ARGOS RADAR · AUSGABE 02/26

RADAR

Das Bedrohungslage-Briefing von Argos Security – hundert Augen auf die Gefahren, die Ihr Unternehmen betreffen.

→ Wer gerade am härtesten angreift

→ Erstmaßnahmen je Gruppe

→ Der Modern Cyber Defense Approach

→ Regulatorik, Haftung & Fallstudie RIVA

EDITORIAL · FRANK PÜTZ, CEO

Angriffe sind der Normalfall. Vorbereitung entscheidet.

Willkommen zur zweiten Ausgabe von ARGOS RADAR. Viermal im Jahr bringen wir Ihnen mit diesem Report auf den Punkt, was in der Bedrohungslage wirklich passiert und was das für Ihre Entscheidungen bedeutet. Ohne Panik, ohne Fachchinesisch, aber mit Klartext.

Die nüchterne Wahrheit vorweg: Cyberangriffe treffen heute Unternehmen jeder Größe. Qilin, The Gentlemen, LockBit, Akira & Co. arbeiten arbeitsteilig, hochprofessionell und rund um die Uhr – und der deutschsprachige Mittelstand steht ausdrücklich auf ihrer Zielliste. In diesem Quartal sehen wir nicht nur mehr Angriffe, sondern auch neue Gruppen, die in Wochen aufsteigen, wo früher Jahre vergingen.

Die gute Nachricht: Dagegen kann man sich wappnen – wenn man aufhört, nur zu reagieren. Ein reines SOC genügt heute nicht mehr. Was es braucht, ist ein **Modern Cyber Defense Approach**: Sicherheit nicht als Sammlung einzelner Werkzeuge, sondern als durchgehend besetztes, geübtes und nachrichtendienstlich informiertes **Cyber Defense Center**. Unsere **Roadmap to Resilience** ist der Weg dorthin – mit dem Ziel, Angriffe früh zu erkennen und einzudämmen, statt ihnen nur hinterherzulaufen.

Dass das funktioniert, zeigt in dieser Ausgabe die Fallstudie **RIVA Engineering**: vom Totalausfall am 15. Dezember zurück in den Regelbetrieb am 7. Januar. Und einen Ausblick geben wir auch: Wir entwickeln unser CDC zu **mehr digitaler Souveränität** (voraussichtlich ab Q1/2027) und mit STACKIT / Schwarz Digits den **IR-Container** – ein mobiles Notfall-Rechenzentrum für den Ernstfall.

Nehmen Sie sich zwanzig Minuten. Geben Sie diesen Report weiter – an Ihre Geschäftsleitung, Ihre IT, Ihren Datenschutz. Und wenn Sie danach eine Frage haben: Wir sind da. Rund um die Uhr.

Frank Pütz

Chief Executive Officer, Argos Security

Frank Pütz, CEO Argos Security

~202 Mrd. €

davon entfallen auf Cyberangriffe – von geschätzt 289,2 Mrd. € jährlichem Schaden für deutsche Unternehmen durch Diebstahl, Spionage und Sabotage (Bitkom, 2025)

KMU

zählen laut BSI-Lagebild 2025 zu den am stärksten von Ransomware betroffenen Zielen

24/7/365

besetzt: das Argos Cyber Defense Center – getragen von über 100 Spezialistinnen und Spezialisten im Unternehmen

Was Sie in Ihre nächste Leitungssitzung mitnehmen

Drei Fragen an Ihre IT-Leitung

- Ist jeder Fernzugang mit Mehr-Faktor-Anmeldung geschützt – VPN und Service Desk eingeschlossen?
- Wann haben wir den Ernstfall zuletzt geübt, und sind unsere Backups wiederherstellbar?
- Welche der in dieser Ausgabe genannten Schwachstellen sind bei uns noch offen?

Drei Beschlüsse für die Geschäftsleitung

- Verantwortlichkeit für Cyberrisiken schriftlich benennen – das verteilt die Aufgabe, nicht die eigene Pflicht der Leitung.
- Das gewünschte Maß an Incident-Response-Bereitschaft festlegen – und finanzieren.
- Einen Termin für die nächste Tabletop-Übung setzen.

Nur zur Orientierung – siehe Seite 21.

DIE LAGE · STAND 3. AUGUST 2026

Die Bedrohung rückt näher – und sie zielt auf den Mittelstand.

Ransomware bleibt die dominierende Gefahr. Neu ist die Geschwindigkeit: Gruppen steigen binnen Wochen auf, professionalisieren ihre Werkzeuge und nutzen Schwachstellen aus, bevor viele Unternehmen überhaupt patchen konnten. In den letzten 90 Tagen zählen wir **183 gelistete Opfer in Deutschland, Österreich und der Schweiz** – und das Feld hat sich gegenüber unserer ersten Ausgabe neu sortiert.

Am stärksten betroffene Sektoren im DACH-Raum

GELISTETE OPFER IN DEUTSCHLAND, ÖSTERREICH UND DER SCHWEIZ · ROLLIERENDE 90 TAGE BIS 3. AUGUST 2026

Gezählt werden auf Leak-Sites veröffentlichte Opfer (Quelle: ransomware.live). Diese Einträge stammen überwiegend aus Selbstauskunft der Täter und sind nicht durchgängig unabhängig bestätigt; sie zeigen gemeldete Fälle, nicht die tatsächliche Gesamtzahl.

Was diese Lage antreibt

Tempo. Von der Veröffentlichung einer Schwachstelle bis zur ersten Ausnutzung vergehen oft nur Tage – das Patch-Fenster schrumpft.

Arbeitsteilung. RaaS-Plattformen vermieten Angriffswerkzeuge; Zugangshändler liefern den Erstzugang. Cybercrime ist eine Industrie.

Datendiebstahl zuerst. Immer mehr Gruppen verzichten ganz auf Verschlüsselung und erpressen allein mit gestohlenen Daten.

DACH im Fokus. Deutschsprachige Länder zählen bei mehreren der aktivsten Gruppen zu den Top-Zielregionen.

Gestohlene Firewall-Zugänge. Im Juni 2026 wurde eine groß angelegte Kampagne zum Abgriff von FortiGate-Zugangsdaten bekannt; Forscher schreiben sie INC Ransom und Lynx zu. Wer FortiGate betreibt: Administrations- und VPN-Zugangsdaten rotieren und aktive Sitzungen beenden.

The Gentlemen
weltweit aktivste Gruppe der letzten 90 Tage (317 gelistete Opfer)

183 Opfer
in DACH gelistet in 90 Tagen – 142 davon in Deutschland

27 Prozent
der DACH-Opfer entfallen auf Fertigung und Industrie – der größte Einzelblock

Die Kernfrage für jedes Unternehmen lautet nicht mehr „Sind wir ein Ziel?“ – sondern „Wie schnell erkennen und stoppen wir einen Angriff, der bereits läuft?“

TOP-BEDROHUNGEN · DAS RADAR, 3. AUGUST 2026

Die zehn Gruppen, die Sie jetzt kennen sollten.

Unser Radar priorisiert nach Aktivität und DACH-Relevanz – nicht nach Bekanntheit. Acht dieser Gruppen stellen wir auf den folgenden Seiten im Detail vor, jeweils mit den konkreten Erstmaßnahmen, die zählen.

#	GRUPPE	STATUS	DACH 90 T	PRIMÄRE ZIELE (DACH)	WARUM JETZT RELEVANT
01	The Gentlemen	AKTIV	26	Fertigung, Technologie, Dienstleistung	317 Opfer in 90 Tagen – derzeit die aktivste Gruppe, die wir beobachten; Deutschland unter den Top-4-Zielländern
02	Qilin / Agenda	AKTIV	20	Gesundheit, Fertigung, Kommunen	313 Opfer in 90 Tagen; 2.098 kumuliert in 101 Ländern; MSP-Angriffe mit Kettenwirkung
03	SafePay	AKTIV	37	Industrie, IT-Dienstleister, MSPs	Deutschland ist weltweit das zweitgrößte Zielland der Gruppe; 125 deutsche Opfer insgesamt
04	DragonForce	AKTIV	9	Handel, Dienstleistung, kritische Infrastruktur	126 Opfer in 90 Tagen; „Kartell“-Modell, aggressive Expansion
05	Deadlock	NEU	6	Fertigung, Dienstleistung, Technologie	95 Opfer in 90 Tagen aus dem Stand – die Leak-Site ging im Juni 2026 online; Profil auf Seite 14
06	INC Ransom	AKTIV	4	Gesundheit, Bildung, Behörden	92 Opfer in 90 Tagen; etablierter Erpresser mit langer Verweildauer
07	Akira	AKTIV	4	Finanz, Fertigung, Bildung	82 Opfer in 90 Tagen; VPN-Appliances ohne MFA als Haupteinfallstor
08	LockBit 5.0	AKTIV	10	Fertigung, Gesundheit, Finanz	54 Opfer in 90 Tagen; nach Operation Cronos zurück im Geschäft
09	Play	AKTIV	3	Fertigung, Bau, öffentlicher Sektor	37 Opfer in 90 Tagen; intermittierende Verschlüsselung, wiederkehrende Kampagnen
10	Cl0p	IN WELLEN	0	Finanz, Software-Lieferketten	Kampagnengetrieben: lange stille Phasen, dann Massenausnutzung einer einzelnen Schwachstelle

Quellen: Argos Threat Intelligence, öffentliche Leak-Site-Auswertungen (u. a. ransomware.live), CISA, Europol. Stand 3. August 2026; 90-Tage-Fenster 5. Mai bis 3. August 2026.
Hinweis: Opferzahlen beruhen überwiegend auf selbstberichteten Leak-Site-Angaben und sind nicht durchgängig unabhängig bestätigt. Die Reihenfolge gewichtet Aktivität und DACH-Relevanz, ist also keine reine Opferzahl-Rangliste; Gruppen, die erst innerhalb dieses Berichtsfensters entstanden sind, stellen wir gesondert auf Seite 14 vor. Das vollständige, wöchentlich aktualisierte Lexikon mit über 70 Profilen: argos.security/wissen/threat-actor-hub

Klartext-Glossar: **RaaS** = vermieteter Ransomware-Baukasten · **Double Extortion** = verschlüsseln plus Daten stehlen · **MFA** = Mehr-Faktor-Anmeldung · **RDP/VPN** = Fernzugänge · **EDR** = Endpunkt-Erkennung und -Reaktion

Beide Enden dieser Tabelle sind wichtig. Cl0p hat in 90 Tagen weltweit ein einziges Opfer gelistet und gehört trotzdem hierher, weil die Gruppe in Wellen zuschlägt. Deadlock existierte im letzten Quartal noch nicht und steigt auf Platz fünf ein. Wer nur den Schlagzeilen folgt, verteidigt gegen die Gruppen von gestern.

GRUPPE IM PROFIL · 1 / 8

Qilin

AKTIV

auch bekannt als: Agenda, Qilin v2

2.098 gelistete Opfer in 101 Ländern seit Oktober 2022 – 313 davon allein in den letzten 90 Tagen; 112 in Deutschland, Österreich und der Schweiz

Qilin war drei Quartale in Folge die weltweit aktivste Ransomware-Gruppe und steht bis heute ganz vorn. Die selbst entwickelte RaaS-Plattform (ursprünglich Go, heute vorwiegend Rust sowie C/Go für Linux-ELF-Varianten) zeichnet sich durch konsequenten Fokus auf VMware-ESXi-Infrastruktur, systematischen Diebstahl von Browser-VPN-Zugangsdaten und aggressive Double-Extortion aus.

> **FÜR ENTSCHEIDER · IN EINEM SATZ**
>
> Eine der beiden aktivsten Gruppen weltweit – trifft Kliniken, Industrie und Kommunen. Wichtigster Schutz: Fernzugänge absichern und Systeme aktuell halten.

Steckbrief

Status	Aktiv
Modell	RaaS (Ransomware-as-a-Service)
Herkunft	russophones Umfeld (vermutet); Attribution nicht abschließend
Aktiv seit	2022 (als „Agenda"), seit 2023 öffentlich als „Qilin"
Gelistete Opfer	2.098 in 101 Ländern
DACH-Opfer	112 (DE 76 / AT 18 / CH 18)

Primäre Zielsektoren

- Gesundheitswesen
- Fertigung/Automobilzulieferer
- Business Services
- Bildung
- kritische Infrastruktur/Kommunen

Vorgehen

Modus Operandi: Double Extortion: Verschlüsselung von Windows- und Linux/ESXi-Systemen kombiniert mit Datendiebstahl und Veröffentlichungsdrohung auf eigener Leak-Site

Einfallstor: häufigster Erstzugang über gekaufte oder per Phishing erbeutete Zugangsdaten sowie über RDP; daneben Ausnutzung öffentlich erreichbarer Anwendungen (u. a. FortiGate-, SAP-NetWeaver- und Citrix-Schwachstellen; CVE-Zuordnungen nicht abschließend gesichert) und kompromittierte Fernwartung. Zunehmend auch über Managed-Service-Provider mit Kettenwirkung.

DACH-Bezug: Qilin nennt DACH offen als eine seiner Zielregionen und trifft dort wie global bevorzugt Fertigung, Gesundheitswesen und Finanzwesen – Sektoren mit hoher Dichte und geringer Ausfalltoleranz im deutschsprachigen Raum.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Exponierte RDP- und VPN-Zugänge (v. a. FortiGate, Citrix) sofort auf Patchstand prüfen und MFA für alle Fernzugriffe erzwingen
+ Fernwartungswerkzeuge auf autorisierte Installationen prüfen und unbekannte Instanzen isolieren
+ Gespeicherte Browser-Zugangsdaten – insbesondere VPN-Logins – unternehmensweit zurücksetzen; genau dieses Abgreifen ist für Qilin berichtet
+ ESXi- und Virtualisierungsinfrastruktur separat absichern – Netzsegmentierung und MFA für das Hypervisor-Management –, da Qilin gezielt auf VMware ESXi geht

Unbedingt vermeiden

– Lösegeld zahlen oder mit den Angreifern direkt verhandeln, ohne vorher forensische Sicherung und Behördenkontakt (BSI / Landeskriminalamt)
– Betroffene Systeme vorschnell neu aufsetzen, bevor Persistenzmechanismen (GPO-Skripte, Scheduled Tasks, Registry Run Keys) vollständig identifiziert und entfernt sind

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 2 / 8

The Gentlemen

AKTIV

auch bekannt als: Betreiber-Handles zeta88, hastalamuerte

696 gelistete Opfer in 82 Ländern seit September 2025 – 317 davon in den letzten 90 Tagen, womit sie derzeit die aktivste Gruppe ist, die wir beobachten; 42 in DACH

The Gentlemen tauchte Mitte 2025 auf und ist schneller gewachsen als jede andere Ransomware-as-a-Service-Operation, die wir verfolgen. Deutschland ist das viertgrößte Zielland. Die USA bleiben mit rund 18 Prozent der gelisteten Opfer das größte Einzelland – das liegt aber deutlich unter dem Anteil vergleichbarer Gruppen, und genau das macht diesen Akteur für europäische Leser ungewöhnlich relevant. Technisch fällt die Gruppe durch selbstverbreitende, plattformübergreifende Verschlüsselung und maßgeschneiderte EDR-Killer auf.

FÜR ENTSCHEIDER · IN EINEM SATZ

Die am schnellsten wachsende Gruppe dieses Quartals – und eine, die gezielt Europa trifft. Wichtigster Schutz: Edge- und VPN-Geräte patchen, EDR gegen Manipulation schützen.

Steckbrief

Status	Aktiv
Modell	RaaS, partnerfreundlich (rund 90/10)
Herkunft	russischsprachige Betreiber (Herkunftsland unbestätigt)
Aktiv seit	Mitte 2025 (erste Leak-Site-Opfer September 2025)
Gelistete Opfer	696 in 82 Ländern
DACH-Opfer	42 (DE 32 / AT 6 / CH 4)

Primäre Zielsektoren

Fertigung · IT- und Business-Services · Technologie · Gesundheitswesen · Bau · Versicherung

Vorgehen

Modus Operandi: Double Extortion mit selbstverbreitender, plattformübergreifender Verschlüsselung (Windows, Linux, ESXi, NAS, BSD); Lösegeldforderungen werden verhandelt – in einem dokumentierten Fall von rund 250.000 auf 190.000 US-Dollar

Einfallstor: Hauptvektor ist die Ausnutzung von Fortinet- und Cisco-Edge- und VPN-Geräten (u. a. der FortiOS-Authentifizierungs-Bypass CVE-2024-55591), ergänzt um gekaufte Zugänge von Initial-Access-Brokern und Infostealer-Logs. Im Netz verbreitet sich die Gruppe wurmartig über Gruppenrichtlinien und schaltet Schutzsoftware mit einem eigenen EDR-Killer und verwundbaren Treibern ab.

DACH-Bezug: Deutschland zählt zu den Top-Zielländern, auch österreichische und schweizerische Opfer sind belegt. Für Leser aus dem europäischen Mittelstand ist das die Gruppe, deren Profil am stärksten vom üblichen US-Fokus abweicht.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Fortinet- und Cisco-Edge- und VPN-Geräte unverzüglich patchen und auf bekannte Authentifizierungs-Bypass-Schwachstellen prüfen – das ist der Hauptvektor
+ Manipulationsschutz (Tamper Protection) für EDR aktivieren und jeden Abschaltversuch alarmieren
+ Änderungen an Gruppenrichtlinien überwachen und unautorisierte Modifikationen alarmieren, da sich die Gruppe über GPO selbst verbreitet
+ Backups offline oder unveränderlich halten und ESXi-, NAS- und BSD-Systeme segmentieren – der Verschlüsseler deckt sie alle ab

Unbedingt vermeiden

– Edge- und VPN-Appliances ungepatcht lassen oder EDR ohne Manipulationsschutz betreiben
– Systeme neu aufsetzen, bevor die Forensik gesichert ist – der Selbstverbreitungsweg muss identifiziert sein, sonst kehrt die Verschlüsselung zurück

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 3 / 8

SafePay

AKTIV

auch bekannt als: SafePay Ransomware

537 gelistete Opfer in 45 Ländern seit November 2024 – 125 davon in Deutschland. Keine andere Gruppe in diesem Report ist so stark auf den deutschen Markt konzentriert

SafePay tauchte Ende 2024 auf und kletterte 2025 in die Spitzengruppe der Ransomware-Akteure. Es ist kein klassisches RaaS: Ein einzelnes, zentral geführtes Kollektiv steuert Einbruch, Verschlüsselung, Verhandlung und Veröffentlichung. Die Codebasis baut auf dem geleakten LockBit-3.0-Quellcode auf. Relevant für diesen Report ist vor allem die Zielgeografie: Deutschland ist nach den USA das zweitgrößte Zielland, und in den letzten 90 Tagen hat die Gruppe mehr DACH-Opfer gelistet als jeder andere Akteur.

FÜR ENTSCHEIDER · IN EINEM SATZ

Die Gruppe mit dem stärksten Deutschlandfokus überhaupt. Sie kommt über Fernzugänge und VPN-Fehlkonfiguration herein. Wichtigster Schutz: kein ungeschütztes RDP, MFA überall, und Vorsicht bei angeblichen IT-Support-Anrufen.

Steckbrief

Status	Aktiv
Modell	privates Kollektiv, zentral geführt (kein klassisches RaaS)
Herkunft	Osteuropa (vermutet); nutzt die LockBit-3.0-Codebasis
Aktiv seit	2024
Gelistete Opfer	537 in 45 Ländern
DACH-Opfer	130 (DE 125 / AT 2 / CH 3)

Primäre Zielsektoren

Industrie/Fertigung · IT-Dienstleister · Managed-Service-Provider · Mittelstand · Handel

Vorgehen

Modus Operandi: Double Extortion – Datendiebstahl, danach intermittierende Verschlüsselung; eine einzige Gruppe führt die gesamte Kette vom Einbruch bis zur Verhandlung und zielt gezielt auf Managed-Service-Provider

Einfallstor: gestohlene oder gekaufte Zugangsdaten (Zugangshändler, Infostealer-Logs), RDP-Brute-Force und fehlkonfigurierte SSL-VPN-Gateways, bei denen sich MFA umgehen lässt. Ein zweiter, gut dokumentierter Weg ist Social Engineering: Die Angreifer geben sich über Microsoft Teams als interner IT-Support aus und missbrauchen Fernwartungswerkzeuge wie ScreenConnect und Quick Assist.

DACH-Bezug: Deutschland ist nach den USA das am stärksten betroffene Land und stellt rund ein Viertel aller SafePay-Opfer. Mehrere DACH-Industrieunternehmen sind gelistet. Wenn Sie nur ein Profil in diesem Report lesen, lesen Sie dieses.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ RDP niemals ungeschützt aus dem Internet erreichbar lassen und MFA auf jedem Fernzugriffsweg erzwingen, auch am VPN-Gateway
+ Im Service Desk eine verpflichtende Identitätsprüfung vor jedem Passwort-Reset einführen – Impersonation über Teams ist ein dokumentierter SafePay-Weg
+ Fernwartungswerkzeuge (ScreenConnect, Quick Assist) inventarisieren und unautorisierte Instanzen sperren
+ Backups offline oder unveränderlich halten und auf ungewöhnliche Anmeldungen sowie Missbrauch bordeigener Systemwerkzeuge achten

Unbedingt vermeiden

– Unaufgeforderte „IT-Support"-Anrufe oder Chat-Anfragen annehmen, ohne den Anrufer über einen bekannten internen Kanal zu verifizieren
– Zahlen ohne forensische Prüfung und Sanktionslisten-Abgleich – es ist kein Entschlüsseler bekannt, und Zahlung schützt nicht zuverlässig vor Veröffentlichung

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 4 / 8

LockBit 5.0

AKTIV

auch bekannt als: LockBit 2.0, LockBit 3.0 (Black), LockBit 4.0, LockBit 5.0

329 gelistete Opfer in 68 Ländern unter der Generation 5.0 – 54 davon in den letzten 90 Tagen. Die Generation startete im September 2025; die Leak-Site-Erfassung unter der aktuellen Kennung beginnt im Dezember 2025, die tatsächliche Zahl liegt also höher

LockBit ist eine der langlebigsten und produktivsten RaaS-Gruppen überhaupt. Trotz der teilweisen Zerschlagung ihrer Infrastruktur durch „Operation Cronos“ im Februar 2024 war die Gruppe binnen Tagen wieder online und veröffentlichte im September 2025 die fünfte Malware-Generation. Sie führt das Feld nicht mehr an – aber sie ist weiterhin sehr aktiv.

FÜR ENTSCHEIDER · IN EINEM SATZ

Der Wiederholungstäter – zerschlagen und zurück. Schutz: Mehr-Faktor-Anmeldung auf Fernzugängen, Perimeter patchen, Protokolle vor Löschung sichern.

Steckbrief

Status	Aktiv
Modell	RaaS, Eigenentwicklung seit 2019
Herkunft	Russland/Osteuropa (vermutet); die NCA und ihre Partner benennen Dmitry Khoroshev, Alias „LockBitSupp“, als mutmaßlichen Kopf – es gilt die Unschuldsvermutung
Aktiv seit	2019
Gelistete Opfer	329 in 68 Ländern (Generation 5.0)
DACH-Opfer	29 (DE 20 / AT 7 / CH 2)

Primäre Zielsektoren

Fertigung · Gesundheitswesen · Finanzdienstleistungen · Regierung/Verwaltung · Recht/Bildung

Vorgehen

Modus Operandi: Double Extortion: Vollverschlüsselung plus Datendiebstahl, Veröffentlichung auf der Leak-Site mit Countdown zur Druckerhöhung

Einfallstor: Phishing mit gefälschten Passwort-Reset-Mails, Missbrauch exponierter RDP-Zugänge (Brute-Force oder Zugangsdaten aus Infostealer-Logs) und Ausnutzung öffentlich erreichbarer Anwendungen – darunter Fortinet FortiOS/FortiProxy, Atlassian Confluence und Log4Shell. Zusätzlich kommen im Darknet gekaufte gültige Konten zum Einsatz.

DACH-Bezug: DACH zählt neben den USA zu den stark betroffenen Regionen. Die Kernzielsektoren Fertigung, Gesundheitswesen und Finanzdienstleistungen decken sich mit den tragenden Branchen des deutschsprachigen Mittelstands und der öffentlichen Verwaltung.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, Notwendigkeit prüfen und MFA erzwingen
+ Öffentlich erreichbare Systeme vorrangig patchen – vor allem Fortinet FortiOS/FortiProxy und Atlassian Confluence
+ Zugangsdaten gegen Infostealer-Logs abgleichen und betroffene Konten zurücksetzen
+ EDR-/AV-Manipulationsschutz aktivieren und Windows-Ereignisprotokolle unveränderlich auslagern – LockBit löscht Protokolle aktiv

Unbedingt vermeiden

– RDP- oder VPN-Zugänge ohne MFA aus dem Internet erreichbar lassen
– Allein auf signaturbasierte Erkennung vertrauen – seit 2025 werden stark verschleierte, häufig wechselnde Varianten berichtet, die rein signaturbasierte Erkennung unterlaufen können

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

ZWISCHENSTAND · HALBZEIT

Acht Gruppen, fünf Muster.

So unterschiedlich Qilin, SafePay, The Gentlemen & Co. auftreten – im Vorgehen ähneln sie sich verblüffend. Wer diese fünf Muster kennt, verteidigt gezielt statt breit.

1

Missbrauch legitimer Zugänge

RDP, VPN und Fernwartung sind das häufigste Einfallstor – fast jede Gruppe nutzt gestohlene oder schwach geschützte Zugänge.

2

Datendiebstahl zuerst

Immer mehr Gruppen verschlüsseln gar nicht mehr, sondern erpressen allein mit gestohlenen Daten.

3

Tempo

Neue Schwachstellen werden in Tagen ausgenutzt – das Patch-Fenster schrumpft rapide.

4

Backups und Virtualisierung im Visier

Schattenkopien, Backups und ESXi-Hosts werden gezielt sabotiert, um die Wiederherstellung zu verhindern.

5

DACH im Fokus

Deutschsprachige Ziele stehen bei vielen Gruppen ausdrücklich auf der Liste – bei SafePay und The Gentlemen am stärksten.

Die gute Nachricht: Gegen alle fünf hilft dasselbe Fundament – MFA auf allen Zugängen, Patch-Disziplin, 24/7-Erkennung und ein geübter Ernstfall. Genau das bündelt ein Cyber Defense Center.

GRUPPE IM PROFIL · 5 / 8

Akira

AKTIV

auch bekannt als: Akira Ransomware

1.558 gelistete Opfer in 71 Ländern seit April 2023 – 82 davon in den letzten 90 Tagen; 101 in DACH, wobei die Schweiz ungewöhnlich stark vertreten ist

Akira ist seit 2023 aktiv und zählt weiterhin zu den produktivsten Ransomware-Gruppen weltweit – ohne Festnahmen oder Zerschlagung bis heute. Die Gruppe entwickelt stetig über mehrere Plattformen hinweg (Windows, Linux/ESXi und seit 2025 auch Nutanix AHV).

FÜR ENTSCHEIDER · IN EINEM SATZ

Kommt fast immer über eine VPN-Appliance herein. Schutz: patchen, MFA erzwingen – und danach die lokalen Konten und Einmalpasswort-Seeds rotieren, sonst bleibt die Tür offen.

Steckbrief

Status	Aktiv
Modell	RaaS (Ransomware-as-a-Service)
Herkunft	Russland/Osteuropa (stark vermutet); mögliche Verbindung zu ehemaligen Conti-Operatoren
Aktiv seit	2023
Gelistete Opfer	1.558 in 71 Ländern
DACH-Opfer	101 (DE 69 / AT 7 / CH 25)

Primäre Zielsektoren

Finanzwesen · Fertigung · Gesundheitswesen · Bildung · kritische Infrastruktur

Vorgehen

Modus Operandi: Double Extortion: Datendiebstahl kombiniert mit Verschlüsselung, Drohung mit Veröffentlichung bei Nichtzahlung

Einfallstor: primär die Ausnutzung öffentlich erreichbarer VPN-Appliances ohne Multi-Faktor-Authentifizierung, insbesondere Cisco-ASA/VPN-Schwachstellen (CVE-2020-3259, CVE-2023-20269) und SonicWall-SonicOS-SSL-VPN (CVE-2024-40766, seit 2025 Hauptvektor), dazu Veeam-Backup-Schwachstellen (CVE-2024-40711, CVE-2023-27532). Ergänzend Spear-Phishing zum Credential-Diebstahl, RDP-Missbrauch mit gestohlenen Zugangsdaten und Password-Spraying.

DACH-Bezug: Akira zielt neben den USA auch auf DACH. Mit 25 Schweizer Opfern ist es relativ betrachtet die Gruppe mit dem stärksten Schweiz-Bezug in diesem Report; ein Schweizer Fertigungsfall aus 2025 ist öffentlich dokumentiert.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Öffentlich erreichbare VPN-Appliances (Cisco ASA, SonicWall SonicOS) gegen die genannten CVEs patchen und MFA auf jedem Fernzugriffsweg erzwingen
+ Nach dem Patchen die lokalen Appliance-Konten rotieren und die Einmalpasswort-Seeds neu ausgeben – Angreifer haben aktive MFA-Abfragen mit Zugangsdaten aus der alten Konfiguration überwunden
+ Veeam Backup & Replication patchen (CVE-2024-40711, CVE-2023-27532) und RDP nicht nach außen exponieren – Akira nutzt Backups als Sprungbrett und löscht Schattenkopien
+ Auf verdächtige Fernwartungswerkzeuge und Erkundungsaktivität achten – typische Vorboten eines Akira-Angriffs

Unbedingt vermeiden

– Zahlen ohne forensische Prüfung und Rechtsberatung – Zahlung schützt nicht zuverlässig vor Veröffentlichung
– Betroffene Systeme neu aufsetzen oder Schattenkopien und Protokolle löschen, bevor Beweise gesichert sind
– Sich allein auf Windows-Endpunktschutz verlassen – Akira verschlüsselt auch ESXi-, Hyper-V- und Nutanix-AHV-Umgebungen, oft ohne dass Windows-Systeme betroffen sind

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 6 / 8

DragonForce

AKTIV

auch bekannt als: DragonForce Ransomware

632 gelistete Opfer in 64 Ländern seit Dezember 2023 – 126 davon in den letzten 90 Tagen, womit die Gruppe nach aktueller Aktivität auf Platz drei liegt; 40 in DACH

DragonForce soll 2023 aus der pro-palästinensischen Hacktivisten-Szene in Malaysia entstanden sein; diese Herkunft ist umstritten, manche Forscher halten die Ransomware-Operation für eine eigenständige Gruppe gleichen Namens. So oder so läuft sie heute als kommerzielle RaaS-Plattform, nutzt geleakten LockBit-3.0- und Conti-Code und beliefert auch Dritte mit ihrem Verschlüsseler.

FÜR ENTSCHEIDER · IN EINEM SATZ

Aggressiv expandierender „Kartell"-Akteur. Schutz: Zugänge härten, verdächtige Aktivität früh erkennen.

Steckbrief

Status	Aktiv
Modell	RaaS seit 2024; Verschlüsseler wird auch an Dritte vermietet
Herkunft	Malaysia berichtet, Herkunftslinie umstritten (hacktivistischer Ursprung, seit 2024 kommerzialisiert)
Aktiv seit	2023
Gelistete Opfer	632 in 64 Ländern
DACH-Opfer	40 (DE 32 / AT 1 / CH 7)

Primäre Zielsektoren

Handel · kritische Infrastruktur · Regierung · Fertigung · Business Services

Vorgehen

Modus Operandi: Double Extortion (Verschlüsselung plus Datenleck), teils zusätzlich DDoS als Druckmittel; der Verschlüsseler wird auch an Drittgruppen vermietet

Einfallstor: mehrere Wege: Social Engineering, Vishing und Help-Desk-Impersonation (Hauptvektor bei den britischen Handelsketten-Angriffen, die Forscher dem Partner Scattered Spider zuschreiben), exponierte RDP-Server und VPN-Portale mit gestohlenen Zugangsdaten sowie öffentlich erreichbare Web- und Anwendungsserver (Log4Shell, Ivanti Connect Secure). RMM-Schwachstellen in SimpleHelp wurden verkettet, um über einen Dienstleister mehrere Kunden zu verschlüsseln.

DACH-Bezug: Die Zielregionen umfassen ausdrücklich auch DACH neben UK, USA und Asien-Pazifik. Die Lieferkettenkompromittierung über SimpleHelp zeigt, dass deutsche, österreichische und schweizerische Kunden von IT-Dienstleistern indirekt betroffen sein können.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, aus dem Internet nehmen oder mit MFA absichern
+ Help-Desk-Prozesse gegen Vishing härten: Rückruf- und Identitätsprüfung vor jedem Passwort-Reset verpflichtend machen
+ Internetseitige Anwendungs- und VPN-Server patchen (Log4Shell, Ivanti Connect Secure) und RMM-Software aktuell halten
+ EDR-/XDR-Alarme zu Treiber-Installationen und gelöschten Ereignisprotokollen sofort eskalieren

Unbedingt vermeiden

– Lösegeld zahlen oder verhandeln, ohne vorher Strafverfolgung und CERT einzubinden
– Sich allein auf Perimeter-Schutz verlassen und interne Segmentierung sowie MFA für Admin-Konten vernachlässigen

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 7 / 8

INC Ransom

AKTIV

auch bekannt als: keine weiteren Aliasse bekannt

883 gelistete Opfer in 71 Ländern seit August 2023 – 92 davon in den letzten 90 Tagen; Gesundheitswesen und Bildung sind deutlich überrepräsentiert

INC Ransom ist seit 2023 aktiv und wurde bislang von keiner Strafverfolgungsbehörde zerschlagen. Kennzeichnend sind auffällig lange Verweildauern zwischen Erstzugriff und Verschlüsselung sowie ein ausgeprägter Fokus auf Gesundheitswesen, Bildung und öffentliche Verwaltung.

FÜR ENTSCHEIDER · IN EINEM SATZ

Etablierter Erpresser, der mit Datendiebstahl arbeitet. Schutz: Zugänge härten, Datenabfluss erkennen, den Ernstfall üben.

Steckbrief

Status	Aktiv
Modell	RaaS (Ransomware-as-a-Service)
Herkunft	unbekannt (Osteuropa vermutet)
Aktiv seit	2023
Hinweis	das BSI führt INC, Lynx und Sinobi als einen Akteur
Gelistete Opfer	883 in 71 Ländern
DACH-Opfer	52 (DE 39 / AT 10 / CH 3)

Primäre Zielsektoren

Gesundheitswesen · Bildung · Regierung · Pharmaindustrie · Verarbeitendes Gewerbe

Vorgehen

Modus Operandi: Double Extortion: Datendiebstahl plus Verschlüsselung, mit auffallend langer Verweildauer vor der eigentlichen Verschlüsselung

Einfallstor: häufig über Schwachstellen in öffentlich erreichbaren Systemen – Citrix NetScaler (CVE-2023-3519 und zuletzt CVE-2025-5777), FortiClient EMS (CVE-2023-48788) und SimpleHelp (CVE-2024-57727) – sowie über per Phishing oder aus Infostealer-Logs erbeutete Zugangsdaten. Sehr aktuelle CVE-Zuordnungen sind nicht abschließend gesichert.

DACH-Bezug: INC Ransom ist ein etablierter, aktiver Double-Extortion-Akteur mit Opfern im gesamten europäischen Raum; kumuliert sind 52 DACH-Opfer gelistet, wobei Österreich vergleichsweise stark vertreten ist.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Citrix NetScaler ADC/Gateway, FortiClient EMS und SimpleHelp-RMM-Installationen unverzüglich gegen die bekannten CVEs patchen oder isolieren
+ Exponierte RDP- und Fernzugriffsdienste (auch AnyDesk, TightVNC) identifizieren, absichern und mit MFA schützen
+ Active-Directory-Erkundung prüfen sowie PsExec unter Tarnnamen wie „winupd“ als Indikator werten
+ Zugriffe auf Veeam-Backup-Zugangsdaten und typische Credential-Dumping-Muster überwachen – die Backup-Infrastruktur wird gezielt angegriffen

Unbedingt vermeiden

– Annehmen, der Schaden ende bei den verschlüsselten Systemen – wegen der langen Verweildauer sind Daten meist parallel abgeflossen
– Eine Lösegeldzahlung ohne Rücksprache mit Ermittlungsbehörden und Rechtsberatung veranlassen – Zahlung garantiert keine Löschung der Daten

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

GRUPPE IM PROFIL · 8 / 8

Play

AKTIV

auch bekannt als: PlayCrypt, Balloonfly

1.290 gelistete Opfer in 44 Ländern seit November 2022 – 37 davon in den letzten 90 Tagen; 51 in DACH

Play ist eine zentral gesteuerte, nicht-affiliierte Ransomware-Gruppe ohne bekannte Verbindung zu anderen Akteuren. Kennzeichnend sind eine eigene Linux/ESXi-Variante, ein individueller Infostealer namens Grixba sowie eine intermittierende Verschlüsselungsstrategie, die klassische Signaturerkennung umgeht.

> **FÜR ENTSCHEIDER · IN EINEM SATZ**
>
> Verschlüsselt schnell und in Wellen. Schutz: Fern- und Perimeterzugänge im Blick behalten, rund um die Uhr überwachen.

Steckbrief

Status	Aktiv
Modell	privates Kollektiv, zentral gesteuert (kein klassisches RaaS)
Herkunft	unbekannt (Lateinamerika vermutet)
Aktiv seit	2022
Gelistete Opfer	1.290 in 44 Ländern
DACH-Opfer	51 (DE 36 / AT 5 / CH 10)

Primäre Zielsektoren

Gesundheitswesen · Recht · Immobilien · Fertigung · IT

Vorgehen

Modus Operandi: Double Extortion: Datendiebstahl plus intermittierende Verschlüsselung (AES-256/RSA-4096, Fallback ChaCha20), Kontakt nur per E-Mail ohne Tor-Verhandlungsportal

Einfallstor: vorrangig die Ausnutzung öffentlich erreichbarer Systeme: FortiOS-SSL-VPN-Schwachstellen (CVE-2018-13379, CVE-2020-12812), Microsoft-Exchange-Lücken (ProxyNotShell, OWASSRF) sowie Cisco-ASA-Firewalls. Ergänzend gekaufte Zugangsdaten von Initial-Access-Brokern, exponierte RDP-/VPN-Endpunkte, SimpleHelp-RMM-Schwachstellen (CVE-2024-57726/27/28) und die Windows-CLFS-Zero-Day-Lücke CVE-2025-29824.

DACH-Bezug: Play zählt DACH zu seinen erklärten Zielregionen; kumuliert sind 51 Opfer in Deutschland, Österreich und der Schweiz gelistet (Angaben der Täter, nicht unabhängig bestätigt).

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt tun – und beim ersten Verdacht

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, absichern und MFA erzwingen
+ Microsoft Exchange (ProxyNotShell/OWASSRF), Fortinet-SSL-VPN, Cisco ASA und die Windows-CLFS-Lücke CVE-2025-29824 unverzüglich patchen
+ SimpleHelp- und andere RMM-Installationen auf Aktualität und unautorisierte Nutzung prüfen
+ ESXi-Hosts isolieren und auf ungewöhnliche .vmdk-/.vmx-Zugriffe sowie Ransom-Notes in /vmfs/volumes/ kontrollieren

Unbedingt vermeiden

– Zahlen ohne forensische Prüfung und Sanktionslisten-Abgleich – Forscher haben eine Zusammenarbeit eines nordkoreanisch verbundenen Akteurs mit Play dokumentiert, was Zahlungen zum Sanktionsrisiko macht
– Auf die E-Mail-Adresse in der Ransom Note antworten oder eigenmächtig verhandeln
– Betroffene Systeme neu aufsetzen, bevor Grixba-Spuren forensisch gesichert sind

Kennzahlen überwiegend aus selbstberichteten Leak-Site-Angaben; nicht durchgängig unabhängig bestätigt. Einzelne CVE- und Werkzeug-Zuordnungen sind Momentaufnahmen (Stand 3. August 2026).

NEU & AUFSTREBEND · DIE NÄCHSTE WELLE

Neue Gruppen entstehen schneller denn je.

Rebrands zerschlagener Gruppen, Ableger auf Basis geleakten Codes, Spezialisten für eine einzelne Schwachstelle: Der Markt sortiert sich ständig neu. Vier Namen, die es in unserer letzten Ausgabe noch nicht gab – und die bereits DACH-Opfer listen.

Deadlock

JETZT NR. 5

Die Leak-Site ging im Juni 2026 mit nachgetragener Opferliste online, und die Gruppe stieg direkt in die Top fünf ein: 95 gelistete Opfer in den letzten 90 Tagen, sechs davon in DACH. Ihre gesamte Historie liegt innerhalb dieses Berichtsfensters – ein Beleg dafür, wie schnell aus einem unbekannten Namen ein reales Risiko wird.

Nova

EX RALORD

Ein Rebrand der RALord-Operation mit ungewöhnlich partnerfreundlicher Aufteilung. 74 Opfer in den letzten 90 Tagen, darunter deutsche Unternehmen.

Krybit

NEU 2026

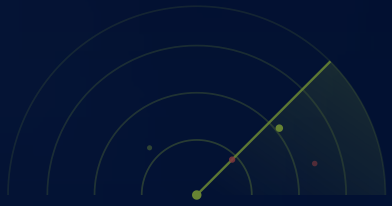
Ein RaaS-Neuling mit ausdrücklichem DACH-Bezug: 62 Opfer in 90 Tagen, fünf davon in Deutschland, Österreich und der Schweiz. Aus dem Nichts binnen eines Quartals gewachsen.

Payload & Aurora

BEOBACHTUNGSLISTE

Zwei kleinere Namen mit überproportionalem Deutschland-Anteil – Payload baut auf der geleakten Babuk-Codebasis auf. Zusammen elf DACH-Opfer in 90 Tagen.

Der Trend hinter den Namen: Datendiebstahl statt Verschlüsselung. Wo früher die Wiederherstellung zählte, entscheidet heute, ob sensible Daten das Haus überhaupt verlassen haben – und ob Sie es rechtzeitig bemerken.



DACH-SPOTLIGHT · NÄHER AM EIGENEN HAUS

Die Gefahr wird lokaler.

Drei Befunde zeigen, wie nah die Szene gerückt ist. Eine Gruppe konzentriert sich stärker auf Deutschland als jeder andere Akteur in diesem Report. Deutschsprachige Einzeltäter missbrauchen legitime Fernwartungssoftware. Und der meistbetroffene Sektor ist die Fertigung.

SafePay – der deutsche Fall

AKTIV

125 von 537 SafePay-Opfern sind deutsch – rund ein Viertel der gesamten Opferliste. In den letzten 90 Tagen nannte die Gruppe 37 DACH-Organisationen, mehr als jeder andere Akteur. Deutschland ist nach den USA das zweitgrößte Zielland. Vollständiges Profil auf Seite 7.

Was das bedeutet

+ Mittelständisch und deutschsprachig zu sein ist kein Schutz durch Unauffälligkeit mehr
+ Fernzugänge und Service-Desk-Prozesse sind die entscheidenden Kontrollpunkte

Deutschsprachige Einzeltäter

KLEIN, ABER REAL

Sicherheitsforscher schreiben den Missbrauch legitimer Fernwartungssoftware (RMM) – genutzt, um in kleinere Unternehmen einzudringen – mutmaßlich deutschsprachigen Einzelpersonen zu. Kein Konzern-Apparat – und trotzdem gefährlich, weil die Werkzeuge unauffällig sind und die Ziele schlecht geschützt. Seit Juni 2026 ist die Aktivität gering, das Muster bleibt.

Was das bedeutet

+ Auch kleine Unternehmen sind gezielte Ziele
+ Fernwartungswerkzeuge gehören lückenlos inventarisiert

Gemeinsamer Nenner: Missbrauch legitimer Zugänge – RDP, VPN und Fernwartung. Inventarisieren Sie diese Wege lückenlos, sichern Sie sie mit MFA und überwachen Sie sie, dann nehmen Sie der Mehrheit der Angreifer ihr wichtigstes Werkzeug aus der Hand.

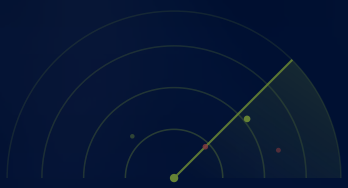
Wenn die Linie steht

Die Fertigung ist der meistbetroffene Sektor im DACH-Raum, mit 50 von 183 gelisteten Opfern. Dabei trifft kaum ein Angriff in diesem Report eine Maschine direkt: Verschlüsselt werden die Virtualisierungsschicht, die Dateifreigaben und die Systeme, die Produktion planen und steuern. Die Linie steht, weil ihr niemand mehr sagt, was sie bauen soll.

Damit ist die Grenze zwischen IT und OT der entscheidende Kontrollpunkt. Die RIVA-Fallstudie auf Seite 18 zeigt, was ein geordneter Notbetrieb wert ist.

+ Produktionsnetz von der Büro-IT segmentieren – und prüfen, ob die Trennung wirklich hält
+ Auflisten, welche OT-Systeme von einem Windows-Server oder Hypervisor abhängen: diese Liste ist Ihr tatsächlicher Wirkungsradius
+ Jetzt festlegen, wie lange Sie auf Papier weiterproduzieren können und wer den Umstieg entscheidet

Die Opferzahlen auf dieser Seite sind Leak-Site-Angaben, überwiegend selbstberichtet von den Tätern und nicht durchgängig unabhängig bestätigt.



DER KERNGEDANKE

Die Frage ist nicht mehr, ob Sie ein Ziel sind.
Sondern wie schnell Sie einen Angriff erkennen, der bereits läuft.

Genau darauf ist der **Modern Cyber Defense Approach** ausgelegt – und die **Roadmap to Resilience** ist der Weg dorthin. Wie der aussieht, zeigen die folgenden Seiten.

ERSTMASSNAHMEN · DIE ERSTE STUNDE

Wenn es brennt: sechs Schritte, die den Schaden begrenzen.

Die ersten sechzig Minuten entscheiden oft über das Ausmaß eines Vorfalls. Dieses Playbook gilt für praktisch jede Gruppe aus diesem Report – hängen Sie es aus, bevor Sie es brauchen.

1 Ruhe, Lagebild & sauberer Kanal

Nicht in Panik abschalten. Verschaffen Sie sich ein Bild: Welche Systeme sind betroffen, läuft die Verschlüsselung noch, sind Daten abgeflossen? Kommunizieren Sie ab jetzt über einen **sauberen Nebenkanal** (Telefon, fremdes Gerät) – Angreifer lesen im Netz oft mit.

2 Isolieren, nicht löschen

Betroffene Systeme vom Netz trennen (Kabel ziehen, WLAN aus), aber möglichst **nicht herunterfahren und nicht neu aufsetzen** – das vernichtet Spuren. (Ausnahme: läuft die Verschlüsselung aktiv, kann schnelles Trennen Vorrang haben – im Zweifel die Hotline fragen.)

3 Beweise, Backups & Zugänge

Protokolle, Speicherabbilder und die Erpressernachricht sichern. **Backups schützen** (offline oder unveränderlich vom Netz nehmen) und **privilegierte Zugänge sofort sperren oder rotieren** – Domain-Admin, Service-, VPN- und Backup-Konten. Fast jede Gruppe lebt von gestohlenen Zugangsdaten.

4 Hotline & Versicherung

Holen Sie früh Spezialisten dazu – die Argos-Notfall-Hotline ist rund um die Uhr erreichbar: **+49 89 45 24 24-112**. Informieren Sie zeitnah Ihre Cyber-Versicherung oder den Breach-Coach; die frühe Meldung ist oft Policen-Bedingung.

5 Die Uhr läuft

Meldepflichten prüfen: nach DSGVO an die Aufsicht (Art. 33, i. d. R. binnen 72 Stunden) und ggf. an die Betroffenen (Art. 34). **Sofern Ihr Unternehmen als besonders wichtige oder wichtige Einrichtung** unter das BSIG fällt (NIS-2-Umsetzung, seit 6. Dezember 2025 in Kraft), gelten zusätzlich Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden und Abschlussbericht binnen eines Monats – ob Sie in den Anwendungsbereich fallen, hängt von Sektor und Größe ab. Zur Orientierung, keine Rechtsberatung – im Einzelfall anwaltlich prüfen. Die Meldung bleibt bei Ihnen.

6 Nicht vorschnell zahlen

Keine Zahlung ohne forensische Prüfung, Sanktionslisten-Abgleich und rechtliche Begleitung. Zahlung schützt nicht zuverlässig vor Veröffentlichung.

Vorab ausfüllen und aushängen: interne Eskalationskette (wer entscheidet den Notbetrieb, wer informiert Geschäftsleitung und Datenschutzbeauftragte), zweite erreichbare Rufnummer, Ihre Argos-Kundennummer und der Ablageort Ihres IR-Plans.

24/7-Notfall-Hotline: +49 89 45 24 24-112 · argos.security/notfall – im Ernstfall reagieren eingespielte IR-Teams. Die Teamgröße richtet sich nach dem Vorfall; bei großen Lagen kommen bis zu 20 Spezialisten zum Einsatz. Vereinbarte Reaktionszeiten gelten für Kunden mit IR-Retainer.

FALLSTUDIE · EIN KUNDE IM ERNSTFALL

RIVA Engineering: vom Totalausfall zurück in den Regelbetrieb.

Wer den Grand Tower in Frankfurt, das Kingdom Centre in Riad oder den Royal Clock Tower in Mekka kennt, sieht das Werk von RIVA Engineering – einem international tätigen Fassadenbau-Unternehmen aus dem Mittelstand. Am 15. Dezember 2025 stand dort plötzlich alles still.

So verlief der Ernstfall

- **15. DEZ · 05:45 UHR**
  Das Telefon klingelt: Mitarbeitende können sich nicht einloggen. Die gesamte virtuelle Umgebung ist verschlüsselt.
- **BINNEN STUNDEN**
  Das Incident-Response-Team von Argos bringt den Angriff unter Kontrolle und sichert Beweise.
- **NOTBETRIEB**
  Ein strukturierter Notbetrieb hält die Produktion am Laufen – auch über Weihnachten, Feiertage und Silvester, durchgehend erreichbar.
- **7. JAN 2026 · REGELBETRIEB**
  Rückkehr in den Regelbetrieb – mit einer Sicherheitsarchitektur, die heute stärker ist als zuvor.

„Wir mussten uns um nichts kümmern. Wir wurden mit Fakten betankt – uns wurde gesagt, was zu tun ist, und wir bekamen eine Entscheidungsgrundlage."

Sebastian Altmann
Head of IT, RIVA Engineering

„Es ist nicht die Frage, ob man gehackt wird, sondern wann. Entscheidend ist, dass Systeme, Teams und Dienstleister zusammenspielen – und dass man Expertise hinzuzieht, statt an der Sicherheit zu sparen."

Sebastian Altmann, Head of IT, RIVA Engineering

~3 Wochen
vom Totalausfall zurück in den Regelbetrieb (15. Dez – 7. Jan)

Durchgängig
Notbetrieb über Weihnachten und Silvester – die Produktion lief weiter

Forensisch
Beweise gesichert – Grundlage für Aufarbeitung, Versicherung und Behörden

Was daraus übertragbar ist

Expertise früh hinzuziehen statt an der Sicherheit zu sparen – im Ernstfall zählen eingespielte Teams.

Notbetrieb strukturieren: ein geordneter Minimalbetrieb hält die Produktion, während wiederhergestellt wird.

Stärker zurückkehren: den Wiederanlauf nutzen, um die Sicherheitsarchitektur dauerhaft zu härten.

Aus der gemeinsam bewältigten Krise ist mehr als eine Lieferantenbeziehung geworden: „Argos Security ist für uns mittlerweile mehr als ein Dienstleister." Die vollständige Case Study – mit Zeitachse, Vorgehen und Lessons Learned – erhalten Sie auf Anfrage.

Einzelfall. Verlauf und Dauer eines Vorfalls hängen von der Umgebung, der Backup-Lage und dem Zeitpunkt ab, zu dem Spezialisten eingebunden werden. Die genannten Werte beschreiben diesen konkreten Einsatz und sind keine Prognose für andere Vorfälle. Veröffentlichung mit Einverständnis von RIVA Engineering; alle Zitate von der genannten Person freigegeben.

MODERN CYBER DEFENSE APPROACH · EIN SOC ALLEIN GENÜGT NICHT

Aufhören zu reagieren. Anfangen zu verteidigen.

Werkzeuge allein – Firewall, Virenschutz, Backup – bilden kein Verteidigungssystem. Der Modern Cyber Defense Approach geht vom Ernstfall aus und fragt nicht nur „Wie halte ich Angreifer draußen?“, sondern vor allem: „Wie schnell erkenne und stoppe ich einen, der bereits drin ist?“ Die **Roadmap to Resilience** ist der Weg dorthin.

WERKZEUG-ZENTRIERT

- Werkzeuge nebeneinander, ohne gemeinsames Lagebild
- Viele Alarme – wenig Priorisierung
- Erkennung oft erst, wenn Schaden entsteht
- Ernstfall selten geübt, Rollen unklar
- Erkennung nicht durchgängig rund um die Uhr

HEUTE · MODERN CYBER DEFENSE (CDC)

+ Ein Lagebild aus allen Quellen – 24/7 im CDC
+ Threat Intelligence steuert die Erkennung
+ Angriffe werden früh erkannt und eingedämmt
+ Incident Response geübt und im Retainer
+ Rund um die Uhr besetzt, KI-gestützt

DER WEG · ROADMAP TO RESILIENCE

1 → 2 → 3 → 4 → 5

1 PREPARE
Vorsorge
Risiken kennen, Angriffsfläche reduzieren, den Ernstfall üben.

2 PROTECT
Schutz
Zugänge, Endpunkte und Netze härten – das Fundament.

3 DETECT
Erkennen
24/7 sehen, was passiert – kalibriert auf Ihre Bedrohungslage.

4 RESPOND
Reagieren
Im Ernstfall sofort eindämmen und den Betrieb wiederherstellen.

5 IMPROVE
Verbessern
Aus jedem Vorfall lernen, den Reifegrad kontinuierlich heben.

Kurz gesagt: aus einer Sammlung von Werkzeugen wird ein System, das rund um die Uhr sieht, bewertet und handelt – Schritt für Schritt zu nachweisbarer Sorgfalt und höherer Reife. Diese Dokumentation ist der Nachweis, auf den sich die Leitung stützen kann, wenn sie später darlegen muss, wie sie gehandelt hat.

DIE ANTWORT · CYBER DEFENSE CENTER

Ein System, das Angriffe früh erkennt und eindämmt.

Das Cyber Defense Center (CDC) ist der Kern des Modern Cyber Defense Approach: ein durchgehend besetztes Verteidigungssystem, das vier Bausteine zu einem Ganzen verbindet – KI-gestützt, auf Wunsch mit Datenhaltung in Deutschland und immer mit erfahrenen Analystinnen und Analysten im Entscheidungsweg.

24/7-Erkennung

Rund-um-die-Uhr-Überwachung im CDC; Alarme werden bewertet, nicht nur gezählt.

Incident Response

Retainer mit vertraglich vereinbarten Reaktionszeiten; je nach Vorfall kommen bis zu 20 Spezialisten zum Einsatz.

Threat Intelligence

Weiß, welche Gruppen auf Ihre Branche zielen – und kalibriert die Erkennung darauf.

IR-Readiness

Übt den Ernstfall, bevor er eintritt: Resilience Check, Workshops, Tabletop.

PREPARE PROTECT **DETECT** **RESPOND** IMPROVE

Das CDC ist der aktive Kern Ihrer **Roadmap to Resilience** – mit Schwerpunkt auf Erkennen und Reagieren, getragen von Vorsorge, Schutz und ständiger Verbesserung.

Was das konkret heißt: Die Erkennung im CDC ist auf genau die Gruppen kalibriert, die dieser Report zeigt – Qilin, SafePay, The Gentlemen & Co. – und wird laufend mit eigener Threat Intelligence nachgeschärft. Kein Werkzeugkasten von der Stange, sondern ein Lagebild für Ihre Branche.

Früher erkennen

Auffälligkeiten können auffallen, bevor aus dem Zugriff ein Schaden wird.

Schneller stoppen

Eine eingespielte Reaktion hilft, einen laufenden Angriff früh einzudämmen.

Nachweisbar handeln

Dokumentierte Entscheidungen belegen die von Ihnen geforderte Sorgfalt.

seit 1999
deutscher Cybersecurity-Spezialist

1.000+
Kunden im DACH-Raum

ISO 27001
TÜV SÜD; Datenhaltung auf Wunsch in Deutschland

bis 20
IR-Spezialisten im Ernstfall

REGULATORIK & HAFTUNG · DIE PFLICHT

Cyberabwehr ist heute gesetzliche Pflicht – und Chefsache.

Die Bedrohungslage ist das eine – die rechtliche Pflicht das andere. NIS-2, DSGVO & Co. verlangen nachweisbare Vorsorge. Wer sie unterlässt, riskiert Bußgelder – und in bestimmten Fällen die persönliche Verantwortung der Leitung. Diese Pflichten lassen sich nicht wegdelegieren; ein Cyber Defense Center unterstützt Sie dabei, sie zu erfüllen.

REGELWERK	WAS ES VERLANGT	WIE DAS CDC UNTERSTÜTZT
NIS-2 / BSIG für besonders wichtige und wichtige Einrichtungen	Risikomanagement, Meldepflichten (24 Stunden / 72 Stunden / ein Monat) und Verantwortung der Leitung. Bußgelder bis 10 Mio. € oder 2 % des weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist – für besonders wichtige Einrichtungen, bis 7 Mio. € oder 1,4 % für wichtige Einrichtungen.	24/7-Erkennung, dokumentierte Prozesse und **Unterstützung bei Ihrer fristgerechten Meldung** – die Meldung selbst bleibt bei Ihnen.
Leitungspflichten § 38 BSIG	Die Geschäftsleitung muss Risikomanagementmaßnahmen selbst billigen und überwachen und sich schulen lassen. Diese Pflichten sind nicht delegierbar; die allgemeine Haftung der Leitung nach Gesellschaftsrecht bleibt unberührt.	Liefert **das Lagebild und die Nachweise**, mit denen die Leitung ihrer Aufsichtspflicht sichtbar nachkommt.
DSGVO Art. 32, 33, 34	Angemessene technische und organisatorische Maßnahmen sowie Meldung von Datenpannen unverzüglich (an die Aufsicht i. d. R. binnen 72 Stunden). Verstöße gegen Art. 32–34 sind mit bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes bedroht, je nachdem welcher Betrag höher ist (Art. 83 Abs. 4 lit. a); andere Verstöße können 20 Mio. € oder 4 % erreichen.	Frühe Erkennung von Datenabfluss und belastbare Dokumentation als Basis Ihrer Meldung.
GmbHG § 43 / AktG § 93 Gesellschaftsrecht	Sorgfalt eines ordentlichen Geschäftsmanns – sonst persönliche Haftung gegenüber der Gesellschaft für den Schaden.	Belegt **nachweisbare Sorgfalt**: durchgehende Überwachung, geübte Reaktion, dokumentierte Entscheidungen.
DORA / KRITIS nur für betroffene Sektoren	DORA: Finanzsektor (EU-Verordnung, anwendbar seit 17. Januar 2025). KRITIS: Betreiber kritischer Infrastrukturen – IKT-Risikomanagement bzw. unverzügliche Störungsmeldung.	Deckt Monitoring, Vorfallreaktion und Berichtsfähigkeit als Bausteine dieser Anforderungen ab.

Warum Dokumentation zählt: Nach § 93 Abs. 2 Satz 2 AktG (und § 43 GmbHG entsprechend) trifft die Leitung die Darlegungs- und Beweislast dafür, dass sie sorgfältig gehandelt hat. Durchgehende Überwachung, eine geübte Reaktion und dokumentierte Entscheidungen erleichtern diesen Nachweis – sie beseitigen weder die Pflicht noch die Haftung.

bis 10 Mio. €

oder 2 % des weltweiten Jahresumsatzes – der Bußgeldrahmen für Verstöße gegen Art. 32–34 DSGVO (Art. 83 Abs. 4 lit. a). Für andere Verstöße gelten höhere Stufen; hinzu kommen kann die persönliche Haftung der Leitung gegenüber der Gesellschaft nach § 43 GmbHG / § 93 AktG. Zum Vergleich: Die Wiederherstellung nach einem Ransomware-Angriff kostete zuletzt im Schnitt 1,53 Mio. US-$ – ohne Lösegeld (Sophos, State of Ransomware 2025).

Unabhängig von jedem Dienstleister bleibt die Grundpflicht bei Ihnen: Verantwortliche benennen, Risiken dokumentieren, Melde- und Eskalationswege festlegen. Ein CDC unterstützt bei der Umsetzung – die Verantwortung bleibt in der Leitung.

AUSBLICK · WAS ALS NÄCHSTES KOMMT

Zwei Schritte, die wir jetzt gehen.

Der RADAR schaut auch nach vorn: An zwei Entwicklungen arbeitet Argos bereits – einem mobilen Notfall-Rechenzentrum für den Ernstfall und mehr digitaler Souveränität für das CDC.

COMING SOON · MIT STACKIT / SCHWARZ DIGITS

Der IR-Container

Ein mobiles Notfall-Rechenzentrum, das nach einer Vollverschlüsselung den Wiederanlauf beschleunigt – die Brücke, bis Ihr Rechenzentrum wieder läuft. Gemeinsam mit STACKIT / Schwarz Digits.

1 Alarm & Bedarf
Umfang klären, Kapazitätsklasse (S/M/L) festlegen.

2 Container rollt an
In der Regel binnen 48 Stunden vor Ort, eigene Uplinks.

3 Minimalbetrieb
Die STACKIT-Umgebung bringt den Notbetrieb zurück (in der Regel 5–7 Tage).

4 Rückführung
Nach Stabilisierung sauber zurück in Ihre Umgebung.

Übergangslösung, kein RZ-Ersatz. Die Werte sind **Zielwerte für ein Angebot in Entwicklung** – Richtwerte, keine Zusagen. **Jetzt vormerken:** argos.security/kontakt

VORAUSSICHTLICH AB Q1/2027

Souveräneres CDC

Digitale Souveränität wird zur Anforderung: Wer hat Zugriff auf sicherheitsrelevante Daten – und unter wessen Rechtsordnung? Argos entwickelt darauf eine Antwort.

Souverän by Design
Darauf ausgelegt, dass Betrieb, Daten und Kontrolle unter deutscher bzw. europäischer Rechtsordnung liegen.

Datenhaltung in DE
Auf Wunsch in Deutschland – darauf ausgelegt, Abfluss in Drittländer zu vermeiden.

Gleiche CDC-Stärke
24/7-Erkennung, Incident Response und Threat Intelligence ohne Kompromiss.

Wer das heute schon fordert: öffentliche Hand und Kommunen · regulierte Branchen unter NIS-2 und DORA · Unternehmen, die Zugriffe aus Drittstaaten auf sensible Daten ausschließen wollen.

In Entwicklung. Verfügbarkeit **voraussichtlich ab Q1/2027**. Als Pilotkunde mitgestalten? Sprechen Sie uns an.

IR-CONTAINER · ECKDATEN (Zielwerte für ein Angebot in Entwicklung – keine Zusagen)

i. d. R. 48 h	5–7 Tage	S · M · L	Zonenmodell
bis vor Ort	bis Notbetrieb (i. d. R.)	Kapazitätsklassen	Quarantäne / Clean / Recovery

Das gemeinsame Fundament: Beide Schritte bauen auf in Deutschland betriebener Infrastruktur – für den IR-Container gemeinsam mit STACKIT / Schwarz Digits. Souveränität entsteht dort, wo Betrieb, Daten und Partner unter einer Rechtsordnung stehen.

Beide Schritte zahlen auf dasselbe Ziel ein: wirksame Verteidigung, die im Ernstfall trägt – und unter Ihrer Kontrolle bleibt.

DAS ANGEBOT · ALLES AUS EINER HAND

Über 30 Leistungen entlang der fünf Säulen.

Von der Vorsorge bis zur Verbesserung: Argos deckt den kompletten Weg zur Cyber-Resilienz ab – koordiniert aus einer Hand, damit zwischen einzeln beschafften Werkzeugen möglichst wenige Lücken entstehen. Zu jeder Leistung gibt es einen kompakten KLARTEXT-Entscheider-Guide.

PREPARE

- Roadmap to Resilience
- Cyber Security Assessment
- CTEM
- IT-Compliance Consulting
- Penetration Testing
- Tabletop Exercises
- Incident Response Plan
- ISB as a Service
- Business Continuity Management

PROTECT

- Managed Firewall
- Endpoint Protection
- Email Security
- Email Encryption
- Email Archiving
- Secure SD-WAN
- SASE
- ZTNA
- Network Access Control (NAC)
- OT-/IoT-Security

DETECT

- Cyber Defense Center
- SOC as a Service
- SIEM as a Service
- Managed XDR
- SOAR

RESPOND

- Incident Response 24/7
- IR-Retainer
- Incident Response Portal
- Krisenmanagement
- Unterstützung bei Behördenmeldungen
- Recovery & Wiederherstellung
- IR-Container (bald)

IMPROVE

- vCISO
- Vulnerability Management
- Security Awareness

Darauf sind wir stolz. Von ISG als **Rising Star** im ISG-Provider-Lens-Quadranten Next-Gen SOC/MDR (Midmarket, Deutschland) ausgezeichnet. Bei den **CRN Channel Awards Deutschland 2026** ist Argos Finalist als MSSP des Jahres, und unsere Head of Partner Ecosystem, Xenia Sausele, ist Finalistin als MSSP Channel Partner des Jahres.

ISG PROVIDER LENS

Rising Star – Next-Gen SOC/MDR (Midmarket)

CRN AWARDS DE 2026 · FINALISTIN

MSSP Channel Partner des Jahres

Xenia Sausele, Head of Partner Ecosystem

Alle Leistungen im Detail: argos.security/leistungen · Entscheider-Guides zu jeder Leistung erhalten Sie auf Anfrage bei Ihrem Argos-Ansprechpartner.

ÜBER ARGOS · IHR PARTNER FÜR CYBER-RESILIENZ

Sprechen Sie mit uns – solange Sie in Ruhe entscheiden können.

Argos Security verteidigt den deutschsprachigen Mittelstand seit 1999 – als spezialisierter deutscher Anbieter mit 24/7-Cyber Defense Center, eingespielten Incident-Response-Teams und Threat Intelligence aus eigener Hand.

IHR ANSPRECHPARTNER · VERTRIEB

Dr. Nils Kaufmann
Chief Sales Officer
+49 89 45 24 24-100
sales@argos.security

Im Notfall – rund um die Uhr

+49 89 45 24 24-112

argos.security/notfall

„Wer die Lage kennt, entscheidet ruhiger. Und rechtzeitig.“

Impressum & Hinweise. Herausgeber: Argos Security GmbH, Koppstraße 14, 81379 München – Amtsgericht München, HRB 125981 – Geschäftsführer: Frank Pütz – USt-IdNr. DE457351414 – Standorte München und Freiburg – +49 89 45 24 24-100 – kontakt@argos.security – argos.security. Verantwortlich für den redaktionellen Inhalt nach § 18 Abs. 2 MStV: Nicolai Landzettel, Chief Marketing Officer, c/o Argos Security GmbH, Anschrift wie oben. Redaktion und Threat Intelligence: Argos Security. ARGOS RADAR ist ein kostenloser, vierteljährlicher Informationsdienst für Kunden und Interessenten und stellt **keine Rechts- oder Anlageberatung** dar. Alle Angaben nach bestem Wissen, Stand 3. August 2026. Wir übernehmen keine Haftung für Richtigkeit, Vollständigkeit oder Aktualität; die Haftung für Vorsatz und grobe Fahrlässigkeit sowie für Schäden an Leben, Körper und Gesundheit bleibt unberührt. Threat-Daten teils selbstberichtet durch die Täter. **Wie Sie diesen Report erhalten:** Wir versenden ARGOS RADAR per E-Mail nur an Empfänger, die eingewilligt haben, oder an Bestandskunden nach § 7 Abs. 3 UWG. Empfänger in Österreich, der Schweiz und dem Vereinigten Königreich erhalten elektronische Zusendungen ausschließlich auf Grundlage vorheriger Einwilligung. Wir verarbeiten Ihre geschäftlichen Kontaktdaten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an Direktwerbung). **Sie können jederzeit nach Art. 21 Abs. 2 DSGVO widersprechen**, kostenfrei abgesehen von Übermittlungskosten nach Basistarif – eine formlose Nachricht an kontakt@argos.security genügt. Datenschutzerklärung: argos.security/datenschutz.

Drittnamen. Genannte Produkt- und Firmennamen sind Marken ihrer jeweiligen Inhaber und werden nur zur Identifikation verwendet. Verweise auf konkrete Produkte beziehen sich ausschließlich auf öffentlich berichtete Schwachstellen und Vorfälle zum genannten Stand; sie treffen keine Aussage über die generelle Sicherheit oder Qualität dieser Produkte und begründen keine Geschäftsbeziehung.

IN DER NÄCHSTEN AUSGABE · 03/26

- → Quartalsrückblick der Bedrohungslage
- → Deep-Dive: das souveräne CDC
- → Branchen-Spotlight: Fertigung & Gesundheit
- → Ihre Fragen an unser CDC-Team