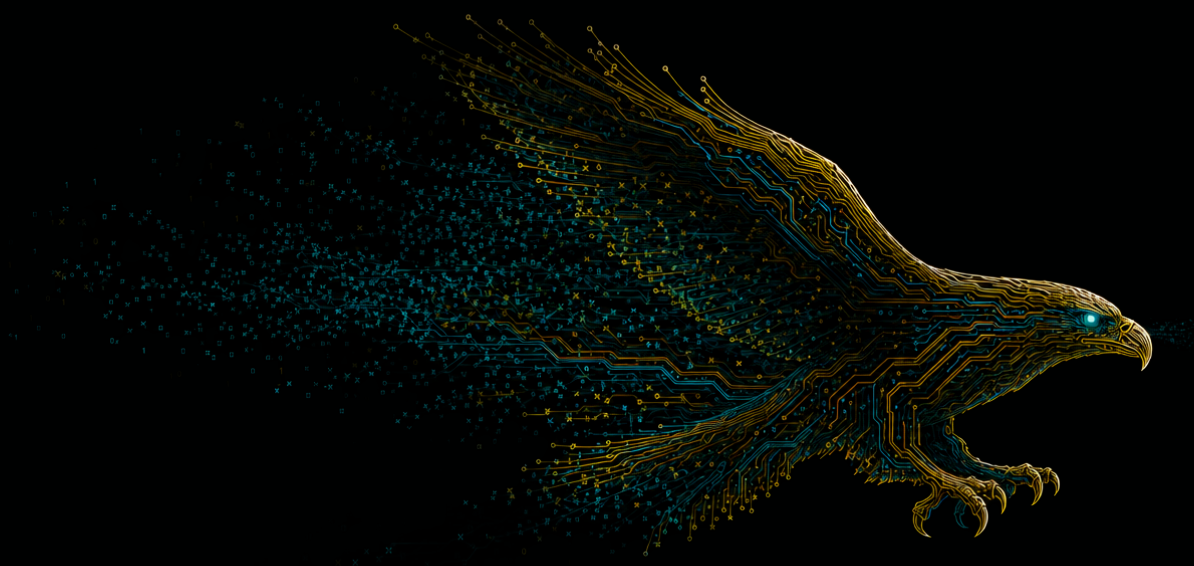
BASEC GMBH
BASECONSULTING
ISMS, BCM, PHYSISCHE SICHERHEIT, KRITIS

CASE STUDY · ÖFFENTLICHER SEKTOR

Den Überblick behalten, wenn es brennt

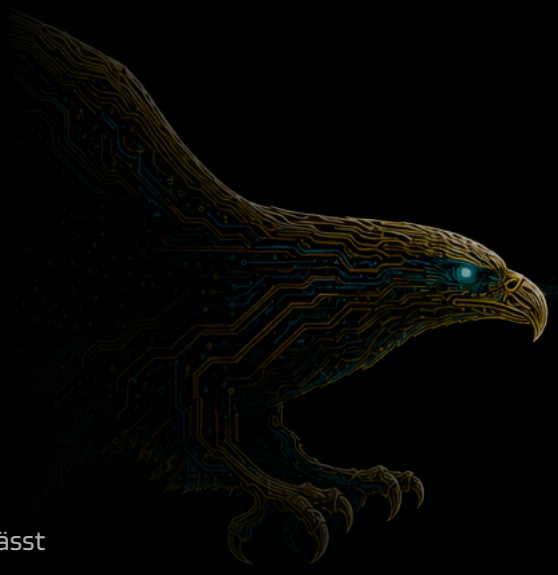
Wie eine große Behörde eine vakante Schlüsselrolle an der Schnittstelle von physischer und Informationssicherheit nahtlos überbrückt, und offene Auditauflagen unter härtestem Zeitdruck fristgerecht schließt.

„Der Adler thront über den Dingen, lässt sich von Böen nicht beirren und greift nur dann ein, wenn es nötig ist, mit absoluter Präzision."



ZUM GELEIT

Das Prinzip des souveränen Überblicks



Der Adler thront über den Dingen. Er hat alles im Blick, lässt sich von Böen nicht beirren und greift nur dann ein, wenn es nötig ist, dann aber mit absoluter Präzision. Seine Stärke ist nicht Hektik, sondern Überblick.

Genau darauf kommt es an, wenn mehrere sicherheitskritische Aufgaben gleichzeitig drängen und die Zeit knapp ist. Diese Case Study zeigt, wie eine plötzlich unbesetzte Schlüsselrolle souverän überbrückt wurde, ohne dass ein einziges Audit ins Wanken geriet.

INHALT

01 · ÜBER DEN KUNDEN

Eine Institution, die nicht ausfallen darf

Unser Kunde ist eine große Behörde im öffentlichen Sektor, ein Betreiber kritischer Infrastruktur (KRITIS). Sicherheit ist hier zweierlei zugleich: der Schutz der Informationen und der Schutz der physischen Bereiche, in denen diese verarbeitet werden, vom Rechenzentrum über Zugangsbereiche bis zur Gebäudeüberwachung.

Genau an dieser Schnittstelle, zwischen physischer Sicherheit und Informationssicherheit, war eine Schlüsselrolle durch strukturelle Veränderungen und den Weggang von Fachpersonal unbesetzt. Die Behörde brauchte dringend temporäre Unterstützung, bis eine neue interne Kraft gefunden ist.

KRITIS · Öffentlicher Sektor · BSI IT-Grundschutz · Vakanz

KUNDENPROFIL

BRANCHE	Öffentlicher Sektor · KRITIS
UMFELD	Rechenzentrum, Zugangsbereiche, Gebäude
RAHMEN	BSI IT-Grundschutz
AUSGANGSLAGE	Schlüsselrolle unbesetzt

BRANCHEN-KONTEXT

Seit Dezember 2025 greifen NIS2 (Cybersicherheit) und das KRITIS-Dachgesetz (physische Resilienz) zusammen, eine duale Architektur gegen die hybride Bedrohungslage. Genau an dieser Naht von physischer und Informationssicherheit lag die Herausforderung.

02 · DER KONTEXT

Eine Schlüsselrolle, die niemand vertrat

Die unbesetzte Rolle war keine gewöhnliche Vakanz. Sie saß an der Nahtstelle zweier Welten: der baulich-physischen Sicherheit (Rechenzentrum, Sicherheitsdienst, Aufschaltstelle, Gebäudeüberwachung und -steuerung) und der Informationssicherheit nach BSI IT-Grundschutz. Der aktuelle Sicherheitsstand musste erst neu ermittelt werden.

01

Unbesetzt

Schnittstelle physische + Informationssicherheit ohne Vertretung.

02

Unklar

Der aktuelle Sicherheitsstand musste erst neu ermittelt werden.

03

Unter Druck

BSI-Anforderungen im KRITIS-Umfeld, bei bereits laufenden Fristen.

■ unbesetzt · unklar · unter Zeitdruck ■

DER KERN DER AUFGABE

Die komplexen BSI-IT-Grundschutz-Anforderungen mussten in diesem speziellen KRITIS-Umfeld auf ihre praktische Umsetzung geprüft und strukturiert werden, ohne dass ein laufendes Verfahren ins Stocken gerät.

03 · DER SCHMERZPUNKT

Mehrere Fristen, ein Monat, kein Vertreter

Der Zeitdruck war massiv. Aus einem vorangegangenen Sicherheitsaudit waren Auflagen offen, die zwingend binnen **eines Monats** geschlossen werden mussten, um die Nachprüfung zu bestehen. Zeitgleich durften wichtige Folgethemen nicht ins Stocken geraten.

Die Vorbereitung eines internen Reifegradaudits, ein Pentest und die Aktualisierung der Sicherheitskonzepte (SiKos) liefen parallel, während sich eine neue Fachkraft erst in ein hochkomplexes Umfeld einarbeiten müsste.

DAS KERNRISIKO

Ohne fristgerechtes Schließen der Auflagen wäre die Audit-Nachprüfung gescheitert, mit unmittelbaren Folgen für den Nachweis der Sicherheit kritischer Bereiche.

BRANCHEN-INSIGHT · FACHKRÄFTEMANGEL

~120.000

Cybersecurity-Fachkräfte fehlen laut ISC²-Studie 2024 allein in Deutschland.

≤ 10

Bewerbungen erhielt 2024 knapp die Hälfte der öffentlichen Organisationen auf eine ausgeschriebene Cyber-Stelle.

04 · DIE ZIELSETZUNG

Überblick schaffen, bevor gehandelt wird

Das Zielbild war nicht, alles auf einmal zu tun, sondern das Richtige zuerst. Vier Leitziele gaben die Richtung vor.

01
Sichten
Den tatsächlichen Sicherheitsstand vollständig und ehrlich erfassen, als belastbare Grundlage.

02
Priorisieren
Die kritischsten Themen, die offenen Auditfindings, sofort und fristgerecht angehen.

03
Strukturieren
Alle weiteren Aufgaben transparent erfassen, terminieren und den Zuständigen zuweisen.

04
Überbrücken
Die Rolle so ausfüllen, dass kein Prozess stagniert und kein Audit fehlschlägt.

AUS ZIELEN WIRD EIN VORGEHEN

01 Sichten → 02 Priorisieren → 03 Strukturieren → 04 Überbrücken

05 · UNSER ANSATZ

Erst den Überblick, dann den Zugriff

Wie der Adler, der die Böen nicht fürchtet, weil er den Überblick behält, wählten wir einen hochgradig strukturierten und priorisierten Ansatz. Die kritischsten Themen, die offenen Audit-Findings, wurden sofort angegangen. Alle weiteren Aufgaben wurden systematisch in einem Risiko-Board erfasst, priorisiert, terminiert und den Zuständigen zugewiesen.

◆ Methodik · Risiko-Board (Kanban) + BSI IT-Grundschutz

AUS DRUCK WIRD ORDNUNG

Aus einer unübersichtlichen Drucksituation entstand eine klare, nachvollziehbare Ordnung, in der jederzeit sichtbar war, **was als Nächstes zählt**.

DREI HEBEL, EIN ÜBERBLICK

01 **Fokus**

02 **Struktur**

03 **Tracking**

→

ERGEBNIS
Souveräner Überblick

UNSER PRINZIP

Erst der Überblick, dann der Zugriff. Wer unter Druck priorisiert, statt hektisch alles gleichzeitig zu versuchen, verliert weder Fristen noch Qualität.

06 · DIE UMSETZUNG

Ein Zyklus, vier präzise Eingriffe

01 Fristgerechte Audit-Rettung — Nachprüfung bestanden

Abarbeitung der offenen Auditfindings mit pragmatischen Kompromissen innerhalb des einen Monats.

02 Reifegradaudit — alle Anmerkungen zu

Intensive Vorbereitung und erfolgreiche Begleitung des internen Reifegradaudits, rund drei Monate später.

03 SiKo + Pentest — SiKo aktuell

Aktualisierung des Sicherheitskonzepts und Durchführung des Pentests, weitere zwei Monate später.

04 Architekturanpassung — Basis für Folgezyklus

Anpassung der Sicherheitsarchitektur und Überführung in das aktualisierte SiKo, als Vorbereitung auf den nächsten Zyklus.

HÜRDE + LÖSUNG

Die extreme Deadline von nur einem Monat für die Audit-Nachprüfung, bei gleichzeitiger Neu-Einarbeitung in ein komplexes Umfeld. Gelöst durch klare Fokussierung, pragmatische Kompromisse und konsequentes Tracking über ein Risiko-Board.

07 · DIE LÖSUNG

Ein Board, das jederzeit zeigt, was zählt

Kern der Lösung war ein transparentes **Risiko-Board**: Jedes Finding, jede Aufgabe wurde erfasst, nach Kritikalität priorisiert, mit einer Frist versehen und einer verantwortlichen Person zugewiesen. So war auf einen Blick sichtbar, was sofort zu tun ist und was terminiert warten kann.

AUDIT- + RISIKO-BOARD — Board-Status

THEMA	PRIORITÄT	FRIST	STATUS
Offene Auditfindings	Kritisch	1 Monat	geschlossen
Reifegradaudit	Hoch	+3 Monate	bestanden
SiKo-Aktualisierung	Hoch	+5 Monate	aktuell
Pentest	Mittel	+5 Monate	getrackt

PROJEKT-TICKER | **Audit-Nachprüfung bestanden** → Reifegradaudit ohne offene Anmerkungen → Si

● geschlossen · bestanden ● in Beobachtung · getrackt ■ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP DES RISIKO-BOARDS

01 **Sichten** → 02 **Priorisieren** → 03 **Terminieren** → 04 **Zuweisen** → 05 **Schließen**

VOM DRUCK ZUR ORDNUNG

Aus vielen gleichzeitigen Anforderungen wurde ein nachvollziehbarer Plan, in dem jederzeit sichtbar war, was zuerst zählt, von der Sichtung bis zum geschlossenen Finding.

08 · ERGEBNIS + WIRKUNG

Jede Frist gehalten, jede Prüfung bestanden

1 Monat Frist

Kritische Auditauflagen fristgerecht geschlossen, Nachprüfung bestanden.

0 offene Anmerkungen

Internes Reifegradaudit erfolgreich abgeschlossen.

Nahtlos überbrückt

Kein Prozessstillstand, Projekt vom Kunden verlängert.

NACHHALTIGE WIRKUNG

Die Vakanz wurde nahtlos und hochprofessionell überbrückt, ohne dass Prozesse stagnierten oder Audits fehlschlugen. Das Sicherheitskonzept ist aktuell, die Pentest-Ergebnisse werden engmaschig getrackt. Die Zusammenarbeit lief so reibungslos, dass das Projekt verlängert wurde, bis eine interne Kraft gefunden ist.

09 · STIMME DES KUNDEN

> **Als die Schnittstelle zwischen physischer und Informationssicherheit plötzlich unbesetzt war, stand unter Zeitdruck viel auf dem Spiel. Dass wir die offenen Auditauflagen fristgerecht geschlossen und parallel Reifegradaudit und Pentest gemeistert haben, verdanken wir einem strukturierten, souveränen Vorgehen, das nie den Überblick verlor.**

Bereichsleitung Sicherheit, Institution im öffentlichen Sektor

10 · KEY ACHIEVEMENTS

Was bleibt

- ✓ Kritische Auditauflagen in der Ein-Monats-Frist geschlossen, Nachprüfung bestanden
- ✓ Internes Reifegradaudit erfolgreich begleitet, alle Anmerkungen geschlossen
- ✓ Sicherheitskonzept (SiKo) aktualisiert, Pentest durchgeführt und getrackt
- ✓ Schnittstelle physische + Informationssicherheit nahtlos überbrückt
- ✓ Alle Aufgaben transparent über ein Risiko-Board priorisiert und verfolgt
- ✓ Sicherheitsarchitektur angepasst und für den nächsten Zyklus vorbereitet
- ✓ Zusammenarbeit verlängert, bis eine interne Kraft gefunden ist

FAZIT · AUS DRUCK WIRD ORDNUNG

Eine unbesetzte Schlüsselrolle und mehrere Fristen zugleich wurden nicht mit Tempo, sondern mit Überblick und Priorisierung gemeistert.

WIE DER ADLER ÜBER DEM STURM

Die Behörde überstand ihre kritischste Phase souverän, ruhig kreisend über dem Geschehen, im richtigen Moment präzise zugreifend, ohne ein einziges Audit zu verlieren.

11 · FAZIT

Aus Druck wird Ordnung.

Eine plötzlich unbesetzte Schlüsselrolle, mehrere Fristen gleichzeitig, ein hochkomplexes KRITIS-Umfeld: Solche Situationen entscheiden sich nicht über Tempo, sondern über Überblick und Priorisierung, so hält strukturierte Sicherheitsexpertise auf Zeit den Betrieb stabil, bis die eigene Kraft wieder übernimmt.

AUSBLICK

Der nächste Zyklus mit neuem Pentest und Reifegradaudit ist bereits in Planung, die Sicherheitsarchitektur dafür vorbereitet.

ÜBERTRAGBAR

Das priorisierte Vorgehen nach BSI IT-Grundschutz lässt sich auf weitere Behörden und KRITIS-Einrichtungen übertragen.

ÜBER BASEC

Wie sicher ist Ihre Organisation wirklich?

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

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