SUCCESS STORY

VON DER ZUSAMMENARBEIT

sure[secure]
your security operations center

BSW

Kurzvorstellung des Partners

Die Badische Stahlwerke GmbH (BSW) ist ein Stahlhersteller aus Deutschland. Am Standort Kehl werden jährlich bis zu 2,4 Millionen Tonnen Stahl produziert. Die Produktion basiert auf dem ressourcen-schonendem Recycling von Stahlschrott. Daraus entstehen unter anderem Stabstahl oder Walzdraht. Mit einem Umsatz von über einer Milliarde Euro und knapp 1.000 Beschäftigten ist die Badische Stahlwerke GmbH ein wichtiger Faktor für die deutsche Stahlbranche und Industrie.

Badische Stahlwerke GmbH

Branche:	Stahlindustrie
Mitarbeitende:	1.000
Gründung:	1955
Stahl p.a.:	2,4 Mio. Tonnen
Umsatz:	1 Mrd. EUR

Diese Themen sind Bestandteil der Success Story

- Incident Response Retainer
- Incident Response Management
- Bedeutung von Vertrauen im Security-Umfeld

Incident Response Retainer: Wenn der Ernstfall Realität wird

„Wir hofften, den Retainer nie zu brauchen. Aber als es darauf ankam, war er Gold wert.“
- Ralf Butsch, CISO, Badische Stahlwerke GmbH

Als Stahlproduzent setzt die Badische Stahlwerke GmbH seit jeher auf vorausschauende IT-Sicherheit. Denn wenn die Stahlproduktion aufgrund von IT-Problemen ausfällt, kann das ernsthafte Folgen haben.

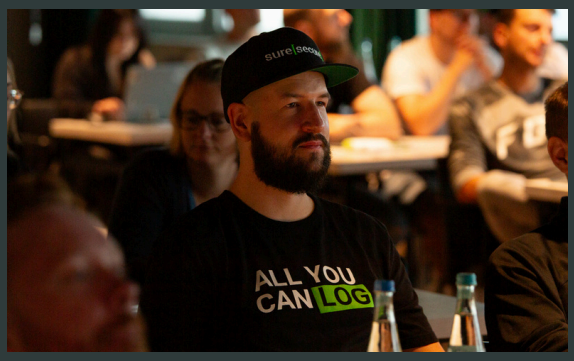
Aus diesem Grund entschied sich das Unternehmen Ende 2022 dazu, einen IR-Retainer abzuschließen. Denn es fehlte die Expertise, um einen Cyberangriff intern zu bewältigen. Wir haben den besonderen Fall mit CISO Ralf Butsch, der erst nach dem Sicherheitsvorfall zur BSW kam, in einem Interview Revue passieren lassen. Er kennt alle Details.

Fotos: Carsten Görling

Ausgangssituation: Vorsorge statt Nachsicht

Nachdem die Entscheidung getroffen wurde war, einen Incident Retainer zu beauftragen, stand die Evaluierung relevanter Anbieter an. Ralf betont aus heutiger Sicht, dass ihm insbesondere folgende Punkte wichtig sind:

- ein fester Ansprechpartner mit Krisenerfahrung
- deutschsprachige Betreuung
- ein belastbares, vertrauensvolles zwischenmenschliches Verhältnis
- regelmäßige Krisenübungen



Ist es überraschend, dass es vorrangig um das Zwischenmenschliche geht? Eigentlich nicht, denn wenn man in einem Incident gemeinsam am Herzen des Unternehmens operiert, ist man froh, wenn man den „Arzt“ kennt und weiß, dass dieser diesen Eingriff schon ein paar Mal gemacht hat. Und dennoch: Bei einer solchen OP arbeiten alle an der Leistungsgrenze.

Als der Stahlproduzent den Incident Response Retainer bei der suresecure GmbH beauftragte, geschah das mit der leisen Hoffnung, ihn nie aktivieren zu müssen. Denn wer wünscht sich schon einen IT-Sicherheitsvorfall im eigenen Unternehmen?

Was jedoch niemand ahnen konnte: Zum Zeitpunkt der Vertragsunterzeichnung war der Angreifer höchstwahrscheinlich bereits im Netzwerk aktiv. Zwar liefen parallel Projekte zur Stärkung der Cyber-Resilienz, diese kamen jedoch zu spät.

Der Notfall: Angriff aus dem Posteingang

Die Attacke begann mehrere Wochen vor dem Ausrollen der Ransomware mit einer klassischen Phishing-Mail. Der Angreifer bewegte sich unbemerkt durch das System, sammelte Berechtigungen und konnte die Schadsoftware platzieren. Als die Systeme schließlich verschlüsselt wurden, war es zu spät für Gegenmaßnahmen:

Nichts ging mehr. Keine Anmeldung, kein Telefon, keine Kommunikation.

“Wir haben das Faxgerät aus dem Keller geholt, um überhaupt noch kommunizieren zu können“, zitiert Ralf Butsch einen Kollegen.

LKWs stauten sich vor dem Werkstor, Kundenanfragen blieben unbeantwortet, die interne Kommunikation fiel aus. Die digitale Infrastruktur des Unternehmens war vollständig lahmgelegt.

Und dann?

„Dann haben wir sofort bei euch angerufen - die Notfallnummer hing da am Tresen. Und 15 Minuten später war Hilfe da. Das war für uns ein Wendepunkt.“

Besonders beeindruckt habe ihn die Geschwindigkeit und die klare Kommunikation:

„Alle waren erleichtert, dass nun jemand da war, der wusste, was zu tun ist.“

Der Wendepunkt: Vom Feuerlöschen zur Brandschutzmauer

Der Vorfall war ein Einschnitt, aber auch der Startpunkt für eine deutlich gestärkte Cyber- und Business-Resilienz. Nach der Aktivierung des Retainers wurden unmittelbar mehrere Workstreams gestartet. Zusätzlich zur forensischen Untersuchung war es wichtig, die Meldepflichten zu berücksichtigen und den gesamten Kommunikationsprozess zu durchleuchten.

Um Reputationsschäden zu vermeiden, ist eine zielgruppengerechte und proaktive Kommunikation entscheidend. Schließlich haben alle Anspruchsgruppen ein berechtigtes Interesse an der Situation. Unser Incident Framework deckt folgende Themen ab:

- **Incident Management**:
  Organisation, Planung, Koordination aller Gewerke
- **Containment**:
  Eindämmung des Schadens, sofern möglich
- **Communication**:
  Zielgruppengerechte Krisenkommunikation
- **Legal**:
  Juristische Begleitung
- **Desaster Plan:**
  Erstellung eines Fahrplans durch den Incident
- **Recovery**:
  Sofortiger Beginn mit dem Wiederaufbau, Säuberung der Infrastruktur
- **Forensics**:
  Tiefgehende Analyse und Rekonstruktion der Cyber-Kill-Chain

Ein Ansprechpartner für alle relevanten Bausteine - auch wenn BSW durchaus über eigene Ressourcen für Communication und Legal verfügt:

„Ein Sparringspartner mit Erfahrung tut in so einer Situation einfach enorm gut, um Sicherheit im Umgang mit der Vielzahl an Themen zu gewinnen“, so Ralf.

Aus meiner Perspektive kann ich nur meinen größten Respekt an das gesamte Incident-Team aussprechen. Was in diesen Zeiten geleistet wird, ist teilweise wirklich unmenschlich.

Ich bin sehr froh und auch stolz, dass wir aus dem Vorfall bei der BSW eine wirklich starke Partnerschaft dazu gewinnen konnten.

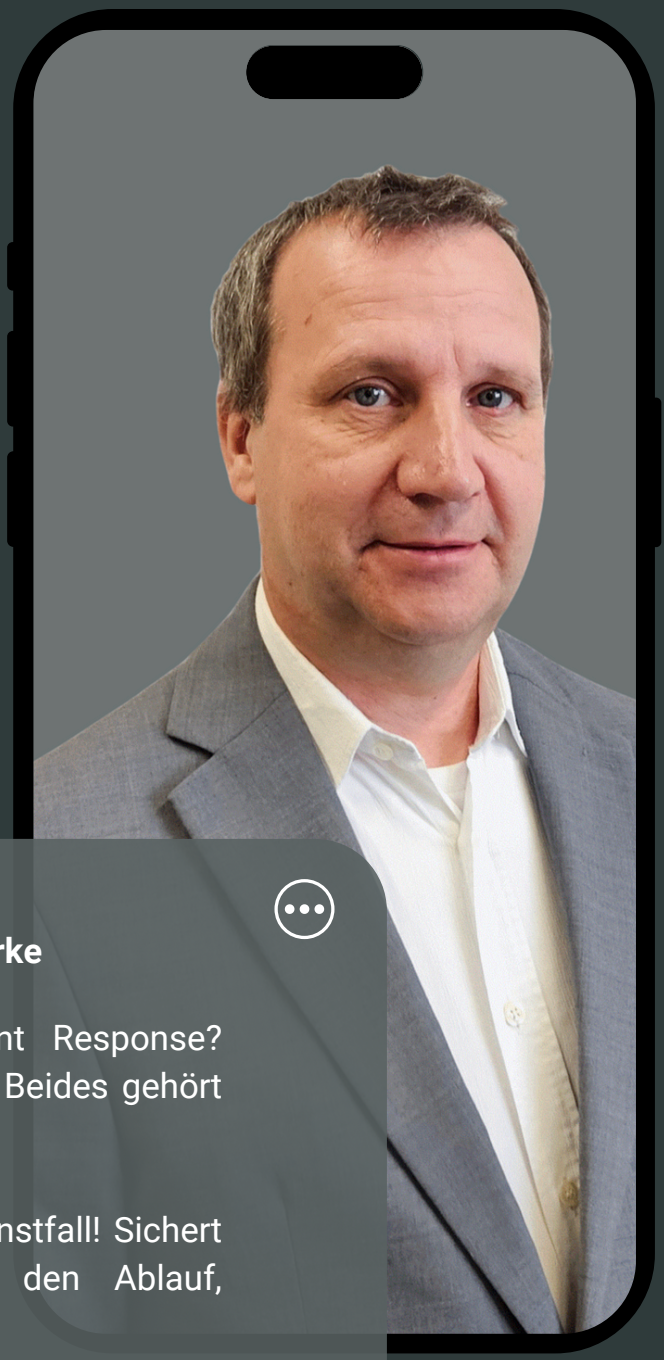
Filip Krauß
Enterprise Account Executive
suresecure GmbH

Der Wendepunkt: Vom Feuerlöschen zur Brandschutzmauer

Nach dem Vorfall wurde ein umfassendes Security Operations Center (SOC) aufgebaut, Prozesse neu definiert und das ISMS geschärft. Heute ist das Unternehmen breiter und besser aufgestellt und betrachtet Cybersicherheit als kontinuierlichen Weiterentwicklungsprozess. Dabei setzt BSW insbesondere im Service-Bereich auf starke Partnerschaften.

SafeGuard, der Incident Response Retainer von suresecure, ist mehr als ein Vertrag - er ist der Beweis, dass im Ernstfall Sekunden zählen…

Sein Rat an Kolleginnen und Kollegen aus der Industrie ist eindeutig:



Ralf Butsch
CISO Badische Stahlwerke

Ein SOC ohne Incident Response? Würde ich nie machen. Beides gehört zusammen.

Wartet nicht auf den Ernstfall! Sichert euch ab und testet den Ablauf, solange ihr noch könnt.

Key Take-Aways:

- Vorbereitung entscheidet den Ernstfall
- Vertrauen schlägt Technik
- Aus dem Angriff wächst Resilienz

suresecure gmbh
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de