ARGOS RADAR · AUSGABE 01/26

RADAR

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

→ Wer Q1 2026 am aktivsten 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 ersten 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, 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 war gestern. Heute braucht es einen **Modern Cyber Defense Approach**: Sicherheit nicht als Sammlung einzelner Werkzeuge, sondern als durchgehend besetztes, geübtes und nachrichtendienstlich informiertes **Cyber Defense Center**. Der Weg dorthin ist unsere **Roadmap to Resilience** – 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 hin 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. €
geschätzter jährlicher Schaden durch Cyberangriffe in Deutschland (Bitkom-Hochrechnung 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

DIE LAGE · Q1 2026

Die Bedrohung verdichtet sich – 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 können. Q1 2026 war Qilin die weltweit aktivste Gruppe – und LockBit meldete sich mit +106 % zum Vorquartal eindrucksvoll zurück.

Am stärksten betroffene Sektoren im DACH-Raum

Qualitative Einordnung (kein Messwert) auf Basis von Argos-Threat-Intelligence & öffentlichen Leak-Site-Auswertungen, Q1 2026. Die Balkenlänge zeigt die relative Betroffenheit; Fertigung und Gesundheitswesen bleiben die Hauptziele.

Was diese Lage antreibt

- **Tempo.** Von der Schwachstellen-Veröffentlichung bis zum Angriff 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 auf Verschlüsselung und erpressen allein mit gestohlenen Daten.
- **DACH im Fokus.** Deutschsprachige Unternehmen zählen bei vielen Gruppen ausdrücklich zu den Top-Zielregionen.

Qilin
weltweit aktivste Gruppe in Q1 2026

+106 %
Anstieg der LockBit-Opferlistungen zum Vorquartal

6 neue
neue & aufstrebende Gruppen in diesem Report porträtiert

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 Q1 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 mit konkreten Erstmaßnahmen im Detail vor.

#	Gruppe	Status	Primäre Ziele (DACH)	Warum jetzt relevant
01	Qilin / Agenda	AKTIV	Gesundheit, Fertigung, Kommunen	Global #1 – 338 Opfer in Q1/26; MSP-Angriffe mit Kettenwirkung
02	Akira	AKTIV	Finanz, Fertigung, Bildung	VPN-Appliances ohne MFA als Haupttor; DACH-Opfer belegt
03	Play	AKTIV	Fertigung, Bau, öffentl. Sektor	Intermittierende Verschlüsselung, wiederkehrende Kampagnen
04	LockBit (5.0)	AKTIV	Fertigung, Gesundheit, Finanz	Comeback nach Cronos: +106 % zum Vorquartal
05	DragonForce	AKTIV	Handel, Dienstleistung	„Kartell“-Modell, aggressive Expansion
06	Cl0p	AKTIV	Finanz, Software-Lieferketten	Massenangriffe über Schwachstellen in Transfer-Tools
07	Rhysida	AKTIV	Gesundheit, Bildung, Behörden	Zielt gezielt auf besonders sensible Sektoren
08	INC Ransom	AKTIV	Gesundheit, Industrie	Etablierter Erpresser mit Datendiebstahl
09	Sarcoma / Lynx	AKTIV	Fertigung, Dienstleistung	Wachsende Mittelstands-Bedrohung
10	Medusa	GESCHWÄCHT	Bildung, Technologie	Deutlich weniger Opfer seit Feb/26 – aber nicht verschwunden

Quellen: Argos Threat Intelligence, öffentliche Leak-Site-Auswertungen (u. a. ransomware.live), CISA, Europol · Stand Juni 2026.
Hinweis: Opferzahlen beruhen überwiegend auf selbstberichteten Leak-Site-Angaben und sind nicht durchgängig unabhängig bestätigt. Die Reihenfolge gewichtet Aktivität, DACH-Relevanz und Neuheit – sie ist keine reine Opferzahl-Rangliste. Das vollständige, wöchentlich aktualisierte Lexikon mit über 60 Profilen: argos.security/wissen/threat-actor-hub

> Klartext-Glossar: **RaaS** = vermietete Ransomware-Baukästen · **Double Extortion** = Verschlüsseln + Datendiebstahl · **MFA** = Mehr-Faktor-Anmeldung · **RDP/VPN** = Fernzugänge · **EDR** = Endpunkt-Erkennung

„Geschwächt“ heißt nicht „weg“: Gruppen wie Medusa pausieren, benennen sich um und kehren zurück.
Wer nur den Schlagzeilen folgt, verteidigt gegen die Gruppen von gestern.

GRUPPE IM PROFIL · 1 / 8

Acht aktive Gruppen im Detail – jeweils mit den Erstmaßnahmen, die im Ernstfall zählen. Was „Sofort tun“ und was „Unbedingt vermeiden“ ist, leitet sich direkt aus dem typischen Vorgehen der Gruppe ab.

Qilin

AKTIV

auch bekannt als: Agenda, Qilin v2

1.929 auf Leak-Sites gelistete Opfer in 99 Ländern seit Oktober 2022 (Stand Mitte Juni 2026), davon 338 gelistete Opfer in Q1 2026

Qilin ist seit drei Quartalen in Folge (Q3 2025 bis Q1 2026) die weltweit aktivste Ransomware-Gruppe. 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

Die derzeit aktivste Gruppe 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"

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 gültige 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 (ScreenConnect, AnyDesk). Zunehmend auch über Managed-Service-Provider mit Kettenwirkung.

DACH-Bezug: Qilin zählt DACH ausdrücklich zu ihren 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 absichern & im Verdachtsfall tun

+ Exponierte RDP- und VPN-Zugänge (insbesondere FortiGate, Citrix) sofort auf Patchstand prüfen und MFA für alle Fernzugriffe erzwingen
+ Fernwartungstools (ScreenConnect, AnyDesk, TeamViewer) auf autorisierte Installationen prüfen und unbekannte Instanzen isolieren
+ Gespeicherte Zugangsdaten in Browsern (insbesondere VPN-Logins) unternehmensweit zurücksetzen, da für Qilin das Abgreifen gespeicherter Browser-Zugangsdaten (u.a. per verteilter Skripte) berichtet wird
+ ESXi- und Virtualisierungsinfrastruktur separat absichern (Netzsegmentierung, MFA für Hypervisor-Management), da Qilin explizit auf VMware ESXi zielt

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-/Werkzeug-Zuordnungen sind Momentaufnahmen (Stand Juni 2026).

GRUPPE IM PROFIL · 2 / 8

LockBit

AKTIV

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

163 Opfer allein in Q1 2026 (+106 % gegenüber Q4 2025) — einer der stärksten Zuwächse im Quartal nach dem Cronos-Rückschlag

LockBit ist eine der langlebigsten und produktivsten RaaS-Gruppen überhaupt: kumulativ über 2.757 gelistete Opfer in mehr als 120 Ländern. Trotz der teilweisen Zerschlagung ihrer Infrastruktur durch „Operation Cronos" (Februar 2024) nahm die Gruppe den Betrieb binnen weniger Wochen wieder auf und veröffentlichte im September 2025 bereits die fünfte Malware-Generation (LockBit 5.0); im ersten Quartal 2026 war sie mit 163 Opfern die weltweit viertaktivste Ransomware-Gruppe.

FÜR ENTSCHEIDER · IN EINEM SATZ

Der Wiederholungstäter – nach der Zerschlagung zurück und stärker. Schutz: Fernzugänge mit Mehr-Faktor-Login, Perimeter patchen, Protokolle sichern.

Steckbrief

Status	Aktiv
Modell	RaaS (Ransomware-as-a-Service), Eigenentwicklung seit 2019
Herkunft	Russland/Osteuropa (vermutet); mutmaßlicher Kopf laut NCA/Europol: Dmitry Khoroshev (Alias „LockBitSupp")
Aktiv seit	2019

Primäre Zielsektoren

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

Vorgehen

Modus Operandi: Double Extortion: Vollverschlüsselung plus Datendiebstahl, Veröffentlichung auf Leak-Seite mit Countdown zur Lösegelderpressung

Einfallstor: Haupteinfallstore sind Phishing/Spear-Phishing mit gefälschten Passwort-Reset-Mails und schädlichen Anhängen, der Missbrauch exponierter RDP-Zugänge (Brute-Force oder aus Infostealer-Logs gestohlene Zugangsdaten) sowie das Ausnutzen öffentlich erreichbarer Anwendungen (u. a. Fortinet FortiOS/FortiProxy, Atlassian Confluence, Log4Shell-Schwachstellen). Zusätzlich kommen im Darknet gekaufte oder gestohlene gültige Konten (Valid Accounts) zum Einsatz.

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

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, Notwendigkeit prüfen und MFA erzwingen
+ Öffentlich erreichbare Systeme (v. a. Fortinet FortiOS/FortiProxy, Atlassian Confluence) umgehend patchen und auf bekannte CVEs prüfen
+ Zugangsdaten aus Infostealer-Logs/Dark-Web-Leaks abgleichen und betroffene Konten zurücksetzen
+ EDR/AV-Manipulationsschutz aktivieren und Windows-Ereignisprotokolle zentral/unveränderlich auslagern, da LockBit Logs aktiv löscht (EvtClearLog) und ETW patcht

Unbedingt vermeiden

– RDP/VPN-Zugänge ungeschützt und ohne MFA aus dem Internet erreichbar lassen
– Auf Signatur-basierte AV-Erkennung allein vertrauen — für LockBit werden seit 2025 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-/Werkzeug-Zuordnungen sind Momentaufnahmen (Stand Juni 2026).

GRUPPE IM PROFIL · 3 / 8

Akira

AKTIV

auch bekannt als: Akira Ransomware

Über 1.000 auf Leak-Sites gelistete Opfer seit März 2023; zählt zu den produktivsten Gruppen weltweit; typische Forderungen 200.000 bis mehrere Mio. USD

Akira ist seit März 2023 aktiv und zählt Stand Juni 2026 zu den produktivsten Ransomware-Gruppen weltweit – ohne bisherige Festnahmen, Zerschlagung oder bestätigtes Rebranding. Kennzeichnend sind die Retro-Gestaltung der Leak-Seite und die konsequente Weiterentwicklung auf mehrere Plattformen (Windows, Linux/ESXi, seit Juni 2025 auch Nutanix AHV).

FÜR ENTSCHEIDER · IN EINEM SATZ

Kommt fast immer über einen VPN-Zugang ohne Mehr-Faktor-Login herein. Schutz: VPN patchen, MFA erzwingen, Backups härten.

Steckbrief

Status	Aktiv
Modell	Ransomware-as-a-Service (RaaS)
Herkunft	Russland/Osteuropa (stark vermutet); mögliche Verbindung zu ehemaligen Conti-Operatoren
Aktiv seit	2023

Primäre Zielsektoren

Finanzwesen · Fertigung · Gesundheitswesen · Bildung · kritische Infrastruktur

Vorgehen

Modus Operandi: Double Extortion: Datendiebstahl kombiniert mit Verschlüsselung, Drohung mit Veröffentlichung auf der Leak-Seite bei Nichtzahlung

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

DACH-Bezug: Akira zielt neben den USA auch auf die DACH-Region; belegt ist unter anderem der Fall eines Schweizer Fertigungsunternehmens (2025).

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Alle öffentlich erreichbaren VPN-Appliances (Cisco ASA, SonicWall SonicOS) umgehend auf die genannten CVEs patchen und MFA für sämtliche VPN-/Fernzugänge erzwingen
+ Veeam Backup and Replication auf aktuellen Patch-Stand prüfen (CVE-2024-40711, CVE-2023-27532), da Akira Backups gezielt als Sprungbrett nutzt und Schattenkopien löscht
+ RDP-Exposition nach außen unterbinden bzw. auf MFA-geschützte Zugänge (z. B. VPN-Gateway) beschränken; interne RDP-Nutzung überwachen
+ Auf verdächtige Remote-Tools wie AnyDesk, LogMeIn, Ngrok und PuTTY-Tunnel sowie auf Discovery-Aktivitäten (Advanced IP Scanner, BloodHound, AdFind) achten – typische Vorboten eines Akira-Angriffs

Unbedingt vermeiden

– Lösegeld ohne vorherige forensische Prüfung und Rechtsberatung zahlen – Akira fordert typischerweise 200.000 bis 4 Mio. USD, Zahlung schützt nicht zuverlässig vor Datenveröffentlichung
– Betroffene Systeme vorschnell neu aufsetzen oder Volume Shadow Copies/Logs löschen lassen, bevor Beweise gesichert sind – Akira löscht selbst Schattenkopien und Admin-Konten zur Behinderung der Reaktion
– Sich allein auf Windows-Endpunktschutz verlassen – Akira verschlüsselt gezielt 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-/Werkzeug-Zuordnungen sind Momentaufnahmen (Stand Juni 2026).

GRUPPE IM PROFIL · 4 / 8

Play

AKTIV

auch bekannt als: PlayCrypt, Balloonfly

Über 900 namentlich gelistete Opfer auf der Leak-Site seit 2022, mit mehr als 6 Opfern an einem einzigen Tag (7. März 2026)

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 (kein klassisches RaaS, zentral gesteuert)
Herkunft	Unbekannt (Lateinamerika vermutet, möglicherweise Brasilien/Argentinien)
Aktiv seit	2022

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: Play verschafft sich Zugang vorrangig über 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 werden gekaufte Zugangsdaten von Initial-Access-Brokern, exponierte RDP-/VPN-Endpunkte sowie zuletzt ausgenutzte SimpleHelp-RMM-Schwachstellen (CVE-2024-57726/27/28) und die Windows-CLFS-Zero-Day-Lücke CVE-2025-29824 genutzt, um Systemrechte zu erlangen.

DACH-Bezug: Play zählt DACH explizit zu den Zielregionen; im Juni 2026 wurde ein deutsches Unternehmen als Opfer auf der Leak-Site gelistet (Angabe der Täter, nicht unabhängig bestätigt).

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, absichern und MFA erzwingen
+ Microsoft Exchange (ProxyNotShell/OWASSRF), Fortinet-SSL-VPN (CVE-2018-13379, CVE-2020-12812), Cisco ASA und die Windows-CLFS-Lücke CVE-2025-29824 umgehend patchen
+ SimpleHelp- und andere RMM-Installationen auf Aktualität (CVE-2024-57726/27/28) sowie unautorisierte Nutzung prüfen
+ ESXi-Hosts isolieren und auf ungewöhnliche .vmdk/.vmx-Zugriffe sowie Ransom-Notes in /vmfs/volumes/ kontrollieren

Unbedingt vermeiden

– Nicht auf die E-Mail-Kontaktadresse in der Ransom Note (PLAY_README.txt) antworten oder eigenmächtig verhandeln
– Betroffene Systeme nicht vorschnell neu aufsetzen, bevor Grixba-Infostealer-Spuren und AdFind/NetScan-Aktivität forensisch gesichert sind

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

ZWISCHENSTAND · HALBZEIT

Acht Gruppen, fünf Muster.

So unterschiedlich Qilin, LockBit, Akira & Co. auftreten – im Vorgehen ähneln sie sich verblüffend. Wer diese fünf Muster kennt, verteidigt gezielter 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 & 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 – bis hin zu deutschsprachigen Einzeltätern.

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

DragonForce

AKTIV

auch bekannt als: DragonForce Ransomware

580 auf Leak-Sites gelistete Opfer auf der DragonForce-Leak-Site (Stand Mitte Juni 2026), davon 101 allein im ersten Quartal 2026 – ein Anstieg von 29 Prozent gegenüber dem vierten Quartal 2025

DragonForce entstand im August 2023 aus der pro-palästinensischen Hacktivisten-Szene in Malaysia und hat sich seither zu einer kommerziellen RaaS-Plattform gewandelt. Die Gruppe nutzt geleakten LockBit-3.0- und Conti-Code und beliefert unter anderem Scattered-Spider-Affiliates mit ihrem Verschlüsseler, wie die Angriffe auf britische Handelsketten 2025 zeigten.

FÜR ENTSCHEIDER · IN EINEM SATZ

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

Steckbrief

Status	Aktiv
Modell	RaaS (Ransomware-as-a-Service, seit 2024)
Herkunft	Malaysia (ursprünglich pro-palästinensische Hacktivisten, seit 2024 kommerzialisiert)
Aktiv seit	2023

Primäre Zielsektoren

Retail · Kritische Infrastruktur · Regierung · Fertigung · Business Services

Vorgehen

Modus Operandi: Double Extortion (Verschlüsselung + Datenleck), teils zusätzlich DDoS-Druckmittel; der Verschlüsseler wird auch an Drittgruppen wie Scattered Spider vermietet

Einfallstor: Erstzugänge erfolgen über mehrere Wege: Social Engineering, Vishing und Help-Desk-Impersonation (Hauptvektor bei den UK-Retail-Angriffen), Kompromittierung exponierter RDP-Server und VPN-Portale mit gestohlenen oder erratenen Zugangsdaten sowie Ausnutzung öffentlich erreichbarer Web- und Anwendungsserver (u. a. Log4Shell, Ivanti-Connect-Secure-Lücken). Zusätzlich wurden RMM-Schwachstellen in SimpleHelp (CVE-2024-57726/57727/57728) verkettet, um über einen Managed-Service-Provider gleich mehrere nachgelagerte Kunden zu verschlüsseln.

DACH-Bezug: Die Zielregionen umfassen laut Quelle ausdrücklich auch die DACH-Region neben UK, USA und Asien-Pazifik; die MSP-Lieferkettenkompromittierung über SimpleHelp (Mai 2025) zeigt zudem, dass auch deutsche, österreichische und schweizerische Kunden von IT-Dienstleistern indirekt betroffen sein können.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Exponierte RDP- und VPN-Zugänge sofort inventarisieren, aus dem Internet nehmen oder mit MFA absichern
+ Help-Desk-Prozesse gegen Vishing/Social-Engineering härten: Rückruf- und Identitätsprüfung vor jedem Passwort-Reset verpflichtend machen
+ Internetseitige Anwendungs- und VPN-Server auf bekannte Schwachstellen (Log4Shell, Ivanti Connect Secure) patchen und RMM-Software wie SimpleHelp auf aktuellen Stand bringen
+ EDR/XDR-Alarme zu Treiber-Installationen (BYOVD, z. B. TrueSight.sys/RentDrv.sys) und Event-Log-Löschungen sofort eskalieren, da dies typische Vorboten der Verschlüsselungsphase sind

Unbedingt vermeiden

– Lösegeld zahlen oder mit den Erpressern in Verhandlung treten, 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-/Werkzeug-Zuordnungen sind Momentaufnahmen (Stand Juni 2026).

GRUPPE IM PROFIL · 6 / 8

Cl0p

AKTIV

auch bekannt als: Clop, TA505

Über 1.254 erfasste Opfer auf ransomware.live (Stand Mitte 2026); allein am 1. Februar 2026 wurden 22 Opfer an einem einzigen Tag veröffentlicht — arbeitet kampagnengetrieben und wellenförmig (zwischen den Wellen oft ruhend).

Cl0p ist aus dem TA505-/FIN11-Netzwerk hervorgegangen und hat sich auf die massenhafte Ausnutzung von Zero-Day- und N-Day-Schwachstellen in unternehmenskritischer Datenübertragungs- und Enterprise-Software spezialisiert.

FÜR ENTSCHEIDER · IN EINEM SATZ

Schlägt in Wellen über Schwachstellen in Datei-Transfer-Tools zu. Schutz: solche Tools sofort patchen, Datenabfluss überwachen.

Steckbrief

Status	Aktiv
Modell	Privates Kollektiv mit RaaS-Elementen; Fokus auf Massenexfiltration statt Verschlüsselung
Herkunft	Russland/Ukraine (vermutet), enge Verbindung zur TA505-/FIN11-Gruppe
Aktiv seit	2019 (als Cl0p); Vorläufer TA505 bereits seit 2014 aktiv

Primäre Zielsektoren

Finanzwesen · Gesundheitswesen · Logistik · Energieversorgung · Staatsbehörden

Vorgehen

Modus Operandi: Massenexfiltration großer Datenmengen über kompromittierte MFT-/Enterprise-Software, danach Erpressung primär durch Datenleck-Drohung statt Verschlüsselung

Einfallstor: Cl0p ist auf die Massen-Ausnutzung von Zero-Day-Schwachstellen in Datei-Transfer-Software spezialisiert (u. a. MOVEit Transfer, GoAnywhere MFT, Cleo, Oracle E-Business Suite). Nach dem Erstzugriff wird Schadcode zur Datenexfiltration platziert; oft wird gar nicht mehr verschlüsselt, sondern allein mit den gestohlenen Daten erpresst.

DACH-Bezug: Deutschsprachige Unternehmen sind über globale Software-Lieferketten (MOVEit, GoAnywhere, Cleo, Oracle EBS) exponiert; in der öffentlich berichteten Oracle-EBS-Kampagne 2025 wurde auch ein Schweizer Technologiekonzern auf der Leak-Seite genannt.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Alle internetseitig erreichbaren MFT- und Enterprise-Systeme (insbesondere MOVEit, GoAnywhere, Cleo, Oracle EBS) unverzüglich auf aktuelle Patches prüfen und bekannte CVEs (u. a. CVE-2025-61882, CVE-2025-61884) priorisiert schließen
+ Betroffene Systeme auf unbekannte Webshells (z. B. DEWMODE, LEMURLOOT) und ungewöhnliche Datei-Uploads oder Admin-Zugriffe untersuchen
+ Ungewöhnlich große oder schnelle Datenabflüsse (Rclone, MEGASync) aus MFT-Systemen und Datenbanken überwachen und blockieren
+ Bei Verdacht auf Kompromittierung sofort Netzwerksegmentierung der MFT-Systeme prüfen und betroffene Zugangsdaten zurücksetzen

Unbedingt vermeiden

– Enterprise-/MFT-Software ungepatcht oder ungeprüft direkt aus dem Internet erreichbar lassen
– Nach Bekanntwerden einer Kompromittierung vorschnell Lösegeld zahlen oder mit der Gruppe verhandeln, ohne forensische Aufklärung des tatsächlichen Datenabflusses

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

GRUPPE IM PROFIL · 7 / 8

Rhysida

AKTIV

auch bekannt als: Rhysida Ransomware Group

272 auf Leak-Sites gelistete Opfer in 39 Ländern bis Mitte 2026 (ransomware.live), rund 80 neue Fälle allein in 2025

Rhysida ist eine seit Mai 2023 aktive RaaS-Gruppe, vermutlich Nachfolgerin von Vice Society. Sie betreibt Double Extortion mit öffentlicher Versteigerung gestohlener Daten und zeigt trotz eines zwischenzeitlich geknackten Verschlüsselungsverfahrens hohe Widerstandsfähigkeit — bislang keine Strafverfolgungsmaßnahme oder Festnahme.

FÜR ENTSCHEIDER · IN EINEM SATZ

Zielt auf Kliniken, Schulen und Behörden. Schutz: besonders sensible Bereiche absichern, durchgehend überwachen.

Steckbrief

Status	Aktiv
Modell	Ransomware-as-a-Service (RaaS)
Herkunft	Unbekannt (osteuropäischer Raum vermutet); möglicher Nachfolger von Vice Society
Aktiv seit	2023

Primäre Zielsektoren

Gesundheitswesen · Bildung · Öffentliche Verwaltung · Verteidigung · Verkehr/Transport

Vorgehen

Modus Operandi: Double Extortion: Verschlüsselung plus öffentliche Auktion der gestohlenen Daten

Einfallstor: Häufigster Erstzugang sind kompromittierte VPN-Zugangsdaten (Credential Stuffing, Darknet-Käufe, Phishing) sowie Brute-Force gegen RDP- und VPN-Portale. Daneben Phishing-Mails mit schädlichem Anhang, SEO-Poisoning/Typosquatting-Domains (getarnt als Angry IP Scanner, PuTTY, Teams, Chrome) zur Verbreitung von CleanUpLoader oder SharpRhino, Malvertising sowie seit April 2025 Gootloader als zusätzlicher Vektor.

DACH-Bezug: Zielregionen umfassen ausdrücklich den DACH-Raum; laut öffentlichen Berichten war zuletzt auch eine deutsche Großstadt betroffen, mit Veröffentlichung von Dokumenten im Darknet.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Exponierte RDP- und VPN-Zugänge sofort auf Multi-Faktor-Authentifizierung prüfen und MFA erzwingen
+ VPN-Zugangsdaten auf Kompromittierung prüfen (Darknet-Leak-Monitoring) und bei Verdacht umgehend rotieren
+ Downloads von Tools wie Angry IP Scanner, PuTTY, Teams oder Chrome ausschließlich über verifizierte Erstanbieter-Quellen zulassen, Typosquatting-Domains blockieren
+ Auf ungewöhnliche geplante Aufgaben (insbesondere mit dem Namen "Rhsd"), Cobalt-Strike-Beacons sowie NTDS.dit-/LSASS-Zugriffe (Secretsdump/Impacket) und BloodHound-Aktivität in Logs achten

Unbedingt vermeiden

– Auf keinen Fall Lösegeld zahlen, ohne vorherige forensische Prüfung und Einbindung von Strafverfolgung/Rechtsberatung — Rhysida versteigert Daten unabhängig von Zahlung weiter
– ESXi-/Virtualisierungsinfrastruktur nicht ungeschützt lassen: eigene Linux/ESXi-Variante existiert seit Mitte 2024
– Sich nicht allein auf den 2024 bekannt gewordenen PRNG-Exploit verlassen — die Schwachstelle wurde von Rhysida umgehend gepatcht

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

GRUPPE IM PROFIL · 8 / 8

INC Ransom

AKTIV

auch bekannt als: INC Ransom (keine weiteren Aliasse bekannt)

834 Opfer auf der Leak-Site (Stand 18. Juni 2026), davon rund 200 allein im Jahr 2025; Gesundheitswesen macht 29 % der 2025er-Fälle aus.

INC Ransom ist eine seit Juli 2023 aktive RaaS-Gruppe, die bislang von keiner Strafverfolgungsbehörde zerschlagen wurde. Kennzeichnend sind lange Verweildauern zwischen Erstzugriff und Verschlüsselung sowie eine ausgeprägte Fokussierung auf das Gesundheitswesen.

FÜR ENTSCHEIDER · IN EINEM SATZ

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

Steckbrief

Status	Aktiv
Modell	Ransomware-as-a-Service (RaaS)
Herkunft	Unbekannt (Osteuropa vermutet)
Aktiv seit	2023

Primäre Zielsektoren

Gesundheitswesen · Bildung · Regierung · Pharmaindustrie · Verarbeitendes Gewerbe

Vorgehen

Modus Operandi: Double Extortion: Datendiebstahl plus Verschlüsselung, mit auffallend langer Dwell Time vor der eigentlichen Verschlüsselung.

Einfallstor: Erstzugang häufig über Schwachstellen in öffentlich erreichbaren Systemen (u. a. Citrix-NetScaler, CVE-2023-3519) 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 auch im europäischen Raum; ein konkret belegter DACH-Fall liegt uns für dieses Quartal nicht vor.

SO WAPPNEN SIE SICH – UND WAS IM ERNSTFALL GILT

Jetzt absichern & im Verdachtsfall tun

+ Citrix NetScaler ADC/Gateway, FortiClient EMS und SimpleHelp-RMM-Installationen sofort auf die genannten CVEs (u. a. CVE-2023-3519, CVE-2023-48788, CVE-2024-57727, CVE-2025-5777) patchen bzw. isolieren
+ Exponierte RDP- und Fernzugriffsdienste (auch AnyDesk/TightVNC) identifizieren, absichern und MFA erzwingen
+ Active-Directory- und Netzwerk-Enumeration-Aktivität prüfen (AdFind, Advanced IP Scanner, Nltest, Net.exe) sowie PsExec-Nutzung unter Tarnnamen wie 'winupd'/'winupdate.exe' als Indikator werten
+ Zugriff auf Veeam-Backup-Zugangsdaten und lsassy.py-typische Credential-Dumping-Muster überwachen, da Backup-Infrastruktur gezielt angegriffen wird

Unbedingt vermeiden

– Verschlüsselte Systeme nicht vorschnell als vollständig kompromittiert abschreiben, ohne die lange typische Dwell Time und mögliche parallele Datenexfiltration zu berücksichtigen
– Keine Lösegeldzahlung ohne Rücksprache mit Ermittlungsbehörden/Rechtsberatung veranlassen, da Forderungen stark variieren (100.000 bis 5 Mio. USD) und Zahlung keine Löschung der Daten garantiert

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

NEU & AUFSTREBEND · DIE NÄCHSTE WELLE

Neue Gruppen entstehen schneller denn je.

Rebrands zerschlagener Gruppen, Ableger mit geleaktem Code, Spezialisten für einzelne Schwachstellen: Der Markt sortiert sich ständig neu. Vier neue Namen stellen wir hier vor – zwei weitere, mit direktem DACH-Bezug, folgen auf der nächsten Seite.

The Gentlemen

NEU 2025

Innerhalb weniger Monate aufgestiegen; DACH zählt zu den Top-Zielregionen. Klassische Double-Extortion mit schneller Opfer-Taktung.

World Leaks

REBRAND 01/2025

Nachfolger von Hunters International – verzichtet bewusst auf Verschlüsselung und erpresst rein mit gestohlenen Daten. Deutschland unter den vier meistbetroffenen Ländern.

Warlock

AUFSTEIGER

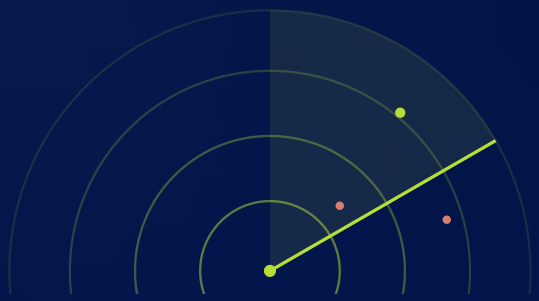
Von Microsoft als „Storm-2603“ verfolgt (Einordnung als Ransomware-Gruppe noch nicht abschließend gesichert). Nutzt die SharePoint-„ToolShell“-Exploit-Kette gegen lokale Server – Opfer auch in DE/AT. Zeigt: ungepatchte Perimeter-Systeme sind das Einfallstor.

Interlock

AUFSTEIGER

Kombiniert „ClickFix“-Social-Engineering (gefälschte „Zum Fortfahren bestätigen“-Dialoge) mit einer Netzwerk-Appliance-Schwachstelle. Der Mensch als erstes Ziel.

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



DACH-SPOTLIGHT · DEUTSCHSPRACHIGE TÄTER

Die Gefahr wird lokaler.

Zwei Entwicklungen zeigen, dass die Szene näher rückt: Ableger auf Basis geleakten Codes mit belegten DACH-Opfern – und deutschsprachige Einzeltäter, die legitime Fernwartung missbrauchen.

Gunra

AKTIV

Baut auf der geleakten **Conti**-Codebasis auf und ist damit sofort schlagkräftig. Ein deutsches Opfer ist belegt – ein Beispiel dafür, wie alter Schadcode als Fundament neuer Gruppen dient.

Was das bedeutet

+ Erprobte, aggressive Verschlüsselung ohne „Anlaufzeit“
+ DACH ausdrücklich im Zielspektrum

Prinz Eugen (Alias: ROOTBOY / germania)

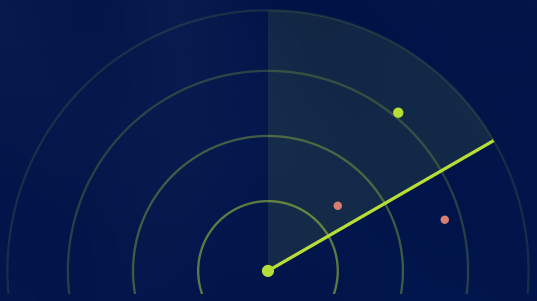
AKTIV

Ein **mutmaßlich deutschsprachiger Einzeltäter**, dem Sicherheitsforscher den Missbrauch legitimer Fernwartungssoftware (RMM) zuschreiben, um in kleinere Unternehmen einzudringen. Kein Konzern-Apparat – und trotzdem gefährlich, weil die Werkzeuge unauffällig und die Ziele schlecht geschützt sind.

Was das bedeutet

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

Gemeinsamer Nenner: Missbrauch legitimer Zugänge – RDP, VPN, Fernwartung. Wer diese Wege lückenlos inventarisiert, mit MFA absichert und überwacht, nimmt der Mehrheit der Angreifer ihr wichtigstes Werkzeug.



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**. Wie der Weg dorthin 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

Logs, Speicherabbilder und die Erpressernachricht sichern. **Backups schützen** (offline / 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 / den Breach-Coach**; die frühe Meldung ist oft Policen-Bedingung.

5 Die Uhr läuft

Meldefristen prüfen: DSGVO an die Aufsicht (Art. 33, i. d. R. 72 h) und ggf. an Betroffene (Art. 34). Nach Inkrafttreten der NIS-2-Umsetzung (Gesetz in DE noch im Verfahren) gelten voraussichtlich Frühwarnung 24 h, Meldung 72 h, Abschluss 1 Monat. 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 & aushängen: interne Eskalationskette (wer entscheidet den Notbetrieb, wer informiert Geschäftsleitung / DSB), zweite erreichbare Rufnummer & Ihre Argos-Kundennummer, Ablageort Ihres IR-Plans.

24/7-Notfall-Hotline: **+49 89 45 24 24-112** · argos.security/notfall – im Ernstfall reagieren eingespielte IR-Teams mit bis zu 20 Spezialisten.

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.“

~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.

MODERN CYBER DEFENSE APPROACH · SOC WAR GESTERN

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?“ Der **Weg dorthin** ist die Roadmap to Resilience.

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 dokumentierte Sorgfalt kann auch die Haftung der Geschäftsleitung mindern.

DIE ANTWORT · CYBER DEFENSE CENTER

Ein System, das Angriffe früh erkennt und stoppt.

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 stets verantwortet von erfahrenen Analystinnen und Analysten.

24/7-Erkennung

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

Incident Response

Retainer mit vertraglich vereinbarten Reaktionszeiten; im Ernstfall bis zu 20 Spezialisten.

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, LockBit, Akira & Co. – und wird laufend mit eigener Threat Intelligence nachgeschärft. Kein Werkzeugkasten von der Stange, sondern ein Lagebild für Ihre Branche.

Früher erkennen

Auffälligkeiten fallen auf, bevor aus dem Zugriff ein Schaden wird.

Schneller stoppen

Eingespielte Reaktion dämmt einen laufenden Angriff früh ein.

Nachweisbar handeln

Dokumentierte Entscheidungen stützen Pflicht & Haftung.

seit 1999
deutscher Cybersecurity-Spezialist

600 +
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 Art. 20, 21, 23	Risikomanagement, Meldepflichten (24 h / 72 h / 1 Monat) und Verantwortung der Leitung. Bußgelder bis **10 Mio. € / 2 %** des Umsatzes.	24/7-Erkennung, dokumentierte Prozesse und **Unterstützung bei der fristgerechten Meldung** – die Meldung selbst bleibt bei Ihnen.
BSIG (künftig) NIS-2-Umsetzungsgesetz (Entwurf); §-Nummer noch nicht final	Nicht delegierbare Billigungs-, Überwachungs- und Schulungspflicht der Geschäftsleitung, mit Innenhaftung.	Liefert das **Lagebild und die Nachweise**, mit denen die Leitung ihrer Aufsichtspflicht sichtbar nachkommt.
DSGVO Art. 32, 33, 34	Angemessene technische Maßnahmen und Meldung von Datenpannen unverzüglich (i. d. R. 72 h). Bußgelder bis **20 Mio. € / 4 %**.	Frühe Erkennung von Datenabfluss und belastbare Dokumentation als Basis Ihrer Meldung.
GmbHG § 43 / AktG § 93	Sorgfalt eines ordentlichen Geschäftsmanns – sonst persönliche Innenhaftung für Schäden.	Belegt **nachweisbare Sorgfalt**: durchgehende Überwachung, geübte Reaktion, dokumentierte Entscheidungen.
DORA / KRITIS nur für betroffene Sektoren	DORA: Finanzsektor (EU-Verordnung, seit 17.01.2025). KRITIS: Betreiber kritischer Infrastrukturen – IKT-Risikomanagement bzw. unverzügliche Störungsmeldung.	Deckt Monitoring, Vorfallreaktion und Berichtsfähigkeit als Bausteine dieser Anforderungen ab.

Der entscheidende Hebel für die Freigabe: Dokumentierte Sorgfalt – durchgehende Überwachung, geübte Reaktion, belegte Entscheidungen – kann die **Haftung von Vorstand und Geschäftsführung spürbar mindern.**

bis 20 Mio. €

DSGVO-Bußgeldrahmen (Art. 83) – plus persönliche Innenhaftung nach § 43 GmbHG / § 93 AktG

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
I. d. R. binnen 48 h vor Ort, eigene Uplinks.

3 Minimalbetrieb
STACKIT-Umgebung bringt den Notbetrieb zurück (i. d. R. 5–7 Tage).

4 Rückführung
Nach Stabilisierung sauber zurück in Ihre Umgebung.

Übergangslösung, kein RZ-Ersatz. 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 welcher Rechtsordnung? Argos entwickelt darauf eine Antwort.

Souverän by Design
Betrieb, Daten und Kontrolle unter deutscher bzw. europäischer Hoheit.

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 / 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

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 – genau daran arbeiten wir.

Beide Schritte zahlen auf dasselbe Ziel ein: **wirksame Verteidigung, die im Ernstfall trägt – und zunehmend 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 keine Lücken zwischen Werkzeugen 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
- SIEM as a Service
- Managed XDR
- SOAR

RESPOND

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

IMPROVE

- vCISO
- Vulnerability Management
- Security Awareness

Darauf sind wir stolz. Von **ISG** als **Rising Star** im Next-Gen SOC/MDR-Markt ausgezeichnet, bei den **CRN Channel Awards 2026** als **MSSP des Jahres** nominiert – und unsere Head of Partner Ecosystem **Xenia Sausele** steht auf der Finalisten-Liste für den **MSSP Channel Partner des Jahres**.

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

CRN AWARDS DE 2026 · NOMINIERT
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 deutschen Mittelstand seit 1999 – also seit mehr als 25 Jahren – 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 (CSO)
+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 & V.i.S.d.P.: Argos Security GmbH, München & Freiburg · argos.security · kontakt@argos.security. Redaktion & Threat Intelligence: Argos Security. ARGOS RADAR ist ein kostenfreier, vierteljährlicher Informationsdienst für Kunden und Interessenten und stellt **keine Rechts- oder Anlageberatung** dar. Alle Angaben nach bestem Wissen, Stand Juli 2026, ohne Gewähr; Threat-Daten teils selbstberichtet. Wir verarbeiten Ihre Kontaktdaten zur Direktansprache bestehender und potenzieller Kunden (Art. 6 Abs. 1 lit. f DSGVO / § 7 UWG); Details in unserer Datenschutzerklärung: argos.security/datenschutz. Sie möchten ARGOS RADAR nicht mehr erhalten? Eine formlose Nachricht an kontakt@argos.security genügt – ein Werbewiderspruch ist jederzeit möglich.

IN DER NÄCHSTEN AUSGABE · 02/26

- → Q2-Rückblick der Bedrohungslage
- → Branchen-Spotlight: Fertigung & Gesundheit
- → Deep-Dive: das souveräne CDC
- → Ihre Fragen an unser CDC-Team