IT-Betrieb

8 Tage
bis zur Teilwiederherstellung

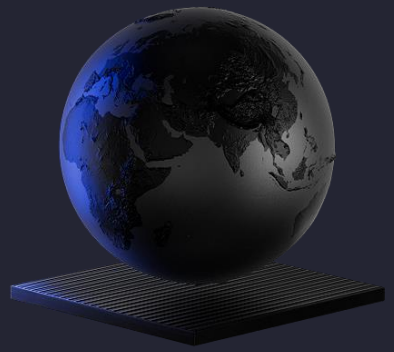
Quelle: Pilz (Unternehmensangaben), Presseberichte 2019

Warum der Überblick oft fehlt



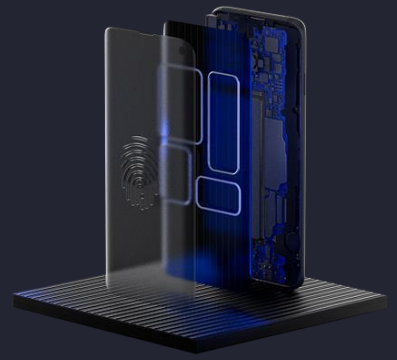
Schatten-IT

Mitarbeitende nutzen eigene Cloud-Dienste oder Tools, ohne die IT zu informieren.



Wachstum & Wechsel

Neue Webseiten, Partner oder Dienstleister erweitern die Angriffsfläche laufend.



Home-Office & mobile Geräte

Private Geräte und Netzwerke lassen sich zentral kaum überblicken.



Vergessene Systeme

Alte Testserver, Subdomains oder Marketing-Seiten bleiben oft jahrelang online.

Was Attack Surface Management bewirkt

Vollständige Sichtbarkeit

Sie sehen alle externen Assets, die zu Ihrem Unternehmen gehören – auch vergessene oder unbekannte.

EtlicheVorfälle starten über exponierte Internet-Dienste. ASM macht sie sichtbar

Klare Prioritäten

Schwachstellen werden nach dem individuellen Risiko Ihres Unternehmens bewertet und priorisiert. Der Risiko-Level wird sichtbar – und seine Entwicklung über einen definierten Zeitraum nachvollziehbar.

Viele Vorfälle nutzen verwundbare öffentliche Anwendungen. ASM zeigt, was zuerst geschlossen werden sollte

Schnellere Reaktion

Neue Risiken werden laufend erkannt – nicht erst bei der nächsten jährlichen Prüfung.

Kampagnen laufen über kompromittierte Websites und Domains. DNS- und Zertifikats-Monitoring meldet sie frühzeitig

Weniger Angriffsfläche

Ungenutzte oder unsichere Zugänge werden sichtbar und können geschlossen werden.

Zugangsverkäufe und Credential-Leaks. ASM meldet sie, bevor Angreifer sie nutzen.

ASM in der Praxis: Angriffe 2025/26

Ausgewählte Kampagnen aus Group-IB Threat Intelligence mit Bezug zu Deutschland – anonymisiert

September 2026

AiTM-Phishing gegen Microsoft 365

42 VPS-Knoten fangen Anmeldesitzungen ab – Hunderte Organisationen in 40+ Ländern, auch in Deutschland.

ASM erkennt

Phishing-Domains und verdächtige DNS-Konfigurationen, die Ihre Anmeldeseiten imitieren.

Juni 2026

Credential-Harvesting an VPN- und Firewall-Gateways

Massenangriffe auf exponierte Perimetergeräte mit schwachen oder Standard-Passwörtern.

ASM erkennt

Alle aus dem Internet erreichbaren Perimetergeräte inklusive riskanter Konfigurationen.

September 2026

Offener Angreifer-Server

Ein ungeschützter Server einer Angreifergruppe enthält 4,9 GB Angriffswerkzeuge und 16.834 Zugangsdaten.

ASM erkennt

Geleakte Zugangsdaten zu Ihren Domains – bevor sie für Credential Stuffing dienen.

August – September 2026

Phishing mit Ausschreibungs-Ködern

73+ kompromittierte Websites hosten gefälschte SharePoint-Weiterleitungen – Ziele u. a. in Deutschland und der Schweiz.

ASM erkennt

Kompromittierte eigene Web-Präsenzen und verdächtige Domain-Registrierungen.

Jedes Unternehmen kann zum Ziel werden – gezielt oder zufällig.

Viele Bedrohungsberichte zu Deutschland in den letzten zwölf Monaten zeigen:
Wer seine externe Angriffsfläche kennt, erkennt Angriffe früher.

1

Angriffsfläche erfassen

Externe Assets automatisiert inventarisieren – inklusive vergessener Systeme.

2

Risiken priorisieren

Schwachstellen und Credential-Leaks nach Geschäftsrisiko bewerten.

3

Laufend überwachen

Mit einem Partner kontinuierlich beobachten, melden und schließen.

Vielen Dank!

für Ihre Aufmerksamkeit

Kay Bandemer

Partner Manager MSSP, DACH

group-ib.com · k.bandemer@group-ib.com