BASEC GMBH
BASECONSULTING
BUSINESS CONTINUITY MGMT

CASE STUDY · ENERGIE

Resilienz, die dem Sturm standhält

Wie ein KRITIS-Energieversorger Informationssicherheit, Notfall- und Krisenmanagement zu einem einzigen, belastbaren System verbindet, und den Ernstfall besteht.

„Eine alte Kiefer bricht nicht, sie biegt sich mit dem Wind, während ihre Wurzeln tief im Fels verankert bleiben."

ZUM GELEIT

Das Prinzip der Betriebskontinuität

Eine alte Kiefer an stürmischer Küste bricht nicht, sie biegt sich mit dem Wind, während ihre Wurzeln tief im Fels verankert bleiben. Genau darin liegt das Prinzip guter Betriebskontinuität: nicht jeden Sturm verhindern, sondern ihn abfedern, aus ihm lernen und danach fester stehen als zuvor.

Für einen Betreiber kritischer Infrastruktur ist das keine Metapher, sondern Pflicht. Diese Case Study zeigt, wie aus drei isolierten Disziplinen ein zusammenhängendes System wurde, das im realen Ernstfall genau so trug, wie es geplant war.

INHALT

01 · ÜBER DEN KUNDEN

Ein Versorger mit Verantwortung für die Grundlast

Unser Kunde ist ein regionaler Energieversorger mit eigener Erzeugungs- und Einspeise-Infrastruktur, der überwiegend Industriekunden mit Strom versorgt. Als Betreiber kritischer Infrastruktur (KRITIS) trägt er eine Aufgabe, die keinen Aufschub kennt: Die Versorgung muss laufen, jederzeit.

Aufgrund der strengen regulatorischen Vorgaben war die Informationssicherheit bereits sehr gut aufgestellt: ein etabliertes ISMS, gelebte Prozesse, klare Verantwortlichkeiten. Was fehlte, war die zweite Hälfte der Resilienz, ein vollumfängliches Notfallmanagement und ein übergreifendes, verknüpftes BCMS.

KRITIS | ISMS etabliert | BCM offen | NIS2

KUNDENPROFIL

BRANCHE	Energie · KRITIS
STRUKTUR	Eigene Erzeugung + Einspeisung
KUNDEN	Überwiegend Industrie
GRÖSSE	Mehrere hundert MA
REIFEGRAD	ISMS stark · BCM lückenhaft

BRANCHEN-KONTEXT

Der Energiesektor ist der am strengsten regulierte NIS2-Bereich, mit 24-Stunden-Meldepflicht, verpflichtenden Risikobewertungen und persönlicher Haftung der Geschäftsleitung.

02 · DER KONTEXT

Drei Disziplinen, die nebeneinander statt miteinander arbeiteten

Den Anstoß gab eine gezielte Frage: Wie belastbar ist unser bestehendes Notfallmanagement wirklich? Die Überprüfung deckte eine strukturelle Lücke auf, das Krisenmanagement war rein auf physische Vorkommnisse ausgelegt. Ein IT-Ausfall oder ein Informationssicherheitsvorfall war darin schlicht nicht vorgesehen.

IS

Informationssicherheit

Stark aufgestellt, aber nicht mit dem Notfallmanagement verzahnt.

BCM

Business Continuity

Auf dem Papier vorhanden, im Alltag nicht aktiv gelebt.

KM

Krisenmanagement

Die einzige, und unzureichende, Schnittstelle zwischen beiden.

▪ isoliert · keine gemeinsame Eskalationskette · blinder Fleck im Ernstfall ▪

DER BLINDE FLECK

Für einen KRITIS-Betreiber liegt die Lücke an genau der Stelle, an der im Ernstfall Sekunden zählen: dort, wo ein technischer Vorfall zur Gefährdung der Versorgung wird.

03 · DER SCHMERZPUNKT

Ein Fundament, das erst noch gegossen werden musste

Ein belastbares BCMS beginnt mit einer sauberen **Business Impact Analysis (BIA)**, der systematischen Bewertung, welche Geschäftsprozesse wie kritisch sind und wie lange sie ausfallen dürfen. Doch dafür fehlte die Grundlage: Ein Teil der Geschäftsprozesse war noch nicht ausreichend beschrieben oder bewertet.

Die Herausforderung war doppelt: die isolierten Disziplinen zusammenzuführen, und gleichzeitig das methodische Fundament zu legen, auf dem eine belastbare BIA überhaupt erst möglich wird.

DAS KERNRISIKO

Als KRITIS-Betreiber muss der Versorger die Stromversorgung zwingend aufrechterhalten. Ohne integriertes Notfallmanagement drohte, bei einem IT-Ausfall oder Sicherheitsvorfall nicht koordiniert und nicht schnell genug reagieren zu können.

BRANCHEN-INSIGHT · BSI-LAGEBERICHT 2025

+31 %

stärkste Angriffszunahme aller Branchen, auf 89 gemeldete Angriffe und 23 bedeutsame Störungen im Energiesektor.

~48 %

der KRITIS-Betreiber verfügen über kein System zur Angriffserkennung.

04 · DIE ZIELSETZUNG

Ein System, in dem alles ineinandergreift

Das Zielbild war kein weiteres Dokument im Regal, sondern ein gelebtes, vernetztes System. Vier Leitziele gaben die Richtung vor, jedes Glied trägt das nächste.

01
Verbinden
Informationssicherheit, Krisen- und Notfallmanagement zu einer durchgängigen Eskalationskette zusammenführen, Schluss mit isolierten Disziplinen.

02
Fundieren
Die Prozesslandschaft methodisch so aufbereiten, dass eine belastbare Business Impact Analysis überhaupt erst möglich wird.

03
Verankern
Richtlinien, Notfallpläne und Eskalationsstufen fest in die bestehenden Unternehmensstrukturen einbetten, damit sie im Alltag greifen.

04
Vernetzen
IT-Komponenten und Geschäftsprozesse systemgestützt koppeln, ein technischer Ausfall wird sofort seiner geschäftlichen Wirkung zugeordnet.

AUS ZIELEN WIRD EINE KETTE

01 Verbinden → 02 Fundieren → 03 Verankern → 04 Vernetzen

05 · UNSER ANSATZ

Den Weg zeigen, ohne das Ruder zu übernehmen

Der Lotsenfisch navigiert Größere sicher durch unruhige Gewässer, er kennt die Klippen, ohne das Ruder zu übernehmen. Genau so verstehen wir unsere Rolle. Statt ein fertiges System überzustülpen, haben wir gemeinsam mit den Verantwortlichen für Informationssicherheit, BCM, IT-Leitung und Prozessmanagement eines aufgebaut, das das Unternehmen selbst tragen und weiterführen kann.

◆ Methodik · BSI-Standard 200-4

INTEGRIERTER ANSATZ

Nach dem Gedanken des BSI-Standards 200-4 werden Business Continuity, Informationssicherheit und Krisenmanagement nicht getrennt betrachtet, sondern als Bausteine **organisatorischer Resilienz** zusammengeführt.

VOM NEBENEINANDER ZUR EINHEIT

IS
Informations-sicherheit

BCM
Business Continuity

KM
Krisen-management

→

ERGEBNIS
Organisatorische Resilienz

UNSER PRINZIP

Gesamtheitlich statt stückweise: erst die Disziplinen verbinden, dann die Infrastruktur aufbauen, in der Prozesse und IT-Komponenten systemgestützt ineinandergreifen.

06 · DIE UMSETZUNG

In vier Schritten vom Flickwerk zum System

01 Analyse + Konzeption — gemeinsamer Rahmen

Überprüfung der bestehenden Schnittstellen und Zusammenführung von Informationssicherheit, Krisen- und Notfallmanagement zu einem gemeinsamen Rahmen.

02 Struktureller Aufbau — Richtlinien + Notfallpläne

Erstellung grundlegender Richtlinien, Notfallpläne und Notfallszenarien, integriert in die bestehenden Unternehmensstrukturen, damit sie im Alltag greifen.

03 Prozessmanagement + BIA — BIA-Fundament

Gemeinsam mit dem internen Prozessmanagement wurde die Prozesslandschaft in einem BPM-System etabliert und darin die Business Impact Analysis vollständig abgebildet, das methodische Fundament des BCMS.

04 Tool-Integration — Ausfall → Prozess-Mapping

Anbindung der Anwendungen über ein EA- und ein Monitoring-System an die IT-Komponenten. Fällt eine Komponente aus, erfolgt sofort die Zuordnung zu den betroffenen Geschäftsprozessen.

HÜRDE + LÖSUNG

Die Prozessdokumentation war unterschiedlich reif. Gelöst durch enge Zusammenarbeit mit dem Prozessmanagement: fehlende Prozesse wurden zuerst sauber aufgenommen, bevor die BIA methodisch belastbar durchgeführt wurde.

07 · DIE LÖSUNG

Ein BCMS, das den Ernstfall kennt, bevor er eintritt

Das Ergebnis ist ein vollständig vernetztes System: Fällt eine IT-Komponente aus, wird der Alarm sofort aufgeschaltet, technisch bewertet und dem betroffenen Geschäftsprozess zugeordnet. Auf einen Blick ist ersichtlich, ob die **RTO-Werte**, die Wiederanlaufzeiten aus der maximal tolerierbaren Ausfallzeit, noch eingehalten werden.

BCMS · BETRIEBSLAGE — ● Live-Status

IT-KOMPONENTE	GESCHÄFTSPROZESS	RTO	STATUS
Netzleitsystem	Stromeinspeisung	15 min	● im Ziel
SCADA-Gateway	Netzüberwachung	30 min	● Eskal. 1
Leitstand-Comms	Krisenkommunikation	60 min	● im Ziel
Abrechnung	Kundenprozesse	4 h	● im Ziel

EREIGNIS-TICKER | 12:04 Ausfall **SCADA-Gateway** erkannt → Prozess **Netzüberwachung** betroffen →

● im Ziel · RTO eingehalten ● Eskalation · Notfallplan aktiv ▪ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP IM ERNSTFALL

01 **Ausfall erkannt** → 02 **Technisch bewertet** → 03 **Prozess zugeordnet** → 04 **Eskalation ausgelöst** → 05 **Wiederanlauf + RTO-Check**

VOM NEBENEINANDER ZUR KETTE

Aus einem reaktiven Nebeneinander ist ein vorausschauendes System geworden: Informationssicherheit, Notfall- und Krisenmanagement greifen als eine durchgängige Kette ineinander, von der Erkennung bis zum geprüften Wiederanlauf.

08 · ERGEBNIS + WIRKUNG

Bestanden, im Audit und in der Realität

Zero Findings

Externes Audit ohne jegliche Abweichungen bestanden.

Real-Test bestanden

Notfallwege durch realen Komponentenausfall erfolgreich erprobt.

3 → 1

Aus drei isolierten Disziplinen wurde ein integriertes System.

NACHHALTIGE WIRKUNG

Der Wert liegt jenseits des Audits: Technische Ausfälle werden sofort erkannt, bewertet und ihrer geschäftlichen Wirkung zugeordnet. Die Mitarbeitenden wurden geschult, und als ein realer Ausfall die Notfallwege auf die Probe stellte, trugen sie genau wie geplant.

09 · STIMME DES KUNDEN

> **Zum ersten Mal greifen Informationssicherheit, Notfall- und Krisenmanagement bei uns wirklich ineinander. Als ein realer Ausfall unsere Notfallwege auf die Probe stellte, funktionierte das System genau so, wie wir es geplant hatten, ruhig, koordiniert und nachvollziehbar.**

Verantwortliche:r für Informationssicherheit, regionaler Energieversorger

10 · KEY ACHIEVEMENTS

Was bleibt

- Vollumfängliches BCMS mit Notfallmanagement und Eskalationsstufen etabliert
- Informationssicherheit, BCM und Krisenmanagement durchgängig verzahnt
- Belastbare BIA auf sauber aufbereiteter Prozesslandschaft
- IT-Komponenten und Geschäftsprozesse systemgestützt gekoppelt
- Externes Audit mit „Zero Findings" bestanden
- Notfallwege im realen Ernstfall erfolgreich erprobt
- Mitarbeitende geschult, Resilienz ist im Alltag verankert

FAZIT · AUS PFLICHT WIRD STÄRKE

Der Versorger hat die fehlende zweite Hälfte seiner Resilienz gewonnen, nicht durch ein weiteres Dokument, sondern durch ein gelebtes System, in dem alle Fäden zusammenlaufen.

WIE DIE KIEFER IM STURM

Der Versorger steht heute fester als zuvor, nicht, weil kein Wind mehr weht, sondern weil er den Schlag abfedern, aus ihm lernen und koordiniert reagieren kann.

11 · FAZIT

Aus Pflicht wird Stärke.

Business Continuity Management macht aus einer regulatorischen Pflicht echte, belastbare Stärke. Der Versorger reagiert im Ernstfall heute ruhig, koordiniert und nachvollziehbar, weil Informationssicherheit, Notfall- und Krisenmanagement als eine Kette ineinandergreifen.

AUSBLICK

Das System ist gelebte Praxis, regelmäßige Übungen, aktualisierte BIA und laufendes Monitoring halten die Resilienz auf Stand.

ÜBERTRAGBAR

Der integrierte Ansatz nach BSI-Standard 200-4 lässt sich auf weitere KRITIS-Sektoren und regulierte Branchen übertragen.

ÜBER BASEC

Wie belastbar ist Ihr Notfallmanagement wirklich?

Basec ist ein kleines, aber sehr feines Cyber-Security-Beratungshaus, persönlich, pragmatisch und auf Augenhöhe. Diese Case Study entstand im Bereich **BaseConsulting, Business Continuity Management**.

IHR ANSPRECHPARTNER

Tim Will

Partnermanagement · Basec GmbH

tim.will@basec.de · +49 6326 346 3005

Erstgespräch vereinbaren →

Basec GmbH · Weinstraße 5b · 67146 Deidesheim · basec.de

Hinweis zur Erstellung. Für Grafik, Gliederung und Textbearbeitung dieser Publikation wurden generative KI-Systeme eingesetzt. Sämtliche Inhalte wurden von Basec fachlich geprüft, überarbeitet und freigegeben. Die inhaltliche Verantwortung liegt bei der Basec GmbH.