ARGOS RADAR · ISSUE 02/26

RADAR

The threat briefing from Argos Security – a hundred eyes on the threats that concern your organisation.

→ Who is attacking hardest right now

→ First actions for every group

→ The Modern Cyber Defense Approach

→ Regulation, liability & the RIVA case study

EDITORIAL · FRANK PÜTZ, CEO

Attacks are now routine. Preparation decides the outcome.

Welcome to the English edition of ARGOS RADAR. Four times a year this report tells you what is really happening in the threat landscape – and what it means for your decisions. No panic, no jargon, just plain language.

The sober truth first: cyberattacks now hit organisations of every size. Qilin, The Gentlemen, LockBit, Akira and their peers work in a division of labour, highly professionally and around the clock – and German-speaking mid-sized companies are explicitly on their target list. This quarter we see not only more attacks, but new groups that rise within weeks where it used to take years.

The good news: you can prepare for this – if you stop merely reacting. A SOC on its own is no longer enough. What it takes today is a **Modern Cyber Defense Approach**: security not as a collection of individual tools, but as a continuously staffed, practised and intelligence-led **Cyber Defense Center**. Our **Roadmap to Resilience** is how you get there – aimed at detecting and containing attacks early instead of only chasing them.

That this works is shown in this issue by the **RIVA Engineering** case study: from total outage on 15 December back to normal operations on 7 January. And we look ahead: we are developing our CDC towards **greater digital sovereignty** (expected from Q1/2027) and, together with STACKIT / Schwarz Digits, the **IR container** – a mobile emergency data centre for the worst case.

Take twenty minutes. Pass this report on – to your management, your IT, your data protection officer. And if you have a question afterwards: we are here. Around the clock.

Frank Pütz

Chief Executive Officer, Argos Security

Frank Pütz, CEO Argos Security

~€202 bn

of the estimated €289.2 bn annual loss to German companies from theft, espionage and sabotage, this share is attributable to cyberattacks (Bitkom, 2025)

SMEs

are among the targets most heavily affected by ransomware, according to the BSI situation report 2025

24/7/365

staffed: the Argos Cyber Defense Center – carried by more than 100 specialists in the company

What to take into your next management meeting

Three questions for your IT leadership

- Is every remote access path behind multi-factor authentication – VPN and service desk included?
- When did we last rehearse an incident, and are our backups restorable?
- Which of the vulnerabilities named in this issue are still unpatched in our estate?

Three decisions for the board

- Name who is accountable for cyber risk, in writing – that assigns the task, not the board's own duty.
- Decide the incident-response readiness you want – and fund it.
- Set a date for the next tabletop exercise.

For orientation only – see page 21.

THE THREAT PICTURE · AS OF 3 AUGUST 2026

The threat is closing in – and the mid-market is in the crosshairs.

Ransomware remains the dominant threat. What is new is the pace: groups rise within weeks, professionalise their tooling and exploit weaknesses before many organisations have even patched. In the last 90 days we counted **183 listed victims across Germany, Austria and Switzerland** – and the leaderboard has been reshuffled since our German edition.

Sectors most affected in DACH

LISTED VICTIMS IN GERMANY, AUSTRIA AND SWITZERLAND · ROLLING 90 DAYS TO 3 AUGUST 2026

Count of victims published on leak sites (source: ransomware.live). Leak-site entries are largely self-reported by the attackers and are not consistently verified independently; they show reported cases, not total incidence.

What is driving this

Speed. Often only days pass between a vulnerability becoming public and its first exploitation – the patch window is shrinking.

Division of labour. RaaS platforms rent out attack tooling; access brokers supply the entry point. Cybercrime is an industry.

Data theft first. More and more groups skip encryption entirely and extort using stolen data alone.

DACH in focus. German-speaking countries rank among the top target regions for several of the most active groups.

Stolen firewall credentials. A large-scale credential-harvesting campaign against FortiGate firewalls came to light in June 2026 and is attributed by researchers to INC Ransom and Lynx. If you run FortiGate: rotate administrative and VPN credentials and terminate active sessions, even if the device is patched.

The Gentlemen
most active group worldwide over the last 90 days (317 listed victims)

183 victims
listed across DACH in 90 days – 142 of them in Germany

27 per cent
of DACH victims come from manufacturing and industry – the largest single block

The core question for every organisation is no longer “are we a target?” – it is “how fast do we detect and stop an attack that is already under way?”

TOP THREATS · THE RADAR, 3 AUGUST 2026

The ten groups you should know now.

Our radar prioritises by activity and DACH relevance – not by notoriety. Eight of these groups are profiled in detail on the following pages, each with the concrete first actions that matter.

#	GROUP	STATUS	DACH 90 D	PRIMARY TARGETS (DACH)	WHY IT MATTERS NOW
01	The Gentlemen	ACTIVE	26	Manufacturing, technology, services	317 victims in 90 days – now the most active group we track; Germany top-4 target country
02	Qilin / Agenda	ACTIVE	20	Healthcare, manufacturing, public sector	313 victims in 90 days; 2,098 cumulative in 101 countries; MSP attacks with chain effects
03	SafePay	ACTIVE	37	Industry, IT service providers, MSPs	Germany is its second-largest target country worldwide; 125 German victims in total
04	DragonForce	ACTIVE	9	Retail, services, critical infrastructure	126 victims in 90 days; “cartel” model, aggressive expansion
05	Deadlock	NEW	6	Manufacturing, services, technology	95 victims in 90 days from a standing start – its leak site opened in June 2026; profile on page 14
06	INC Ransom	ACTIVE	4	Healthcare, education, government	92 victims in 90 days; established extortionist with long dwell times
07	Akira	ACTIVE	4	Finance, manufacturing, education	82 victims in 90 days; VPN appliances without MFA as the front door
08	LockBit 5.0	ACTIVE	10	Manufacturing, healthcare, finance	54 victims in 90 days; back in business after Operation Cronos
09	Play	ACTIVE	3	Manufacturing, construction, public sector	37 victims in 90 days; intermittent encryption, recurring campaigns
10	Cl0p	IN BURSTS	0	Finance, software supply chains	Campaign-driven: long quiet phases, then mass exploitation of a single vulnerability

Sources: Argos Threat Intelligence, public leak-site analysis (including ransomware.live), CISA, Europol. Figures as of 3 August 2026; 90-day window 5 May to 3 August 2026.
Note: victim counts rest largely on self-reported leak-site entries and are not consistently verified independently. The ranking weighs activity, DACH relevance and novelty – it is not a pure victim-count table. The full, weekly-updated lexicon with more than 70 profiles: argos.security/wissen/threat-actor-hub

Plain-language glossary: **RaaS** = rented ransomware kit · **Double extortion** = encrypt plus steal data · **MFA** = multi-factor authentication · **RDP/VPN** = remote access · **EDR** = endpoint detection

Both ends of this table matter. Cl0p listed a single victim worldwide in 90 days and still belongs here, because it strikes in waves. Deadlock did not exist last quarter and entered at number five. Anyone who follows only the headlines is defending against yesterday’s groups.

GROUP IN PROFILE · 1 / 8

Qilin

ACTIVE

also known as: Agenda, Qilin v2

2,098 victims listed on leak sites across 101 countries since October 2022 – 313 of them in the last 90 days alone; 112 in Germany, Austria and Switzerland

Qilin was the most active ransomware group in the world for three consecutive quarters and remains at the very top today. The self-developed RaaS platform (originally Go, now predominantly Rust plus C/Go for Linux ELF variants) is characterised by a consistent focus on VMware ESXi infrastructure, systematic theft of browser-stored VPN credentials and aggressive double extortion.

FOR DECISION-MAKERS · IN ONE SENTENCE

One of the two most active groups worldwide – it hits hospitals, industry and local government. The most important protection: secure remote access and keep systems patched.

Fact sheet

Status	Active
Model	RaaS (ransomware-as-a-service)
Origin	Russian-speaking sphere (suspected); attribution not conclusive
Active since	2022 (as “Agenda”), publicly as “Qilin” since 2023
Victims listed	2,098 in 101 countries
DACH victims	112 (DE 76 / AT 18 / CH 18)

Primary target sectors

Healthcare · Manufacturing / automotive suppliers · Business services · Education · Critical infrastructure / municipalities

How they operate

Modus operandi: double extortion – encryption of Windows and Linux/ESXi systems combined with data theft and the threat of publication on their own leak site

Initial access: most frequently through valid credentials that were bought or phished, and through RDP; also exploitation of internet-facing applications (including FortiGate, SAP NetWeaver and Citrix vulnerabilities; CVE attributions not conclusively confirmed) and compromised remote monitoring and management tools (ScreenConnect, AnyDesk). Increasingly also via managed service providers, with chain effects.

DACH relevance: Qilin openly names DACH among its target regions and, there as globally, prefers manufacturing, healthcare and financial services – sectors with high density and low tolerance for downtime in the German-speaking market.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Immediately check patch levels on exposed RDP and VPN access (FortiGate and Citrix in particular) and enforce MFA for all remote access
+ Audit remote access and support tooling (ScreenConnect, AnyDesk, TeamViewer) for authorised installations and isolate unknown instances
+ Reset credentials stored in browsers company-wide, especially VPN logins – harvesting stored browser credentials is reported for Qilin
+ Secure ESXi and virtualisation infrastructure separately (network segmentation, MFA for hypervisor management), because Qilin goes after VMware ESXi by design

Avoid at all costs

– Paying a ransom or negotiating directly with the attackers without prior forensic preservation and contact with the authorities (BSI / state criminal police)
– Rebuilding affected systems prematurely, before persistence mechanisms (GPO scripts, scheduled tasks, registry run keys) have been fully identified and removed

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 2 / 8

The Gentlemen

ACTIVE

also known as: operator handles zeta88, hastalamuerte

696 listed victims in 82 countries since September 2025 – 317 of them in the last 90 days, making it currently the most active group we track; 42 in DACH

The Gentlemen appeared in mid-2025 and has grown faster than any other ransomware-as-a-service operation we follow. Germany is its fourth-largest target country. The United States is still its single biggest market at around 18 per cent of listed victims – but that is far below the share most comparable groups show, which is what makes this actor unusually relevant to European readers. Technically it stands out for self-propagating, cross-platform encryption and purpose-built EDR killers.

FOR DECISION-MAKERS · IN ONE SENTENCE

The fastest-growing group of this quarter – and one that deliberately targets Europe. The most important protection: patch edge and VPN devices, and protect your EDR against tampering.

Fact sheet

Status	Active
Model	RaaS, affiliate-friendly (approx. 90/10 split)
Origin	Russian-speaking operators (country not confirmed)
Active since	mid-2025 (first leak-site victims September 2025)
Victims listed	696 in 82 countries
DACH victims	42 (DE 32 / AT 6 / CH 4)

Primary target sectors

Manufacturing · IT and business services · Technology · Healthcare · Construction · Finance

How they operate

Modus operandi: double extortion with self-propagating, cross-platform encryption (Windows, Linux, ESXi, NAS, BSD); ransom demands are negotiated – one documented case moved from roughly USD 250,000 to 190,000

Initial access: exploitation of Fortinet and Cisco edge and VPN devices is the main vector (including the FortiOS authentication bypass CVE-2024-55591), supplemented by purchased access from initial-access brokers and infostealer logs. Inside the network the group spreads worm-like via group policy and disables protection using a dedicated EDR killer and vulnerable drivers.

DACH relevance: Germany ranks among the top target countries, with Austrian and Swiss victims documented as well. For a European mid-market reader this is the group whose profile deviates most sharply from the usual US focus.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Patch Fortinet and Cisco edge and VPN devices without delay and check them for known authentication-bypass vulnerabilities – this is the main vector
+ Switch on tamper protection for your EDR and alert on any attempt to disable it
+ Monitor group-policy changes and alert on unauthorised modifications, because the group spreads itself through GPO
+ Keep backups offline or immutable and segment ESXi, NAS and BSD systems – the encryptor covers all of them

Avoid at all costs

– Leaving edge and VPN appliances unpatched or running EDR without tamper protection
– Rebuilding systems before forensics are secured – the self-propagation route has to be identified, otherwise the encryption returns

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 3 / 8

SafePay

ACTIVE

also known as: SafePay Ransomware

537 listed victims in 45 countries since November 2024 – 125 of them in Germany. No other group in this report is so strongly concentrated on the German market

SafePay emerged at the end of 2024 and climbed into the top tier of ransomware actors during 2025. It is not a classic RaaS: a single collective centrally controls intrusion, encryption, negotiation and leak. The code base builds on the leaked LockBit 3.0 source. What makes SafePay relevant for this report is its target geography – Germany is its second-largest target country after the United States, and in the last 90 days it listed more DACH victims than any other group.

FOR DECISION-MAKERS · IN ONE SENTENCE

The group with the strongest German focus of all. It comes in through remote access and VPN misconfiguration. The most important protection: no unprotected RDP, MFA everywhere, and watch out for fake IT support calls.

Fact sheet

Status	Active
Model	private collective, centrally controlled (not a conventional RaaS)
Origin	Eastern Europe (suspected); uses the LockBit 3.0 code base
Active since	2024
Victims listed	537 in 45 countries
DACH victims	130 (DE 125 / AT 2 / CH 3)

Primary target sectors

Industry / manufacturing · IT service providers · Managed service providers · Mid-sized companies · Retail

How they operate

Modus operandi: double extortion – data theft followed by intermittent encryption; a single group runs the whole chain from intrusion to negotiation, and targets managed service providers deliberately

Initial access: stolen or purchased credentials (access brokers, infostealer logs), RDP brute force and misconfigured SSL VPN gateways that allow MFA to be bypassed. A second, well-documented route is social engineering: attackers impersonate internal IT support over Microsoft Teams and abuse remote tools such as ScreenConnect and Quick Assist to get in.

DACH relevance: Germany is the second most affected country after the United States and accounts for roughly a quarter of all SafePay victims. Several DACH industrial companies have been listed. If you read only one profile in this report, read this one.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Never expose RDP unprotected to the internet and enforce MFA on every remote path, including the VPN gateway
+ Give your service desk a mandatory identity check before any password reset – impersonation over Teams is a documented SafePay route
+ Inventory remote-support tooling (ScreenConnect, Quick Assist) and block unauthorised instances
+ Keep backups offline or immutable and monitor for unusual logins and living-off-the-land tool use

Avoid at all costs

– Accepting unsolicited “IT support” calls or chat requests without verifying the caller through a known internal channel
– Paying without forensic assessment and sanctions-list screening – there is no known decryptor, and payment does not reliably prevent publication

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 4 / 8

LockBit 5.0

ACTIVE

also known as: LockBit 2.0, LockBit 3.0 (Black), LockBit 4.0, LockBit 5.0

329 listed victims in 68 countries recorded under the 5.0 generation – 54 of them in the last 90 days. The generation launched in September 2025; leak-site tracking under the current identifier begins in December 2025, so the true figure is higher

LockBit is one of the longest-lived and most productive RaaS groups. Despite the partial takedown of its infrastructure by Operation Cronos in February 2024, the group was back online within days and released its fifth malware generation in September 2025. It is no longer the leader by volume – but it is still very much in business.

FOR DECISION-MAKERS · IN ONE SENTENCE

The repeat offender – broken up and back. Protection: multi-factor login on remote access, patch the perimeter, secure your logs against deletion.

Fact sheet

Status	Active
Model	RaaS, in-house development since 2019
Origin	Russia / Eastern Europe (suspected); the NCA and its partners name Dmitry Khoroshev, alias "LockBitSupp", as the alleged leader – presumption of innocence applies
Active since	2019
Victims listed	329 in 68 countries (5.0 generation)
DACH victims	29 (DE 20 / AT 7 / CH 2)

Primary target sectors

Manufacturing · Healthcare · Financial services · Government / administration · Legal and education

How they operate

Modus operandi: double extortion – full encryption plus data theft, published on a leak site with a countdown to increase pressure

Initial access: phishing with faked password-reset mails, abuse of exposed RDP (brute force or credentials from infostealer logs), and exploitation of internet-facing applications – among them Fortinet FortiOS/FortiProxy, Atlassian Confluence and Log4Shell. Valid accounts bought on criminal marketplaces are used as well.

DACH relevance: Alongside the United States, DACH is among the most heavily affected regions. The core target sectors – manufacturing, healthcare and financial services – mirror the backbone industries of the German-speaking mid-market and public administration.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Inventory exposed RDP and VPN access immediately, question whether it is needed at all and enforce MFA
+ Patch internet-facing systems without delay, above all Fortinet FortiOS/FortiProxy and Atlassian Confluence, and check them against known CVEs
+ Compare your credentials against infostealer logs and reset affected accounts
+ Enable EDR/AV tamper protection and ship Windows event logs to immutable storage – LockBit actively clears logs

Avoid at all costs

– Leaving RDP or VPN reachable from the internet without MFA
– Relying on signature-based detection alone – heavily obfuscated, frequently changing variants have been reported since 2025 that can slip past purely signature-based tooling

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

TAKING STOCK · HALFWAY THROUGH

Eight groups, five patterns.

However differently Qilin, SafePay, The Gentlemen and the rest present themselves – in their methods they resemble one another strikingly. Knowing these five patterns lets you defend in a targeted way instead of broadly.

1

Abuse of legitimate access

RDP, VPN and remote monitoring tools are the most common way in – almost every group uses stolen or weakly protected credentials.

2

Data theft first

More and more groups no longer encrypt at all and extort using stolen data alone.

3

Speed

New vulnerabilities are exploited within days – the patch window is shrinking rapidly.

4

Backups and virtualisation in the crosshairs

Shadow copies, backups and ESXi hosts are sabotaged deliberately to prevent recovery.

5

DACH in focus

German-speaking targets are explicitly on the list for many groups – SafePay and The Gentlemen most of all.

The good news: the same foundation helps against all five – MFA on every access path, patch discipline, 24/7 detection and a rehearsed emergency response. That is exactly what a Cyber Defense Center bundles.

GROUP IN PROFILE · 5 / 8

Akira

ACTIVE

also known as: Akira Ransomware

1,558 listed victims in 71 countries since April 2023 – 82 of them in the last 90 days; 101 in DACH, with Switzerland unusually strongly represented

Akira has been active since 2023 and remains one of the most productive ransomware groups worldwide, with no arrests or takedowns to date. It develops steadily across several platforms (Windows, Linux/ESXi and, since 2025, Nutanix AHV).

FOR DECISION-MAKERS · IN ONE SENTENCE

Almost always gets in through a VPN appliance. Protection: patch it, enforce MFA – and rotate the local accounts and one-time-password seeds afterwards, or the door stays open.

Fact sheet

Status	Active
Model	RaaS (ransomware-as-a-service)
Origin	Russia / Eastern Europe (strongly suspected); possible link to former Conti operators
Active since	2023
Victims listed	1,558 in 71 countries
DACH victims	101 (DE 69 / AT 7 / CH 25)

Primary target sectors

Finance · Manufacturing · Healthcare · Education · Critical infrastructure

How they operate

Modus operandi: double extortion – data theft combined with encryption and the threat of publication on the leak site if no payment is made

Initial access: primarily the exploitation of internet-facing VPN appliances without multi-factor authentication, in particular Cisco ASA/VPN vulnerabilities (CVE-2020-3259, CVE-2023-20269) and SonicWall SonicOS SSL VPN (CVE-2024-40766, the main vector since 2025), plus Veeam backup vulnerabilities (CVE-2024-40711, CVE-2023-27532). The group also uses spear phishing for credential theft, RDP abuse with stolen credentials and password spraying.

DACH relevance: Akira targets DACH alongside the United States. With 25 Swiss victims it is, in relative terms, the group with the strongest Swiss footprint in this report; a Swiss manufacturing case from 2025 is publicly documented.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Patch all internet-facing VPN appliances (Cisco ASA, SonicWall SonicOS) against the CVEs listed above without delay – and enforce MFA on every VPN and remote path
+ After patching, rotate the local appliance accounts and re-issue the one-time-password seeds – attackers have passed active MFA challenges using credentials carried over from the old configuration
+ Patch Veeam Backup & Replication (CVE-2024-40711, CVE-2023-27532) and stop exposing RDP externally – Akira uses backups as a stepping stone and deletes shadow copies
+ Watch for suspicious remote tools and discovery activity (Advanced IP Scanner, BloodHound, AdFind) – typical precursors of an Akira attack

Avoid at all costs

– Paying without forensic assessment and legal advice – payment does not reliably prevent publication
– Rebuilding systems or deleting volume shadow copies and logs before evidence is secured
– Relying on Windows endpoint protection alone – Akira encrypts ESXi, Hyper-V and Nutanix AHV environments, often without Windows systems being affected at all

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 6 / 8

DragonForce

ACTIVE

also known as: DragonForce Ransomware

632 listed victims in 64 countries since December 2023 – 126 of them in the last 90 days, putting the group third by current activity; 40 in DACH

DragonForce is reported to have emerged in 2023 from the pro-Palestinian hacktivist scene in Malaysia; that lineage is disputed, and some researchers treat the ransomware operation as a separate group of the same name. Either way it now runs as a commercial RaaS platform. The group uses leaked LockBit 3.0 and Conti code and supplies its encryptor to third-party affiliates, as the attacks on British retail chains in 2025 demonstrated.

FOR DECISION-MAKERS · IN ONE SENTENCE

An aggressively expanding “cartel” actor. Protection: harden access paths and detect suspicious activity early.

Fact sheet

Status	Active
Model	RaaS since 2024; encryptor also rented to third-party groups
Origin	Malaysia reported, lineage disputed (hacktivist origin, commercialised since 2024)
Active since	2023
Victims listed	632 in 64 countries
DACH victims	40 (DE 32 / AT 1 / CH 7)

Primary target sectors

Retail · Critical infrastructure · Government · Manufacturing · Business services

How they operate

Modus operandi: double extortion (encryption plus data leak), at times with additional DDoS pressure; the encryptor is also rented to third-party groups

Initial access: several routes: social engineering, vishing and help-desk impersonation (the main vector in the UK retail attacks, which researchers attribute to the Scattered Spider affiliate using DragonForce’s encryptor), compromise of exposed RDP servers and VPN portals using stolen or guessed credentials, and exploitation of internet-facing web and application servers (including Log4Shell and Ivanti Connect Secure vulnerabilities). RMM vulnerabilities in SimpleHelp (CVE-2024-57726/57727/57728) were chained to encrypt several downstream customers through a single managed service provider.

DACH relevance: The target regions squarely include DACH alongside the UK, the US and Asia-Pacific. The SimpleHelp supply-chain compromise shows that German, Austrian and Swiss customers of IT service providers can be affected indirectly.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Inventory exposed RDP and VPN access immediately, take it off the internet or protect it with MFA
+ Harden help-desk processes against vishing and social engineering: make call-back and identity verification mandatory before every password reset
+ Patch internet-facing application and VPN servers against known vulnerabilities (Log4Shell, Ivanti Connect Secure) and bring RMM software such as SimpleHelp up to date
+ Escalate EDR/XDR alerts about driver installations and event-log deletion immediately – typical precursors of the encryption phase

Avoid at all costs

– Paying a ransom or entering negotiations without first involving law enforcement and your CERT
– Relying on perimeter protection alone while neglecting internal segmentation and MFA for administrative accounts

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 7 / 8

INC Ransom

ACTIVE

also known as: no further aliases known

883 listed victims in 71 countries since August 2023 – 92 of them in the last 90 days; healthcare and education are heavily over-represented

INC Ransom has been active since 2023 and has not been disrupted by law enforcement so far. It is characterised by unusually long dwell times between initial access and encryption, and by a pronounced focus on healthcare, education and public administration.

FOR DECISION-MAKERS · IN ONE SENTENCE

An established extortionist working through data theft. Protection: harden access, detect data leaving the building, and rehearse your incident response.

Fact sheet

Status	Active
Model	RaaS (ransomware-as-a-service)
Origin	unknown (Eastern Europe suspected)
Active since	2023
Note	the German BSI groups INC, Lynx and Sinobi as one actor
Victims listed	883 in 71 countries
DACH victims	52 (DE 39 / AT 10 / CH 3)

Primary target sectors

Healthcare · Education · Government · Pharmaceuticals · Manufacturing

How they operate

Modus operandi: double extortion – data theft plus encryption, with a strikingly long dwell time before the encryption itself

Initial access: frequently through vulnerabilities in internet-facing systems – Citrix NetScaler (CVE-2023-3519 and, more recently, CVE-2025-5777), FortiClient EMS (CVE-2023-48788) and SimpleHelp (CVE-2024-57727) – and through credentials obtained by phishing or taken from infostealer logs. Very recent CVE attributions are not conclusively confirmed.

DACH relevance: INC Ransom is an established, active double-extortion actor with victims across Europe; 52 DACH victims are listed cumulatively, with Austria comparatively strongly represented.

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Patch or isolate Citrix NetScaler ADC/Gateway, FortiClient EMS and SimpleHelp RMM installations against the known CVEs without delay
+ Identify, secure and MFA-protect exposed RDP and remote-access services, including AnyDesk and TightVNC
+ Review Active Directory and network enumeration activity (AdFind, Advanced IP Scanner, Nltest, Net.exe) and treat PsExec use under cover names such as “winupd” as an indicator
+ Monitor access to Veeam backup credentials and typical credential-dumping patterns – backup infrastructure is attacked deliberately

Avoid at all costs

– Assuming the damage stops at the encrypted systems – INC’s long dwell times mean data has usually been exfiltrated in parallel
– Initiating a ransom payment without consulting investigating authorities and legal counsel – demands vary widely and payment guarantees no deletion of the data

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

GROUP IN PROFILE · 8 / 8

Play

ACTIVE

also known as: PlayCrypt, Balloonfly

1,290 listed victims in 44 countries since November 2022 – 37 of them in the last 90 days; 51 in DACH

Play is a centrally controlled, non-affiliated ransomware group with no known links to other actors. It is characterised by its own Linux/ESXi variant, a bespoke infostealer named Grixba and an intermittent encryption strategy that evades conventional signature-based detection.

FOR DECISION-MAKERS · IN ONE SENTENCE

Encrypts quickly and in waves. Protection: keep remote and perimeter access under control and monitor around the clock.

Fact sheet

Status	Active
Model	private collective, centrally controlled (not a conventional RaaS)
Origin	unknown (Latin America suspected)
Active since	2022
Victims listed	1,290 in 44 countries
DACH victims	51 (DE 36 / AT 5 / CH 10)

Primary target sectors

Healthcare · Legal · Real estate · Manufacturing · IT

How they operate

Modus operandi: double extortion – data theft plus intermittent encryption (AES-256/RSA-4096, ChaCha20 as fallback), contact only by e-mail with no Tor negotiation portal

Initial access: primarily the exploitation of internet-facing systems: FortiOS SSL VPN vulnerabilities (CVE-2018-13379, CVE-2020-12812), Microsoft Exchange vulnerabilities (ProxyNotShell, OWASSRF) and Cisco ASA firewalls. In addition the group buys credentials from initial-access brokers and uses exposed RDP/VPN endpoints, SimpleHelp RMM vulnerabilities (CVE-2024-57726/27/28) and the Windows CLFS zero-day CVE-2025-29824 to gain system privileges.

DACH relevance: Play counts DACH among its declared target regions; 51 victims across Germany, Austria and Switzerland are listed cumulatively (attacker-supplied entries, not independently confirmed).

HOW TO PREPARE – AND WHAT TO DO IF IT HAPPENS

Do now – and at the first sign of trouble

+ Inventory exposed RDP and VPN access immediately, secure it and enforce MFA
+ Patch Microsoft Exchange (ProxyNotShell/OWASSRF), Fortinet SSL VPN (CVE-2018-13379, CVE-2020-12812), Cisco ASA and the Windows CLFS vulnerability CVE-2025-29824 without delay
+ Check that SimpleHelp and other RMM installations are up to date (CVE-2024-57726/27/28) and not being used without authorisation
+ Isolate ESXi hosts and check for unusual .vmdk/.vmx access and ransom notes in /vmfs/volumes/

Avoid at all costs

– Paying without forensic assessment and a sanctions-list screening – researchers have documented a North Korean state-linked actor working with Play, which makes payment a sanctions risk
– Replying to the e-mail address in the ransom note or negotiating on your own initiative
– Rebuilding affected systems before Grixba infostealer traces and enumeration activity have been forensically secured

Figures rest largely on self-reported leak-site entries and are not consistently verified independently. Individual CVE and tooling attributions are snapshots (as of 3 August 2026).

NEW & RISING · THE NEXT WAVE

New groups appear faster than ever.

Rebrands of broken-up groups, offshoots built on leaked code, specialists for a single vulnerability: the market re-sorts itself constantly. Four names that did not exist in our last edition – and that are already listing DACH victims.

Deadlock

NOW NO. 5

Its leak site went live in June 2026 with a backfilled victim list, and it went straight into the top five by volume: 95 listed victims in the last 90 days, six of them in DACH. Its entire history falls inside this reporting window – a reminder of how fast an unknown name becomes a real risk.

Nova

EX RALORD

A rebrand of the RALord operation with an unusually affiliate-friendly split. 74 victims in the last 90 days, with German organisations among them.

Krybit

NEW 2026

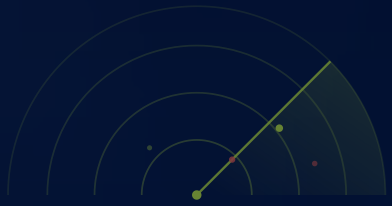
A RaaS newcomer with an explicit DACH footprint: 62 victims in 90 days, five of them in Germany, Austria and Switzerland. Grew from nothing within one quarter.

Payload & Aurora

WATCH LIST

Two smaller names with a disproportionate German share – Payload builds on the leaked Babuk code base. Together they account for eleven DACH victims in 90 days.

The trend behind the names: data theft instead of encryption. Where recovery used to be the deciding factor, what matters today is whether sensitive data left the building at all – and whether you noticed in time.



DACH SPOTLIGHT · CLOSE TO HOME

The threat is moving closer to home.

Three findings show how close the threat has come. One group concentrates on Germany more strongly than any other actor in this report. And German-speaking lone operators are abusing legitimate remote monitoring and management software.

SafePay – the German case

ACTIVE

125 of 537 SafePay victims are German – roughly a quarter of everything the group lists. In the last 90 days it named 37 DACH organisations, more than any other actor. Germany is its second-largest target country after the United States. Full profile on page 7.

What this means

+ Being mid-sized and German-speaking is no longer protection through obscurity
+ Remote access and service-desk processes are the decisive control points

German-speaking lone operators

SMALL BUT REAL

Security researchers attribute the abuse of legitimate remote monitoring and management (RMM) software – used to break into smaller companies – to individuals believed to be German-speaking. No corporate apparatus – and dangerous precisely because the tooling looks inconspicuous and the targets are poorly protected. Activity has been low since June 2026, but the pattern remains.

What this means

+ Small companies are deliberately chosen targets too
+ RMM tooling belongs in a complete inventory

The common denominator: abuse of legitimate access – RDP, VPN and remote monitoring tools. Inventory these paths completely, protect them with MFA and monitor them, and you take away the single most important tool most attackers rely on.

When the line stops

Manufacturing is the most affected sector in DACH, with 50 of 183 listed victims. Yet hardly any of the attacks in this report hit a machine directly: what gets encrypted is the virtualisation layer, the file shares and the systems that plan and schedule production. The line stops because nothing is telling it what to build.

That makes the IT-to-OT boundary the control point that matters. The RIVA case on page 18 shows what orderly fallback operations buy you.

+ Segment the production network from office IT – and test that the segmentation holds
+ List which OT systems depend on a Windows server or a hypervisor: that list is your real blast radius
+ Decide now how long you could run on paper, and who calls the switch

Victim counts on this page are leak-site entries, largely self-reported by the attackers and not consistently verified independently.

THE CORE IDEA

The question is no longer whether you are a target.
It is how quickly you detect an attack that is already under way.

That is precisely what the **Modern Cyber Defense Approach** is built for – and the **Roadmap to Resilience** is how you get there. The following pages show what that looks like in practice.

FIRST ACTIONS · THE FIRST HOUR

When it happens: six steps that limit the damage.

The first sixty minutes often decide the scale of an incident. This playbook applies to practically every group in this report – put it on the wall before you need it.

1 Stay calm, get a picture, open a clean channel

Do not shut everything down in panic. Get an overview: which systems are affected, is encryption still running, has data left the network? From now on communicate over a **clean side channel** (phone, separate device) – attackers often read along inside the network.

2 Isolate, do not delete

Disconnect affected systems from the network (pull the cable, switch off Wi-Fi), but if possible **do not shut them down and do not rebuild them** – that destroys traces. (Exception: if encryption is actively running, disconnecting fast may take priority – when in doubt, call the hotline.)

3 Evidence, backups and access

Secure logs, memory images and the ransom note. **Protect backups** (take them offline or make them immutable) and **lock or rotate privileged access immediately** – domain admin, service, VPN and backup accounts. Almost every group lives on stolen credentials.

4 Hotline and insurer

Bring specialists in early – the Argos emergency hotline is reachable around the clock: **+49 89 45 24 24-112**. Inform your cyber insurer or breach coach promptly; early notification is often a condition of the policy.

5 The clock is running

Check your reporting obligations: under the GDPR, notify the supervisory authority (Art. 33, generally within 72 hours) and, where required, the individuals affected (Art. 34). **If your organisation qualifies as an essential or important entity** under the German BSIG (NIS-2 implementation, in force since 6 December 2025), an early warning within 24 hours, a notification within 72 hours and a final report within one month also apply – whether you fall within scope depends on sector and size. For guidance only, not legal advice – have your specific case reviewed by counsel. The report remains yours to make.

6 Do not pay in haste

No payment without forensic assessment, sanctions-list screening and legal support. Payment does not reliably protect against publication.

Fill in and post up in advance: your internal escalation chain (who decides to switch to fallback operations, who informs management and the data protection officer), a second reachable phone number, your Argos customer number and where your IR plan is filed.

24/7 emergency hotline: +49 89 45 24 24-112 · argos.security/notfall – in an emergency, practised IR teams respond. Team size depends on the incident; in major incidents up to 20 specialists are deployed. Agreed response times apply to customers with an IR retainer.

CASE STUDY · A CUSTOMER IN AN EMERGENCY

RIVA Engineering: from total outage back to normal operations.

Anyone who knows the Grand Tower in Frankfurt, the Kingdom Centre in Riyadh or the Royal Clock Tower in Mecca has seen the work of RIVA Engineering – an internationally active facade construction company from the German mid-market. On 15 December 2025 everything there suddenly stood still.

How the emergency unfolded

- **15 DEC · 05:45**
  The phone rings: staff cannot log in. The entire virtual environment is encrypted.
- **WITHIN HOURS**
  The Argos incident response team brings the attack under control and secures evidence.
- **FALLBACK OPERATIONS**
  A structured fallback operation kept production running – through Christmas, the holidays and New Year, reachable throughout.
- **7 JAN 2026 · NORMAL OPERATIONS**
  Return to normal operations – with a security architecture that is stronger today than before.

> **“We didn’t have to work anything out for ourselves. They kept the facts coming – they told us what to do, and gave us something to decide on.”**

Sebastian Altmann
Head of IT, RIVA Engineering

> “It is not a question of whether you get hacked, but when. What matters is that systems, teams and service providers work together – and that you bring in expertise instead of saving on security.”
>
> Sebastian Altmann, Head of IT, RIVA Engineering

~3 weeks
from total outage back to normal operations (15 Dec – 7 Jan)

Continuous
fallback operations over Christmas and New Year – production kept running

Forensic
evidence secured – the basis for review, insurance and authorities

What this means for your organisation

Bring in expertise early instead of saving on security – in an emergency, practised teams are what count.

Structure fallback operations: an orderly fallback operation holds production while systems are restored.

Come back stronger: use the restart to harden the security architecture for good.

Out of the jointly managed crisis grew more than a supplier relationship: “Argos Security is by now more than a service provider to us.” The full case study – with timeline, approach and lessons learned – is available on request.

Individual case. The course and duration of an incident depend on the environment, the backup situation and how early specialists are involved. The figures describe this specific engagement and are not a projection for other incidents. Published with the consent of RIVA Engineering; all quotations released by the person named.

MODERN CYBER DEFENSE APPROACH · THE SOC HAS HAD ITS DAY

Stop reacting. Start defending.

Tools alone – firewall, antivirus, backup – do not add up to a defence system. The Modern Cyber Defense Approach starts from the emergency and asks not only "how do I keep attackers out?" but above all: "how quickly do I detect and stop one who is already inside?" The **Roadmap to Resilience** is how you get there.

TOOL-CENTRIC

- – Tools side by side, with no shared picture
- – Many alerts – little prioritisation
- – Detection often only once damage appears
- – Incident response rarely rehearsed; roles unclear
- – Detection not continuous around the clock

TODAY · MODERN CYBER DEFENSE (CDC)

- + One picture from all sources – 24/7 in the CDC
- + Threat intelligence steers the detection
- + Attacks detected and contained early
- + Incident response rehearsed and under retainer
- + Staffed around the clock, AI-supported

THE PATH · ROADMAP TO RESILIENCE

1	2	3	4	5
PREPARE	PROTECT	DETECT	RESPOND	IMPROVE
Prevention	Protection	Detection	Response	Improvement
Know your risks, reduce the attack surface, rehearse the emergency.	Harden access, endpoints and networks – the foundation.	See around the clock what is happening – calibrated to your threat exposure.	Contain immediately in an emergency and restore operations.	Learn from every incident, raise maturity continuously.

In short: a collection of tools becomes a system that sees, assesses and acts around the clock – step by step towards demonstrable diligence and higher maturity. That documented diligence can also reduce the liability exposure of your management.

THE ANSWER · CYBER DEFENSE CENTER

A system built to detect attacks early and contain them faster.

The Cyber Defense Center (CDC) is the core of the Modern Cyber Defense Approach: a continuously staffed defence system that joins four building blocks into one whole – AI-supported, with data residency in Germany on request, and always with experienced analysts in the loop.

24/7 detection

Round-the-clock monitoring in the CDC; alerts are assessed, not merely counted.

Incident response

Retainer with contractually agreed response times; depending on the incident, up to 20 specialists are deployed.

Threat intelligence

Knows which groups target your sector – and calibrates the detection accordingly.

IR readiness

Rehearses your response before you need it: resilience check, workshops, tabletop exercises.

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

The CDC is the active core of your **Roadmap to Resilience** – focused on detecting and responding, carried by prevention, protection and continuous improvement.

> **What that means concretely:** detection in the CDC is calibrated to exactly the groups this report describes – Qilin, SafePay, The Gentlemen and the rest – and is continuously re-sharpened with our own threat intelligence. Not an off-the-shelf toolbox, but a picture of the situation for your sector.

Detect earlier

Anomalies can surface before access turns into damage.

Stop faster

A practised response helps contain a running attack at an early stage.

Act demonstrably

Documented decisions help you show the care required of you – they neither remove the duty nor exclude liability.

since 1999
German cybersecurity specialist

1,000+
customers across DACH

ISO 27001
certified by TÜV SÜD; data residency in Germany on request

up to 20
IR specialists in an emergency

REGULATION & LIABILITY · THE DUTY

Cyber defence is now a legal duty – and a board matter.

The threat landscape is one thing – the legal duty is another. NIS-2, the GDPR and their peers demand demonstrable precaution. Failing to provide it risks fines – and in certain cases the personal accountability of the management body. These duties cannot be delegated away; a Cyber Defense Center supports you in meeting them.

FRAMEWORK	WHAT IT REQUIRES	HOW THE CDC SUPPORTS
NIS-2 / BSIG for essential and important entities	Risk management, reporting duties (24 hours / 72 hours / one month) and accountability of the management body. Fines up to €10 million or 2 % of worldwide annual turnover, whichever is higher, for essential entities, up to €7 million or 1.4 % for important entities.	24/7 detection, documented processes and **support with your timely report** – the report itself remains yours to make.
Management duties § 38 BSIG	Directors must personally approve and oversee risk-management measures and undergo training. These duties cannot be delegated; general liability of the management body under company law remains unaffected.	Provides **the threat picture and the evidence** with which management visibly meets its supervisory duty.
GDPR Art. 32, 33, 34	Appropriate technical and organisational measures, and notification of personal data breaches without undue delay (to the supervisory authority generally within 72 hours). Infringements of Art. 32–34 carry fines of up to €10 million or 2 % of total worldwide annual turnover, whichever is higher (Art. 83(4)(a)); other infringements can reach €20 million or 4 %.	Early detection of data exfiltration and robust documentation as the basis for your notification.
GmbHG § 43 / AktG § 93 German corporate law	The diligence of a prudent business person – otherwise personal internal liability for damages.	Evidences **demonstrable diligence**: continuous monitoring, rehearsed response, documented decisions.
DORA / KRITIS only for affected sectors	DORA: financial sector (EU regulation, applicable since 17 January 2025). KRITIS: operators of critical infrastructure – ICT risk management and prompt incident notification.	Covers monitoring, incident response and reporting capability as building blocks of these requirements.

Why documentation matters: under § 93(2) sentence 2 AktG (and § 43 GmbHG applied accordingly) the management body carries the burden of showing it acted with due care. Continuous monitoring, a rehearsed response and evidenced decisions make that showing easier – they neither remove the duty nor exclude liability.

up to €10 m

or 2 % of total worldwide annual turnover – the fine range for breaches of Art. 32–34 GDPR (Art. 83(4)(a)). Higher tiers apply to other infringements; management can also be personally liable to the company under § 43 GmbHG / § 93 AktG. For comparison: the average cost of recovering from a ransomware attack – excluding any ransom payment – was US$1.53 million (Sophos, State of Ransomware 2025).

Whatever service provider you use, the underlying duty stays with you: name those responsible, document risks, define reporting and escalation paths. A CDC supports the implementation – the responsibility remains with the management.

This overview is for orientation and does not replace legal advice. Argos does not provide legal services; whether and to what extent a rule applies to your organisation must be assessed by counsel in the individual case.

OUTLOOK · WHAT COMES NEXT

Two steps we are taking now.

RADAR also looks forward. Argos is already working on two developments – a mobile emergency data centre for the worst case, and more digital sovereignty for the CDC.

COMING SOON · WITH STACKIT / SCHWARZ DIGITS

The IR container

A mobile emergency data centre that accelerates the restart after full encryption – the bridge until your own data centre is running again. Built together with STACKIT / Schwarz Digits.

1 Alert & requirement

Clarify scope, fix the capacity class (S/M/L).

2 The container rolls in

Typically on site within 48 hours, with its own uplinks.

3 Minimum operations

The STACKIT environment restores minimum operations (typically 5–7 days).

4 Return

After stabilisation, a clean move back into your own environment.

Transitional solution, not a data-centre replacement. Values are **target figures for an offering in development** – guide values, not commitments. **Register interest now:** argos.security/kontakt

EXPECTED FROM Q1/2027

A more sovereign CDC

Digital sovereignty is becoming a procurement requirement: who has access to security-relevant data – and under which legal order? Argos is developing an answer to that.

Sovereign by design

Designed so that operation, data and control sit under German and European jurisdiction.

Data residency in Germany

On request in Germany – designed to avoid outflow to third countries.

Same CDC strength

24/7 detection, incident response and threat intelligence without compromise.

Who is already asking for this today: public sector and municipalities · regulated industries under NIS-2 and DORA · organisations that want to exclude third-country access to sensitive data.

In development. Availability **expected from Q1/2027**. Interested in helping shape it as a pilot customer? Talk to us.

IR CONTAINER · KEY FIGURES (target values for a service in development – not commitments)

approx. 48 hours	5–7 days	S · M · L	Zone model
until on site	to minimum operations (typically)	capacity classes	quarantine / clean / recovery

The shared foundation: both steps build on infrastructure operated in Germany – for the IR container together with STACKIT / Schwarz Digits. Sovereignty arises where operation, data and partners sit under one legal order.

Both steps serve the same goal: defence that holds when it matters – and stays under your control.

THE PORTFOLIO · EVERYTHING FROM ONE PROVIDER

More than 30 services across five pillars.

From prevention to improvement: Argos covers the complete path to cyber resilience – coordinated end to end, designed to minimise the gaps that open up between separately procured tools. A compact decision-maker guide exists for every service.

PREPARE

- Roadmap to Resilience
- Cyber Security Assessment
- CTEM
- IT Compliance Consulting
- Penetration Testing
- Tabletop Exercises
- Incident Response Plan
- Information Security Officer 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 and 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
- Crisis Management
- Support with Authority Notifications
- Recovery & Restoration
- IR Container (soon)

IMPROVE

- vCISO
- Vulnerability Management
- Security Awareness

Something we are proud of. Recognised by ISG as a **Rising Star** in the ISG Provider Lens Next-Gen SOC/MDR quadrant (midmarket, Germany). At the **CRN Channel Awards Germany 2026** Argos is a finalist for MSSP of the Year, and our Head of Partner Ecosystem, Xenia Sausele, is a finalist for MSSP Channel Partner of the Year.

ISG PROVIDER LENS

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

CRN AWARDS DE 2026 · NOMINATED

MSSP Channel Partner of the Year

Xenia Sausele, Head of Partner Ecosystem

Every service in detail: argos.security/leistungen · decision-maker guides for each service are available from your Argos contact on request.

ABOUT ARGOS · YOUR PARTNER FOR CYBER RESILIENCE

Talk to us – while the decision is still yours to make calmly.

Argos Security has been defending the German-speaking mid-market since 1999 – for more than 25 years – as a specialised German provider with a 24/7 Cyber Defense Center, practised incident response teams and in-house threat intelligence.

YOUR CONTACT · SALES

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

In an emergency – around the clock

+49 89 45 24 24-112

argos.security/notfall

“Know where you stand and you decide more calmly – and in time.”

Imprint & notes. Publisher: Argos Security GmbH, Koppstraße 14, 81379 Munich, Germany – registered at Amtsgericht München, HRB 125981 – Managing Director: Frank Pütz – VAT ID: DE457351414 – offices in Munich and Freiburg – +49 89 45 24 24-100 – kontakt@argos.security – argos.security. Responsible for editorial content under § 18(2) MStV: Nicolai Landzettel, Chief Marketing Officer, c/o Argos Security GmbH, address as above. Editorial and threat intelligence: Argos Security. ARGOS RADAR is a free quarterly information service for customers and prospective customers and does **not constitute legal or investment advice**. All information compiled to the best of our knowledge, as of 3 August 2026. We accept no liability for the accuracy, completeness or currency of this information; liability for intent and gross negligence, and for injury to life, body or health, remains unaffected. Threat data are partly self-reported by the actors. **How you receive this report:** we send ARGOS RADAR by e-mail only to recipients who have consented, or to existing customers under § 7(3) of the German Unfair Competition Act (UWG). Recipients in Austria, Switzerland and the United Kingdom receive electronic mailings only on the basis of prior consent. We process your business contact details on the basis of Art. 6(1)(f) GDPR (legitimate interest in direct marketing). **You may object at any time under Art. 21(2) GDPR**, free of charge apart from transmission costs at basic rates – an informal message to kontakt@argos.security is enough. Privacy notice: argos.security/datenschutz (German).

Third-party names. Product and company names are trademarks of their respective owners and are used for identification only. References to specific products relate exclusively to publicly reported vulnerabilities and incidents as of the date above; they are not a statement about the general security or quality of those products and imply no business relationship.

IN THE NEXT ISSUE · 03/26

- → Quarterly review of the threat landscape
- → Deep dive: the sovereign CDC
- → Sector spotlight: manufacturing & healthcare
- → Your questions to our CDC team