CASE STUDY

RIVA Engineering übersteht Ransomware-Angriff – mit Incident Response von Argos Security

Am frühen Morgen des 15. Dezember 2025 stehen bei RIVA Engineering die Systeme still: Die gesamte virtuelle Umgebung des international tätigen Fassadenbau-Unternehmens ist verschlüsselt. Mit dem Incident-Response-Team von Argos Security bringt RIVA den Angriff binnen Stunden unter Kontrolle, hält über einen strukturierten Notbetrieb die Produktion am Laufen und kehrt bereits am 7. Januar 2026 in den Regelbetrieb zurück – mit einer Sicherheitsarchitektur, die heute stärker ist als zuvor.

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. Das Ingenieur- und Fassadenbauunternehmen aus dem Mittelstand realisiert anspruchsvolle Gebäudehüllen rund um den Globus. Mit dem Wachstum stieg auch der Anspruch an die eigene IT. Sebastian Altmann kam im Juli 2024 als Head of IT an Bord – mit einem klaren Auftrag der Geschäftsleitung: die IT von Grund auf neu zu strukturieren.

AUSGANGSLAGE: EINE IT-SICHERHEIT IM WANDEL

Gemeinsam mit dem Partner Argos Security war RIVA bereits auf einem guten Weg. Viele Einzelsysteme liefen zuverlässig, doch sie bildeten noch keine Einheit. Das Monitoring war noch nicht lückenlos, zwei zentrale Bausteine fehlten. „Wir waren noch nicht am Limit, aber die Systeme haben noch keine Harmonie gebildet“, erinnert sich Sebastian Altmann. Beide Bausteine waren geplant und bereits im Projekt – nur noch nicht im Einsatz. „Leider ist es so, dass es immer zum falschen Zeitpunkt kommt.“

05:45 UHR: DER TAG, AN DEM NICHTS MEHR GING

Der 15. Dezember 2025 beginnt für Sebastian Altmann um 05:45 Uhr mit einem klingelnden Telefon. Niemand weiß zunächst, was los ist: Mitarbeitende können sich nicht einloggen, Systeme sind schlicht nicht erreichbar, in der Frühschicht lassen sich keine Aufträge mehr bearbeiten. „Der Tag war ziemlich bescheiden“, fasst Altmann rückblickend zusammen. Auf der halbstündigen Fahrt in die Firma telefoniert er bereits und sortiert die Möglichkeiten – an einen Angriff denkt er anfangs nicht. Doch je näher er dem Standort kommt, desto deutlicher drängt sich dieses Szenario auf.

Rund zweieinhalb Stunden versuchen Altmann und seine Admins mit allen verfügbaren Mitteln, wieder Zugriff auf die Systeme zu bekommen – ohne Erfolg. Die gesamte virtuelle Umgebung ist verschlüsselt. Weil RIVA in der Produktion mit Vorlauf arbeitet, steht zwar nicht sofort alles still, doch in mehreren Bereichen ist kein Arbeiten mehr möglich. „In meiner Position hört man viel davon und fragt sich: Kann uns das passieren? Und was ist, wenn es uns passiert?“

EIN ANRUF, ZEHN MINUTEN, EIN TEAM

Altmann entscheidet sich, seinen Ansprechpartner Leonard Bunjaku bei Argos Security anzurufen. Weil beide Seiten zuvor oft über genau dieses Szenario und über eine nachhaltige Lösung gesprochen hatten, genügen wenige Worte. „Es war schon ein bisschen wie in einem Film“, beschreibt Altmann die Situation.

Die Reaktionszeit nach dem Anruf beträgt keine zehn Minuten. Zunächst geht es um die Lagebestimmung: Wo steht das Unternehmen, was ist passiert? Parallel prüft das Forensik-Team von Argos Security gemeinsam mit der internen IT-Abteilung die Systeme. Zwischen 10 und 12 Uhr steht das vollständige Bild. „Um 12 Uhr wussten wir, was passiert ist, was wir tun müssen und wie die kommenden Wochen aussehen werden“, so Altmann.

ECKDATEN

Kunde: RIVA GmbH Engineering
Branche: Ingenieur- und Fassadenbau
Hauptsitz: Backnang
Mitarbeiterzahl: ca. 225
Umsatz: 15,7 Millionen Euro (2023)

PROJEKT UND VORTEILE

- Schnelle Incident Response nach Ransomware-Angriff – Mobilisierung des Teams binnen 10 Minuten
- Forensische Analyse und vollständiges Lagebild noch am selben Vormittag
- Strukturiertes Krisenmanagement auf Basis eines erprobten Incident Response Plans
- Aufbau und Steuerung von Notbetrieb und Wiederanlaufplan – Produktion weitgehend aufrechterhalten
- Systematische Wiederherstellung und Absicherung aller Endgeräte und Maschinen
- Rückkehr in den Regelbetrieb innerhalb von rund drei Wochen
- Nachhaltige Härtung der Sicherheitsarchitektur nach dem Vorfall

Argos Security GmbH
Koppstraße 14
81379 München

Tel. +49 89 45 24 24-100
Fax +49 89 45 24 24-199

sales@argos.security
www.argos.security

CASE STUDY

Wir mussten uns in erster Linie um nichts kümmern. Wir wurden einfach mit Fakten betankt: Uns wurde gesagt, was zu tun ist, und wir bekamen eine Entscheidungsgrundlage, ohne uns tiefgründig damit beschäftigen zu müssen.“

Sebastian Altmann
Head of IT, RIVA Engineering

ÜBER ARGOS SECURITY

Argos Security zählt zu den führenden Managed Security Service Providern (MSSP) im DACH-Raum und unterstützt den gehobenen Mittelstand, Konzerne und öffentliche Auftraggeber mit einem ganzheitlichen Ansatz für moderne Cybersecurity. Das nach ISO/IEC 27001 zertifizierte Unternehmen mit Standorten in München und Freiburg vereint mehr als 100 Cybersecurity-Expertinnen und Experten mit Erfahrung in Managed Security Services, Incident Response und Forensik. Zum Leistungsumfang gehören ein deutsches 24/7-Security Operations Center, Managed Detection & Response, ein eigenes Incident Response Team sowie IT-Sicherheits-, Netzwerk- und Datacenter-Lösungen und sicherheitsstrategische Beratung. So begleitet Argos Security seine Kunden von Prävention und Erkennung über Reaktion bis hin zur kontinuierlichen Weiterentwicklung ihrer Sicherheits- und Cyber-Resilienz-Strategie.

Sie wollen mehr erfahren?

Ihr persönlicher Ansprechpartner berät Sie gerne. Kontaktieren Sie uns einfach:

Argos Security GmbH
Koppstraße 14
81379 München

Tel. +49 89 45 24 24-100
Fax +49 89 45 24 24-199

sales@argos.security
www.argos.security

KEIN SCHWARZES LOCH, SONDERN EIN PLAN

Im Ernstfall steht ein betroffenes Unternehmen zunächst vor einem riesigen schwarzen Loch: Wo fängt man an, wie agiert man, mit wem nimmt man Kontakt auf? Hier setzt der Incident Response Plan von Argos Security an. „Wir mussten uns in erster Linie um nichts kümmern“, erklärt Altmann. „Wir wurden mit Fakten betankt, uns wurde gesagt, was zu tun ist, und wir bekamen eine Entscheidungsgrundlage, ohne uns tiefgründig damit beschäftigen zu müssen.“ In einer hochbelastenden Phase übernimmt Argos die Strategie und gibt RIVA die nötige Handlungssicherheit.

NOTBETRIEB UND WIEDERANLAUF

RIVA startet sofort in den Notbetrieb. Alle Standorte und Leitungen werden abgeriegelt, es gibt keine Verbindung mehr nach außen. Intern werden die Systeme voneinander isoliert. Schritt für Schritt entsteht gemeinsam mit Argos ein Wiederanlaufplan: Was ergibt Sinn, wie lässt sich arbeiten, welche Prioritäten gelten in der Produktion? Das Ergebnis kann sich sehen lassen – in der ersten Woche wird von Montag bis Donnerstag weiter produziert, bevor ein Ausfall von lediglich zwei Tagen folgt. „Das war schon sehr stark“, sagt Altmann.

WIEDERHERSTELLUNG IM SCHULTERSCHLUSS

Die Wiederherstellung erfordert auch eine optimale Zusammenarbeit von RIVA und Argos Security: Die Forensiker von Argos übernehmen die Analyse, während interne Spezialisten die Endgeräte absichern. Computer werden, wo möglich, neu installiert; andere Geräte werden über eine spezielle Software gescannt und durch Argos ausgewertet, bis ihre Unbedenklichkeit feststeht. Erst dann gibt RIVA sie – ebenso wie die Maschinen – wieder für den Betrieb frei. Bereits am 7. Januar 2026 wird wieder regulär gearbeitet. Für einen Vorfall dieser Größenordnung ein bemerkenswert zügiger Wiederanlauf.

STÄRKER AUS DER KRISE – UND EINE PARTNERSCHAFT, DIE BLEIBT

Heute ist RIVA Engineering so aufgestellt, wie es schon vor dem Vorfall geplant war, und betrachtet Security konsequenter als je zuvor. Auf Endgeräten und Servern sorgt XDR für erweiterte Erkennung und Transparenz über sicherheitsrelevante Ereignisse. Die Microsoft-365-Umgebung ist gezielt gegen Phishing, Malware und Spam abgesichert, ergänzt um Backup, Archivierung und Security Awareness. Und eine kontinuierliche, betreute Bedrohungserkennung sorgt dafür, dass potenzielle Vorfälle frühzeitig auffallen, eingeordnet und priorisiert werden. „Wir haben jetzt alles, was geht", so Altmann.

Sein Rat an andere IT-Verantwortliche ist eindeutig: „Es ist nicht die Frage, ob man gehackt wird, sondern wann. Keiner ist sicher.“ Entscheidend sei, dass Systeme, Teams und Dienstleister zusammenspielen – und dass man Expertise hinzuzieht, statt an der Sicherheit zu sparen.

Aus der gemeinsam bewältigten Krise ist mehr als eine Lieferantenbeziehung geworden. Die Fachleute von Argos Security waren über Weihnachten, die Feiertage und Silvester durchgehend für ihren Kunden RIVA erreichbar; Auswertungen und nachhaltige Lösungen entstehen seither gemeinsam. „Argos Security ist für uns mittlerweile einfach mehr als ein Dienstleister geworden“, resümiert Altmann.

Verdacht auf einen Cyberangriff?

Unsere **Incident-Response-Experten** sind 24/7 & 365 Tage im Jahr für Sie da:

Ihre Notfallhotline: +49 89 45 24 24-112