Argos Security

Cyber attack? Run this!
We hope you never need it.

Incident Response Action Plan

Argos wacht, wenn andere noch schlafen.

Argos stammt aus der griechischen Mythologie: Der Wächter mit den hundert Augen. Selbst wenn einige ruhten, blieben andere offen. Genau dieses Prinzip steht hinter moderner Incident Response:

Aufmerksamkeit, Lagekontrolle und Reaktionsfähigkeit ohne Blindflug. Für uns ist Argos mehr als ein Bild.

Der neue Markenname Argos Security verbindet die Stärken der zwei Unternehmen **indevis** und **Data-Sec** zu einer klaren Haltung. indevis steht für Struktur, Weitblick und belastbare Sicherheitsarchitektur. Data-Sec steht für kompromisslose Reaktion, Forensik und Führung im Ernstfall. Gemeinsam entsteht eine Marke für Unternehmen, die im Cyber-Notfall keine allgemeine Hotline brauchen, sondern ein deutsches 24/7-Spezialistenteam mit operativer Tiefe.

+40 Jahre Erfahrung

+100 Security-Experten

+30 Gesicherte Fälle

+600 Treue Kunden

24/7 Cybernotfall-Hotline

+49 89 45 24 24-112

See Beyond.
Secure Beyond.

Inhalt

When things get serious,
Argos keeps watching.

We hope you never need it,
but if you do, we‘re ready.

Incident Response Action Plan

Das Notfall-Handbuch für die ersten 72 Stunden.

Ein Cyberangriff betrifft nie nur die IT. Er ist gleichzeitig Betriebsrisiko, Rechtsfall, Stresstest, Kommunikationskrise, Versicherungsfall – und eine Führungsaufgabe. Dieses Playbook zeigt Schritt für Schritt, was in den ersten 60 Minuten, 24 Stunden und 72 Stunden wirklich zählt:
klar priorisiert, verständlich erklärt und ohne Raum für Panik.

> **Als es passiert ist, hatten wir keine Zeit mehr nachzudenken. Ein Anruf und Argos hat übernommen. Ohne sie wäre das für uns ein ganz anderes Ende gewesen.**
>
> – Sebastian Altmann, CIO Riva Engeneering

> **Dank der professionellen und schnellen Hilfe können wir Vorfälle jederzeit und schnell bereinigen. Die umfassende und kompetente Beratung inklusive rechtlicher Betreuung ist unbezahlbar.**
>
> – Sascha Prütz, Vorstand WIIT AG

1. Die goldenen Regeln

- **Nicht improvisieren!**
- **Nicht vertuschen!**
- **Nicht vorschnell löschen!**

Ziel in den ersten Stunden:

- Schaden begrenzen
- Beweise sichern
- Handlungsfähigkeit erhalten
- Meldepflichten prüfen
- Rechtsbeistand früh einbinden
- IR-Team aktivieren

Wichtig: Vor externen Meldungen sollte immer ein Rechtsbeistand mit im Boot sitzen, damit Meldewege, Formulierungen, Policenbedingungen und Haftungsfragen sauber geprüft werden.

IR-Team sofort aktivieren: +49 89 45 24 24 - 112

2. Die erste Stunde zählt

Do:

- Incident-Response-Verantwortliche benennen
- Backups sofort logisch und physisch vom Netz trennen
- Internetverbindungen bei Ausbreitungsgefahr kappen
- VPN-Zugänge deaktivieren oder hart einschränken
- Betroffene Systeme isolieren, nicht herunterfahren
- Erste Fakten Dokumentieren: Zeitpunkt, Auffälligkeiten, betroffene Nutzer, Systeme, Meldungen
- Interne Eskalationskette starten
- Privilegierte Konten absichern
- Rechtsbeistand, Datenschutz, Versicherung & IR früh einbinden

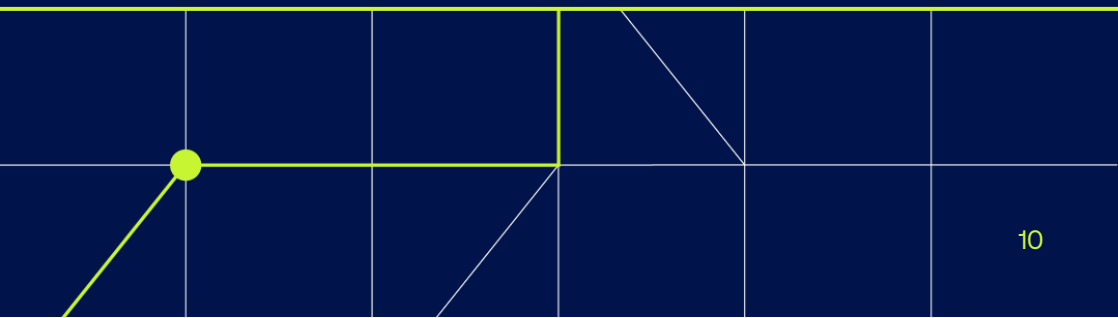
Don’t

- Keine vorschnelle Löschung von Dateien, Mails oder Logs
- Keine Kommunikation auf kompromittierten Systemen
- Keine unkoordinierten Passwort-Resets im Blindflug
- Keine externe Meldung ohne juristische Einordnung & Policenprüfung
- Keine Aussage an Kunden, Presse, Behörden ohne Lagebild
- Keine Täterkommunikation ohne Verhandler, Forensik und Rechtsbegleitung

Hundert Augen sehen,
was Hektik übersieht.

3. Erste Maßnahmen

Bereich	Sofortmaßnahme	Ziel
IT	Backups vom Netz trennen	Schutz der letzten sauberen Wiederanlaufbasis
Netzwerk	Internet/VPN kappen oder einschränken	Ausbreitung & Daten-abfluss stoppen
Management	Krisenlead benennen	Entscheidungen bündeln
Recht	Anwalt und Policenprüfung aktivieren	Fristen, Deckung und Haftung absichern
Forensik	Beweise sichern	Ursache & Umfang klären
Kommunikation	Sprachregelung festlegen	Chaos vermeiden



4. Was wir von Ihnen brauchen

- Ansprechpartner mit Mobilfunknummern und Funktion
- Liste kritischer Systeme und Standorte mit Prioritäten
- Übersicht zu Auslandsniederlassungen
- Admin-Zugänge und Notfallfreigaben
- Bestehende Backups und Backup-Status
- Sicherheitslösungen im Einsatz
- Auffällige E-Mails, Dateien, Screenshots
- Zeitpunkt der ersten Entdeckung
- Bereits ergriffene Maßnahmen
- Ansprechpartner für Datenschutz, Recht, PR und Versicherung Cyber-Police, Versicherer, Schadenhotline & Vertragsbedingungen

5. Recht in der ersten Phase

Relevante Vorschriften und Pflichten:

- **DSGVO Art. 33:** Meldung an die zuständige Aufsichtsbehörde binnen 72 Stunden bei Risiko für personenbezogene Daten
- **DSGVO Art. 34:** Benachrichtigung betroffener Personen bei hohem Risiko
- **NIS2 / nationale Umsetzung:** Zusätzliche Meldepflichten für betroffene Einrichtungen und wichtige Unternehmen
- **BSIG / BSI-Meldepflichten:** Relevant insbesondere für KRITIS, besondere Einrichtungen oder andere gesetzlich erfasste Betreiber
- **Vertragliche Pflichten:** Kunden-, Partner- und Versicherungsverträge prüfen
- **Auslandsbezug:** Sind Niederlassungen im Ausland betroffen, können zusätzliche lokale Meldepflichten gelten - auch dort müssen Behörden, Regulatoren oder Datenschutzstellen geprüft werden

Leitlinie: Erst Lagebild, dann Meldung — aber nie ohne Rechtsprüfung. Ein Rechtsbeistand sollte vor jeder externen Meldung eingebunden sein, damit Wortlaut, Fristen, Zuständigkeiten und Policenbedingungen sauber abgestimmt sind.

6. Check Meldepflicht DSGVO

5 Fragen zur Einordnung:

1. Sind personenbezogene Daten betroffen?
2. Liegt ein Risiko für Rechte und Freiheiten natürlicher Personen vor?
3. Sind Kundendaten, Mitarbeiterdaten, sensible Daten betroffen?
4. Gibt es Hinweise auf Exfiltration, unbefugten Zugriff oder Verlust?
5. Ist eine Meldung an die Datenschutzaufsicht innerhalb von 72 Stunden zu prüfen?

Wenn mehrere Fragen mit Ja beantwortet werden:

DSGVO-Meldepflicht dringend mit Rechtsbeistand und Daten- schutzbeauftragtem prüfen.

7. Check Meldepflicht NIS2

5 Fragen zur Einordnung:

1. Gehört das Unternehmen zu einem wesentlichen/wichtigen Sektor?
2. Erbringt das Unternehmen kritische oder besonders relevante digitale oder physische Dienste?
3. Hat der Vorfall erhebliche Auswirkungen auf die Dienstleistung oder Versorgung?
4. Sind mehrere Standorte, Kunden oder Länder betroffen?
5. Besteht eine Pflicht zur Meldung an die zuständige nationale Stelle nach NIS2-Umsetzung?

Wenn mehrere Fragen mit Ja beantwortet werden: NIS2-Relevanz sofort juristisch und regulatorisch prüfen.

8. Check Meldepflicht BSI / BSIG

5 Fragen zur Einordnung:

1. Ist das Unternehmen KRITIS-Betreiber oder gesetzlich besonders erfasst?
2. Ist die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit kritischer Systeme beeinträchtigt?
3. Hat der Vorfall erhebliche Auswirkungen auf den Betrieb oder die Versorgung?
4. Besteht bereits eine bekannte Meldebeziehung zum BSI?
5. Muss das BSI nach BSIG oder branchenspezifischen Vorgaben informiert werden?

Wenn mehrere Fragen mit Ja beantwortet werden: BSI-Meldung mit Rechtsbeistand und zuständigen Fachverantwortlichen prüfen.

9. Die ersten 24 Stunden

Vom Schock zur Struktur:

In den ersten 24 Stunden geht es darum, das Lagebild zu vervollständigen und die Organisation handlungsfähig zu halten.

Prioritäten

1. Angriffspfad verstehen
2. Betroffene Assets identifizieren
3. Persistenz und Seitwärtsbewegung prüfen
4. Kommunikationslinie festlegen
5. Meldepflichten und Versicherungsbedingungen bewerten
6. Auslandsbezug und lokale Pflichten prüfen


Argos schläft nie.
Gute Response auch nicht.

10. Do‘s in den ersten 24 Stunden

- Forensische Sicherung priorisieren
- Logquellen zentral sammeln
- Identitäten, Admin-Konten und Remote-Zugänge prüfen
- Backup-Integrität verifizieren
- Datenschutzbeauftragte und Rechtsberater einbinden
- Cyberversicherung frühzeitig informieren
- Auslandsniederlassungen einbeziehen
- Geschäftsführung regelmäßig mit Lageupdates versorgen

11. Dont‘s in den ersten 24 Stunden

- Kein produktiver Wiederanlauf ohne Mindestprüfung
- Keine Generalentwarnung auf Basis von Vermutungen
- Keine Ad-hoc-Kommunikation ohne Freigabeprozess
- Keine Meldung ohne Prüfung von Zuständigkeit, Frist, Formulierung
- Keine Verhandlungen ohne Strategie, Forensik und Rechtsrahmen


Nicht der Angriff entscheidet,
sondern Ihre Vorbereitung.

12. Entscheidungsboard

Frage	Warum relevant	Wer entscheidet
Sind personen-bezogene Daten betroffen?	DSGVO-Meldung	Recht + DSB
Ist der Angriff aktiv?	Eindämmung	IT + IR
Sind Backups sauber?	Recovery	IT + Forensik
Muss die Versicherung informiert werden?	Deckungsschutz	Management + Recht
Sind Auslandsein-heiten betroffen?	Lokale Melde-pflichten	Recht + lokale Ver-antwortliche
Brauchen wir externe Kommunikation?	Reputationsschutz	Management + PR

13. Die ersten 72 Stunden

Stabilisieren, melden, wiederherstellen:

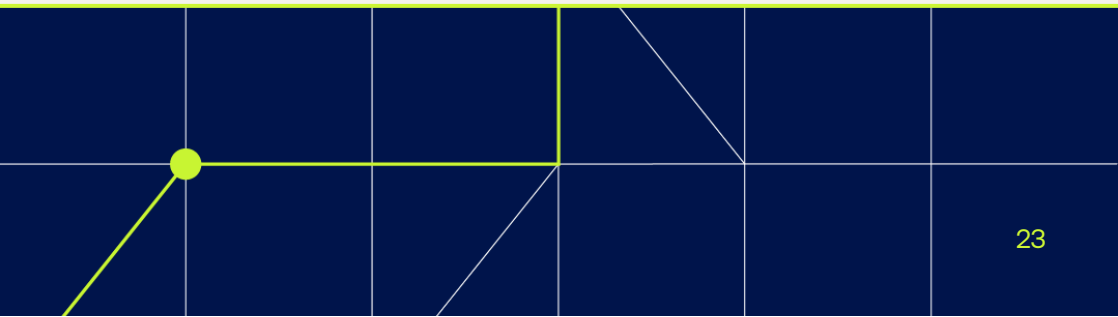
Jetzt zählt belastbare Führung. Das Ziel ist nicht Technik zu reparieren, sondern das Unternehmen kontrolliert zurück in den Betrieb zu führen.

Fokus auf

1. Vollständigeres Lagebild
2. Meldungen fristgerecht abschließen
3. Recovery priorisieren
4. Stakeholder managen
5. Lessons Learned vorbereiten

14. Maßnahmen in 72h

1. Systeme nach Kritikalität priorisiert wiederherstellen
2. Zusätzliche Sicherheitskontrollen einziehen
3. Ursachenanalyse dokumentieren
4. Betroffene Dritte identifizieren
5. Kunden- und Partnerkommunikation vorbereiten
6. Management-Briefing mit klaren Optionen erstellen
7. Internationale Meldepflichten & Dokumentationspflichten final prüfen




Nicht jeder Sturm ist vermeidbar.
Aber kein Sturm sollte Sie unvorbereitet treffen.

15. Recovery Checklist

Thema	Prüffrage	Status
Identitäten	Sind kompromittierte Konten bereinigt?	◯
Endpunkte	Sind betroffene Geräte neu aufgesetzt oder validiert?	◯
Server	Sind Logs, Images und Härtung erfolgt?	◯
Kommunikation	Sind alle Kernbotschaften freigegeben?	◯
Recht	Sind alle Fristen ein-gehalten?	◯
International	Sind lokale Meldungen geprüft/erledigt?	◯

16. Was Sie uns sofort für Recovery liefern sollten

1. Priorisierte Business-Services
2. RTO/RPO-Vorgaben
3. Liste geschäftskritischer Benutzer
4. Backup- und Restore-Verantwortliche
5. Freigaben für Abschaltung, Neuaufbau & Kommunikation
6. Übersicht externer Dienstleister
7. Liste betroffener Länder und Niederlassungen


Back to business.
Aber sicher.

17. Kommunikation im Ernstfall

Gute Kommunikation ist Teil der Incident Response:

1. **Intern:**
   knapp, faktenbasiert, handlungsorientiert

2. **Extern:**
   abgestimmt mit Recht, Datenschutz und Management

4. **Gegenüber Kunden:**
   transparent, aber nicht spekulativ

5. **Gegenüber Behörden:**
   fristgerecht, sauber dokumentiert

6. **Gegenüber Versicherern:**
   policenkonform und nachvollziehbar

18. Ransomware-Sonderfall

Bei Ransomware gelten zusätzliche Anforderungen:

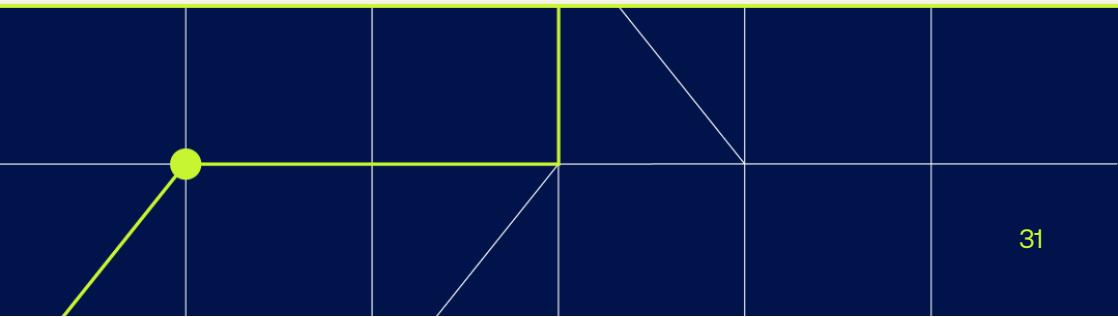
- Verschlüsselung und Exfiltration getrennt bewerten
- Verhandlungsstrategie nie isoliert treffen
- Sanktionen, Geldwäsche- und Haftungsfragen prüfen
- Forensik, Recht und Management eng verzahnen
- Backups, Offline-Kopien und Wiederanlaufpfade priorisieren


Hundert Augen, ein Fokus:
Kontrolle im Chaos.

19. Unser Einsatzmodell

Argos Security bringt:

- 24/7 deutschsprachige Spezialisten
- Incident Response
- Forensik
- Ransomware-Verhandlung
- Rechtsnahe Koordination mit externem Legal-Team
- Unterstützung bei Versicherungsfällen
- Führung bis zum Normalbetrieb



20. Incident-Response-Glossar: Angriffsmethoden und Fachbegriffe

Advanced Persistent Threat (APT):

Eine APT ist ein hochprofessioneller, zielgerichteter und meist langfristig angelegter Angriff auf ausgewählte Organisationen. Solche Akteure sind oft staatlich unterstützt oder sehr gut organisiert.

Brute Force:

Ein Brute-Force-Angriff versucht systematisch viele Passwortkombinationen, bis die richtige gefunden wird. Diese Methode ist besonders wirksam bei schwachen Passwörtern oder wenn kein Schutz wie MFA aktiv ist.

Credential Harvesting:

Credential Harvesting ist das Sammeln von Zugangsdaten über Phishing, gefälschte Login-Seiten oder manipulierte Formulare. Das Ziel ist meist der spätere Zugriff auf E-Mail-, VPN- oder Cloud-Konten.

Credential Stuffing:

Credential Stuffing nutzt zuvor gestohlene Benutzernamen-Passwort-Kombinationen aus anderen Datenleaks. Angreifer testen diese automatisiert auf vielen Diensten, weil viele Nutzer Passwörter mehrfach verwenden.

Cross-Site Scripting (XSS):

XSS ist ein Webangriff, bei dem schädlicher Code in eine Website eingeschleust wird. Wenn andere Nutzer die manipulierte Seite aufrufen, kann der Code im Browser ausgeführt werden.

DDoS:

Ein DDoS-Angriff überlastet einen Dienst oder Server mit sehr vielen Anfragen, sodass legitime Nutzer keinen Zugriff mehr haben. Im Unterschied zu anderen Angriffen steht hier nicht der Zugang zum System, sondern die Störung des Betriebs im Vordergrund.

Double Extortion:

Bei Double Extortion stehlen Angreifer vor der Verschlüsselung Daten und drohen zusätzlich mit deren Veröffentlichung. Dadurch entsteht Druck, selbst wenn Backups vorhanden sind.

Exploit:

Ein Exploit ist ein Angriff, der gezielt eine Schwachstelle in Software oder Systemen ausnutzt. Exploits werden oft verwendet, um unautorisierten Zugriff zu erhalten oder Rechte zu erweitern.

Initial Access Broker:

Ein Initial Access Broker verschafft sich Zugang zu einem Opfernetzwerk und verkauft oder vermietet diesen Zugang anschließend an andere Angreifer. Diese Rolle ist besonders wichtig im Ransomware-Ökosystem.

Malware:

Malware ist Schadsoftware, die Systeme infiziert, ausspäht, sabotiert oder verschlüsselt. Dazu zählen unter anderem Trojaner, Spyware, Würmer und Ransomware.

Man-in-the-Middle (MITM):

Bei einem MITM-Angriff schaltet sich ein Angreifer zwischen zwei Kommunikationspartner und kann Daten mitlesen, verändern oder weiterleiten. Das ist besonders kritisch in unsicheren oder schlecht abgesicherten Netzwerken.

Password Spraying:

Beim Password Spraying werden wenige häufig verwendete Passwörter gegen viele Konten getestet. Das Ziel ist, Sperrmechanismen zu umgehen und einzelne schwache Konten zu finden, ohne viele Fehlversuche pro Konto auszulösen.

Phishing:

Phishing ist eine Täuschungsmethode, bei der Angreifer gefälschte E-Mails, Nachrichten oder Websites nutzen, um Zugangsdaten, Zahlungsdaten oder andere sensible Informationen zu stehlen. Häufig ist das Ziel, Nutzer zum Anklicken eines Links oder zum Öffnen eines Anhangs zu bewegen.

Port Scanning:

Port Scanning ist das systematische Prüfen offener Netzwerkports auf einem Zielsystem. Damit erkennen Angreifer, welche Dienste erreichbar sind und wo sich Einfallstore befinden könnten.

Ransomware:

Ransomware verschlüsselt Daten oder Systeme und fordert ein Lösegeld für die Wiederherstellung. Moderne Gruppen kombinieren Verschlüsselung oft mit Datenabfluss und Erpressung über Leak-Seiten.

Sniffing:

Sniffing bezeichnet das Abfangen und Analysieren von Datenverkehr im Netzwerk. Angreifer nutzen es, um unverschlüsselte Informationen wie Zugangsdaten oder sensible Inhalte mitzulesen.

Spear-Phishing:

Spear-Phishing ist eine gezielte Form von Phishing gegen eine bestimmte Person oder Organisation. Die Nachricht ist oft personalisiert, wirkt glaubwürdig und soll den Empfänger dazu bringen, vertrauliche Daten preiszugeben oder eine schädliche Aktion auszuführen.

SQL Injection:

SQL Injection ist ein Angriff auf Datenbanken, bei dem schädliche Befehle in Eingabefelder eingeschleust werden. Dadurch können Angreifer Daten auslesen, verändern oder löschen.

Zero-Day-Exploit:

Ein Zero-Day-Exploit nutzt eine Schwachstelle aus, die dem Hersteller noch nicht bekannt ist oder für die noch kein Patch existiert. Solche Angriffe sind besonders gefährlich, weil klassische Schutzmaßnahmen oft erst später greifen.

Das Glossar bildet die terminologische Grundlage für ein konsistentes Verständnis zentraler Angriffsmethoden und Bedrohungsbegriffe im Rahmen der Incident Response. Es unterstützt die strukturierte Bearbeitung von Sicherheitsvorfällen und trägt zu einer einheitlichen Kommunikation zwischen den beteiligten Fachbereichen bei.

Die Inhalte dieses Glossars sind regelmäßig auf Aktualität, Relevanz und organisationsspezifische Anforderungen zu überprüfen. Änderungen in der Bedrohungslage, neue Angriffsformen sowie interne Erkenntnisse aus Vorfällen und Übungen sind fortlaufend zu berücksichtigen.

21. Top 10 Bedrohungsakteure im DACH-Raum

1. Akira

Einordnung:
Akira ist eine Ransomware-as-a-Service-Gruppe mit hoher Relevanz für Deutschland und die Schweiz.

Vorgehen:
Die Gruppe nutzt häufig kompromittierte Zugangsdaten, unsichere Remote-Zugänge oder Schwachstellen in VPN- und Edge-Systemen. Nach dem Erstzugang folgen laterale Bewegung, Datendiebstahl und anschließend Verschlüsselung der Systeme.

Methoden:
Typisch sind Double Extortion, Shadow-Copy-Löschung, Eingriffe in Sicherheitswerkzeuge und Angriffe auf Backup- und Wiederherstellungswege.

Verschlüsselung:
Akira verschlüsselt Systeme und Dateien aktiv und kombiniert dies mit Datendiebstahl im Sinne der doppelten Erpressung. Die Gruppe exfiltriert sensible Daten vor der Verschlüsselung und droht anschließend mit Veröffentlichung, falls nicht gezahlt wird.

DACH-Relevanz:
Ein Vorfall in Deutschland hatte 2023 Auswirkungen auf mehr als 70 Kommunen. Das zeigt die hohe Relevanz für öffentliche Einrichtungen, kommunale IT-Dienstleister und Lieferketten.

2. LockBit

Einordnung:
LockBit ist eines der bekanntesten Ransomware-as-a-Service-Ökosysteme der letzten Jahre und bleibt trotz Takedowns relevant.

Vorgehen:
Der Erstzugang erfolgt typischerweise über gestohlene Zugangsdaten, kompromittierte VPN-Zugänge oder schlecht abgesicherte Remote-Dienste. Danach folgen Privilegieneskalation, laterale Bewegung, Exfiltration und Verschlüsselung.

Methoden:
LockBit arbeitet mit einem starken Affiliate-Modell, Leak-Sites und hohem Erpressungsdruck. Die Gruppe ist für schnelle Skalierung und viele parallele Angriffe bekannt.

Verschlüsselung:
LockBit ist eine klassische Ransomware-as-a-Service-Gruppe mit aktivem Verschlüsselungsanteil. Zusätzlich nutzt die Gruppe Datenexfiltration und Leak-Drohungen, also ebenfalls ein Double-Extortion-Modell.

DACH-Relevanz:
In Deutschland war LockBit mehrfach eine der sichtbarsten und schädlichsten Gruppen.
Auch nach Strafverfolgungsmaßnahmen blieb die Bedrohung durch Affiliates und Rebrandings bestehen.

3. Black Basta

Einordnung:
Black Basta ist eine professionelle Ransomware-Gruppe mit Fokus auf Unternehmensumgebungen.

Vorgehen:
Die Gruppe beschafft Zugang über kompromittierte Anmeldedaten, Phishing oder vorgeschaltete Initial-Access-Akteure. Anschließend nutzt sie administrative Werkzeuge und Netzwerkzugriffe für die laterale Bewegung.

Methoden:
Typisch sind Datenexfiltration, Verschlüsselung produktiver Systeme und Angriffe auf zentrale Identitäts- und Dateisysteme.

Verschlüsselung:
Black Basta verschlüsselt produktive Systeme und kombiniert dies mit vorheriger Exfiltration sensibler Daten. Das Ziel ist maximaler operativer Druck durch Ausfallzeit und Veröffentlichungsdrohung.

DACH-Relevanz:
Black Basta ist im DACH-Raum relevant, weil die Gruppe gut zu mittelgroßen und großen Unternehmensumgebungen passt und dort erhebliche Betriebsunterbrechungen auslösen kann.

4. RansomHub

Einordnung:
RansomHub ist eine schnell gewachsene Ransomware-as-a-Service-Gruppe mit hoher Aktivität seit 2024.

Vorgehen:
Die Gruppe nutzt ein flexibles Affiliate-Modell. Nach dem Erstzugang folgen laterale Bewegung, Datendiebstahl und Erpressung über Leak-Drohungen oder Verschlüsselung.

Methoden:
Typisch sind Double Extortion, Partnerstrukturen und eine schnelle Anpassung an Verschiebungen im RaaS-Markt.

Verschlüsselung:
Ja, typischerweise mit zusätzlicher Exfiltration.
RansomHub folgt dem heute üblichen RaaS-Muster aus Datendiebstahl, Verschlüsselung und Leak-Erpressung. Die Gruppe ist damit klar dem Double-Extortion-Modell zuzuordnen.

DACH-Relevanz:
Für DACH-Organisationen ist RansomHub vor allem wegen seiner hohen Aktivität und der breiten Partnerstruktur wichtig. Dadurch steigt die Wahrscheinlichkeit, dass verschiedene Zugangspfade parallel genutzt werden.

5. Play

Einordnung:
Play ist eine beständig aktive Ransomware-Gruppe mit Fokus auf Unternehmensziele in Europa.

Vorgehen:
Das Muster ist meist geradlinig: Zugriff auf das Netzwerk, Sammlung und Exfiltration von Daten, Verschlüsselung und danach Erpressung über Leak-Infrastruktur.

Methoden:
Typisch sind Doppel-Erpressung, gezielte Unternehmensangriffe und operative Zurückhaltung vor der finalen Schadensphase.

Verschlüsselung:
Play verschlüsselt betroffene Systeme und nutzt zusätzlich die Veröffentlichung oder Androhung geleakter Daten als Druckmittel. Die Gruppe gehört damit ebenfalls zu den klassischen Double-Extortion-Akteuren.

DACH-Relevanz:
Play ist im DACH-Kontext relevant, weil die Gruppe in europäischen Auswertungen kontinuierlich auftaucht und typische Enterprise-Ziele adressiert.

6. Qilin

Einordnung:
Qilin ist eine Ransomware-as-a-Service-Gruppe, die 2025 stark auffiel.

Vorgehen:
Die Gruppe arbeitet mit Partnern und folgt einem standardisierten Ablauf aus Zugangsbeschaffung, interner Ausbreitung, Datendiebstahl, Verschlüsselung und Veröffentlichung bei Nichtzahlung.

Methoden:
Typisch sind Leak-Sites, Double Extortion und die wiederholbare Nutzung etablierter RaaS-Taktiken.

Verschlüsselung:
Qilin setzt auf Verschlüsselung plus Datendiebstahl und nutzt Leak-Sites zur zusätzlichen Erpressung. Das Vorgehen entspricht dem etablierten Muster moderner Ransomware-as-a-Service-Gruppen.

DACH-Relevanz:
Qilin ist für DACH-Unternehmen relevant, weil die Gruppe keine exotischen Spezialtechniken braucht, sondern mit professioneller Umsetzung bekannter TTPs erheblichen Schaden verursachen kann.

7. 8Base

Einordnung:
8Base ist eine Erpressungsgruppe mit Schwerpunkt auf Datendiebstahl und Leak-basiertem Druck.

Vorgehen:
Die Gruppe nutzt kompromittierte Zugänge oder verwundbare Systeme, um Daten zu extrahieren und anschließend Zahlungen zu erzwingen.

Methoden:
Im Vordergrund stehen Exfiltration, Veröffentlichungsszenarien und Reputationsdruck auf betroffene Organisationen.

Verschlüsselung:
8Base wird teils als Daten-Erpressungsoperation beschrieben, nutzt aber nachweislich auch Verschlüsselung von Dateien und kombiniert diese mit Exfiltration. In der Praxis ist die Gruppe daher als Double-Extortion-Akteur einzuordnen.

DACH-Relevanz:
8Base ist im DACH-Raum besonders dort problematisch, wo sensible Geschäfts- oder Personendaten betroffen sind. Schon ohne große Verschlüsselung können erhebliche Folgeschäden entstehen.

8. INC Ransom

Einordnung:
INC Ransom ist eine professionelle Erpressungsgruppe, die in aktuellen Auswertungen als aktiver Akteur erscheint.

Vorgehen:
Die Gruppe kombiniert Datendiebstahl mit Verschlüsselung und setzt Opfer anschließend über Leak-Infrastrukturen unter Druck.

Methoden:
Typisch sind Double Extortion, zielgerichtete Angriffe auf Unternehmensumgebungen und ein professionelles Auftreten gegenüber Opfern.

Verschlüsselung:
INC Ransom kombiniert Datendiebstahl und Verschlüsselung und setzt Opfer anschließend über Leak-Infrastrukturen unter Druck. Die Gruppe entspricht damit dem üblichen Double-Extortion-Modell.

DACH-Relevanz:
INC Ransom zeigt, dass auch weniger bekannte Namen erhebliche Schäden verursachen können. Für Playbooks ist die Gruppe ein gutes Beispiel für mittelgroße, aber schlagkräftige Akteure.

9. ALPHV / BlackCat

Einordnung:
ALPHV, auch BlackCat genannt, war eines der prägendsten Ransomware-as-a-Service-Ökosysteme der letzten Jahre.

Vorgehen:
Die Gruppe nutzte kompromittierte Accounts oder vorgeschaltete Initial-Access-Ketten, breitete sich in Active-Directory-Umgebungen aus, exfiltrierte Daten und verschlüsselte produktive Systeme.

Methoden:
Typisch waren Partnerprogramme, mehrstufige Erpressung, Behinderung von Wiederherstellungsoptionen und Angriffe auf Windows- und Linux-Systeme.

Verschlüsselung:
ALPHV/BlackCat verschlüsselt aktiv Dateien und Systeme und setzt gleichzeitig auf Datendiebstahl und Leak-Erpressung. Die Gruppe ist als Ransomware-as-a-Service organisiert und kann Windows-, Linux- und VMware-Umgebungen angreifen.

DACH-Relevanz:
Für Deutschland ist ALPHV/BlackCat besonders relevant, weil Ermittlungsbehörden den verursachten Schaden auf rund 455 Millionen Euro bezifferten. Die Gruppe eignet sich daher als Referenzfall für besonders schädliche moderne RaaS-Kampagnen.

10. Cl0p / TA505

Einordnung:
Cl0p ist ein datengetriebener Erpressungsakteur mit Fokus auf Massenkompromittierung über File-Transfer-, SaaS- und Supply-Chain-Schwachstellen. Besonders kritisch: Ein einzelner Exploit kann viele Organisationen gleichzeitig treffen.

Vorgehen:
Die Gruppe nutzt vor allem Schwachstellen in Managed-File-Transfer-Systemen und anderen zentralen Plattformen. Beim MOVEit-Fall wurden Daten über eine SQL-Injection-Schwachstelle aus Progress MOVEit Transfer gestohlen.

Methoden:
Mass Exploitation, Datendiebstahl, Leak-Drohungen und Erpressung über regulatorischen, geschäftlichen und reputativen Druck.

Verschlüsselung:
Verschlüsselung steht nicht immer im Mittelpunkt. Häufig liegt der Fokus auf Datenabfluss und Veröffentlichung sensibler Informationen über Leaks.

DACH-Relevanz:
Hoch für Unternehmen mit MFT-, Dateiübertragungs-, B2B-Integrations- und SaaS-Abhängigkeiten. Besonders relevant für Lieferketten, Versicherungen, Industrie, Beratung, öffentliche Hand und kritische Dienstleister.

We hope you never need it.
But if you do, call the team that keeps watching.

+49 (0) 89 45 24 24-112
kontakt@argos.security