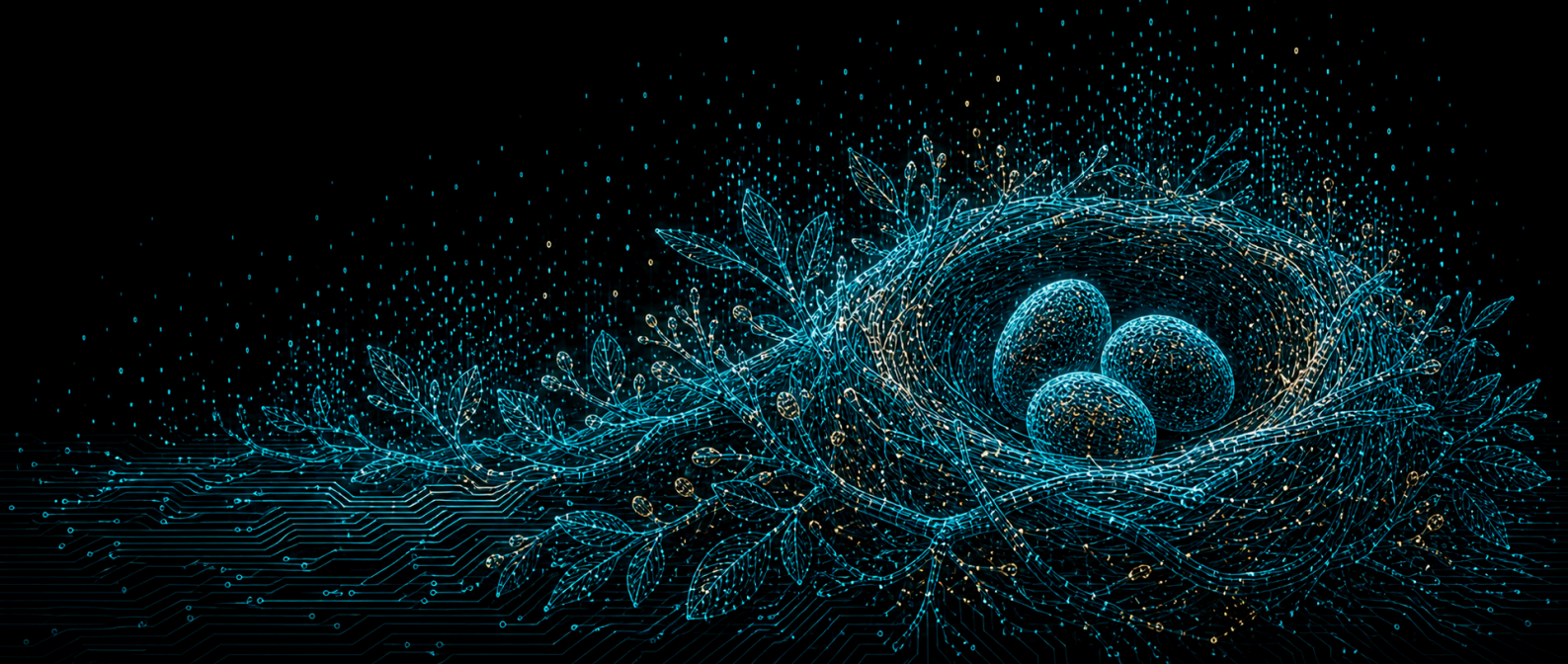
BASEC GMBH
BASECONSULTING
ISMS, BSI IT-GRUNDSCHUTZ

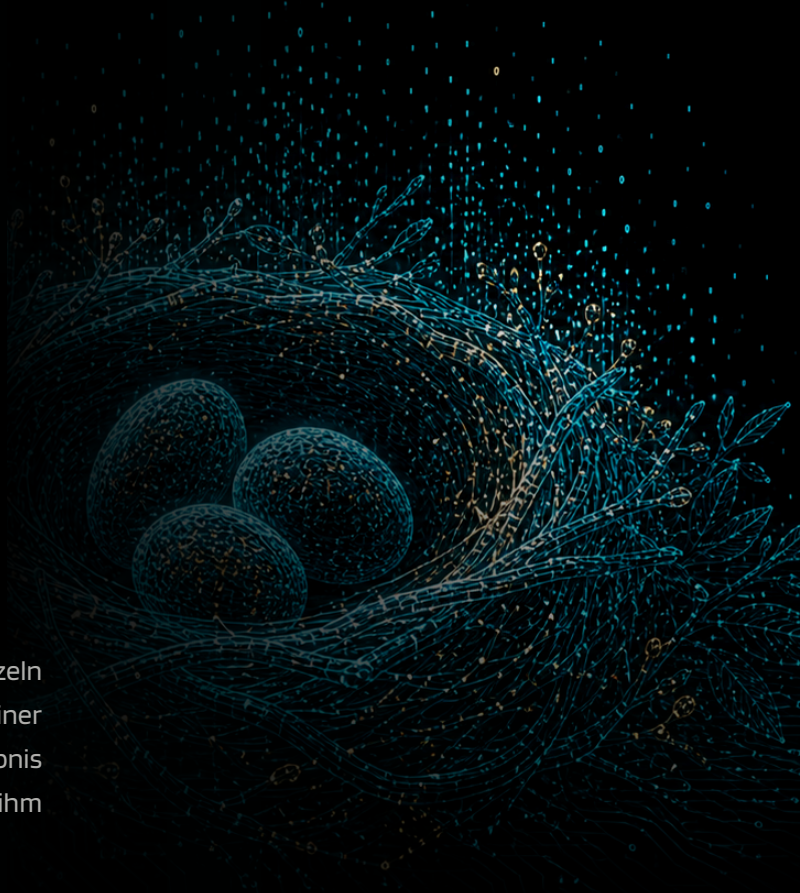
CASE STUDY · INFORMATION UND KOMMUNIKATION

Aus Gewachsenem eine tragende Struktur

Wie ein zentraler IT-Dienstleister der öffentlichen Verwaltung seine Sicherheitsarchitektur standardisiert, den Engpass an Security-Architekten auflöst und den BSI IT-Grundschutz dauerhaft nachweisbar hält.

„Ein Nest besteht aus tausenden losen Zweigen. Erst die Bauordnung macht daraus eine Struktur, die trägt."





ZUM GELEIT

Das Prinzip der gebauten Ordnung

Ein Vogel sammelt Zweige, Halme und Fasern, die einzeln nichts tragen. Er legt sie nicht ab, er verwebt sie, nach einer Ordnung, die über Generationen erprobt ist. Das Ergebnis hält Wind, Regen und Gewicht aus und schützt, was in ihm liegt.

Gewachsene IT-Landschaften entstehen anders. Sie sammeln über Jahre Systeme, Verfahren und Ausnahmen, ohne dass jemand die Bauordnung mitschreibt. Diese Case Study zeigt, wie aus vielen Einzelentscheidungen eine belastbare Sicherheitsarchitektur wurde, mit standardisierten Reviews, einer gemeinsamen Datenbasis und einem Grundschutz, der sich nachweisen lässt.

INHALT

01 · ÜBER DEN KUNDEN

Ein Dienstleister, an dem die Verwaltung hängt

Unser Kunde ist ein zentraler IT-Dienstleister der öffentlichen Verwaltung. Er betreibt eine sehr komplexe IT-Landschaft, in der Fachverfahren, Netze und Plattformen über Jahre gewachsen sind. Wenn dort ein Verfahren stillsteht, merken das nicht nur die Beschäftigten des Dienstleisters, sondern Bürgerinnen und Bürger an der Schnittstelle zur Verwaltung.

Die Informationssicherheit liegt beim CISO und seiner Stellvertretung. Beide haben das Projekt von Beginn an begleitet, fachlich und politisch. Das war ein wesentlicher Grund dafür, dass die Veränderungen nicht in der Architekturabteilung hängen blieben.

IT-Dienstleister | Öffentliche Verwaltung | BSI IT-Grundschutz | Sicherheitsarchitektur

KUNDENPROFIL

BRANCHE	Information + Kommunikation
ROLLE	Zentraler IT-Dienstleister der öffentlichen Verwaltung
IT-LANDSCHAFT	Hohe Verfahrensdichte, historisch gewachsen
AUFTRAGGEBER	CISO + Stellvertretung

BRANCHEN-KONTEXT

Ein zentraler Dienstleister bündelt Risiken. Was bei ihm ungeprüft freigegeben wird, wirkt in viele Behörden gleichzeitig, deshalb ist seine Architekturentscheidung nie nur eine technische.

02 · DER KONTEXT

Regulierung, die bis in die Architektur reicht

Die regulatorischen Vorgaben sind in den vergangenen Jahren deutlich strenger geworden, vor allem durch den BSI IT-Grundschutz. Der verlangt keine Absichtserklärung, sondern eine nachvollziehbare Kette: Welches Verfahren steht auf welcher Infrastruktur, welche Bausteine gelten dafür, wer hat die Umsetzung geprüft?

Genau an dieser Kette wurde sichtbar, dass IT-Architektur und Informationssicherheit zu weit voneinander entfernt arbeiteten. Architekturentscheidungen fielen dort, wo die technische Notwendigkeit saß. Die Sicherheitsbewertung kam später, manchmal zu spät. In einer gewachsenen Infrastruktur summiert sich das schnell: Am Ende weiß niemand mehr verlässlich, wo die relevanten Risiken liegen.

01

Verzahnt

IT-Architektur und Informationssicherheit mussten näher zusammenrücken.

02

Gewachsen

Historische Infrastruktur, hohe Verfahrensdichte, wenig dokumentierte Bauordnung.

03

Verpflichtend

BSI IT-Grundschutz als prüfbarer Maßstab, nicht als Empfehlung.

▪ verzahnt · gewachsen · verpflichtend ▪

WORAN GEMESSEN WIRD

Der Grundschutz fragt nicht, ob eine Entscheidung gut gemeint war. Er fragt, ob sie dokumentiert, begründet und geprüft ist.

03 · DER SCHMERZPUNKT

Zu viele Verfahren, zu wenige Architekten

Vor unserer Unterstützung liefen die Prozesse für Architekturanfragen weitgehend **manuell**. Jede Anfrage wurde einzeln bewertet, oft von unterschiedlichen Personen, ohne gemeinsames Prüfraster. Das Ergebnis waren uneinheitliche Entscheidungen: Zwei fachlich vergleichbare Anträge konnten unterschiedlich ausgehen, je nachdem, wer sie bearbeitete.

Dazu kam ein struktureller Engpass. Der Vielzahl an IT-Systemen und Verfahren stand ein Team mit zu wenigen IT-Security-Architekten gegenüber. Compliance-Lücken drohten, und unkoordinierte Netzwerkfreigaben stellten die Integrität des Technologie-Stacks infrage.

DAS KERNRISIKO

Uneinheitlich bewertete Architektur und unkoordinierte Freigaben erzeugen Risiken, die im Betrieb unsichtbar bleiben, bis sie im Audit oder im Vorfall sichtbar werden. Eine einzelne Firewall-Regel, die niemand mehr begründen kann, ist genau die Art von Altlast, die später keiner anfassen will.

BRANCHEN-INSIGHT · BSI IT-GRUNDSCHUTZ

111

Bausteine umfasst das BSI IT-Grundschutz-Kompendium (Edition 2023) auf rund 1.500 Seiten. Jede Architekturentscheidung muss den dafür relevanten Bausteinen standhalten.

92 %

der in Deutschland befragten Fachkräfte berichten laut ISC²-Studie 2025 von mindestens einem Sicherheitsvorfall, der auf Kompetenzdefizite zurückging. Solche Engpässe sind kein Einzelfall, sondern der Normalzustand.

04 · DIE ZIELSETZUNG

Entscheidungen, die wiederholbar sind

Das Zielbild war nicht, mehr zu entscheiden, sondern gleich zu entscheiden. Vier Leitziele gaben die Richtung vor.

01
Handlungsfähig
Genug qualifizierte Kapazität, um Architekturanfragen ohne Rückstau zu bearbeiten.

02
Standardisiert
Ein einheitliches Prüfraster für Architektur-Reviews, unabhängig von der Person.

03
Zusammengeführt
Eine gemeinsame Datenbasis für Schwachstellen, Vorfälle und Architekturbewertungen.

04
Nachweisbar
Konformität mit dem BSI IT-Grundschutz laufend belegbar, nicht nachträglich rekonstruiert.

AUS ZIELEN WIRD EIN WEG

01 Handlungsfähig → 02 Standardisiert → 03 Zusammengeführt → 04 Nachweisbar

05 · UNSER ANSATZ

Erst die Bauordnung, dann der Ausbau

Wir haben zuerst das Team verstärkt. Nicht als Dauerlösung, sondern um den Rückstau abzubauen und gleichzeitig Raum für die eigentliche Arbeit zu schaffen: die Bauordnung aufzuschreiben, nach der künftig entschieden wird. Unsere IT-Security-Architekten haben mitgearbeitet und dabei standardisierte Architektur-Reviews eingeführt, aufgebaut auf den bewährten TOGAF®-Prinzipien.

◆ Methodik · TOGAF®-Prinzipien + BSI IT-Grundschutz

WARUM EIN FESTES RASTER

Ein Review nach festem Raster macht Entscheidungen begründbar. Wer eine Freigabe verweigert, kann zeigen, an welchem Kriterium sie scheitert. Wer eine erteilt, hinterlässt eine **Spur, die im Audit trägt**.

KAPAZITÄT UND STRUKTUR, GLEICHZEITIG

A Kapazität

B Prüfraster

C Datenbasis

→

ERGEBNIS

Eine Architekturfunktion, die trägt

UNSER PRINZIP

Kapazität löst den Rückstau. Struktur verhindert, dass er zurückkommt.

06 · DIE UMSETZUNG

In fünf Schritten von der Anfrage zur Freigabe

01 Team verstärkt — Rückstau abgebaut

Kompetente IT-Security-Experten übernahmen laufende Architekturanfragen und schufen so den Freiraum für den Aufbau der Standards.

02 Architektur-Reviews standardisiert — einheitliche Entscheidungen

Ein festes Prüfraster auf Basis der TOGAF®-Prinzipien, für jede Anfrage derselbe Weg.

03 Security-Plattform aufgebaut — eine Datenbasis

Schwachstellenmanagement nach OWASP und FIRST, Sicherheitsvorfälle und Architekturbewertungen laufen in einem Bild zusammen.

04 Freigaben koordiniert — Integrität des Stacks

Netzwerk- und Firewall-Freigaben wurden geordnet beantragt, bewertet und dokumentiert.

05 Grundschutz fortgeschrieben — laufend nachweisbar

Die Infrastruktur wurde kontinuierlich nach den BSI-IT-Grundschutz-Vorgaben geprüft und erweitert.

HÜRDE + LÖSUNG

Die hohe Verfahrensdichte ließ sich nicht wegorganisieren. Wir haben die Anforderungen der beteiligten Abteilungen harmonisiert, statt für jede Abteilung einen eigenen Weg zu bauen.

07 · DIE LÖSUNG

Eine Plattform, die alles an einen Ort bringt

Der Kern der Lösung wirkt sofort: eine **Security-Plattform**, die zusammenführt, was vorher in getrennten Werkzeugen lag. Schwachstellen aus dem Scanning, bewertet nach den gängigen Standards von OWASP und FIRST. Sicherheitsvorfälle aus dem Betrieb. Ergebnisse der Architektur-Reviews. Offene und erteilte Netzwerkfreigaben. Erst in dieser Zusammenschau entsteht die Frage, die vorher niemand beantworten konnte: Welches Risiko ist heute das wichtigste?

SECURITY-PLATTFORM · DATENQUELLEN — ● Konsolidiert

BEREICH	GRUNDLAGE	TAKT	STATUS
Schwachstellen	OWASP + FIRST	laufend	● konsolidiert
Sicherheitsvorfälle	Betrieb	laufend	● konsolidiert
Architektur-Reviews	TOGAF®-Raster	je Anfrage	● standardisiert
Netz-Freigaben	Antragsprozess	je Antrag	● koordiniert
Grundschutz-Bausteine	BSI-Kompendium	zyklisch	● laufend

PROJEKT-TICKER | Anfrage standardisiert → **Risiko bewertet** → Freigabe dokumentiert → **Grund**

● im Regelbetrieb ● laufende Fortschreibung ▪ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP

01 **Verstärken** → 02 **Standardisieren** → 03 **Zusammenführen** → 04 **Koordinieren** → 05 **Nachweisen**

AUS VIELEN WERKZEUGEN EIN BILD

Ohne gemeinsames Bild wird nach Lautstärke priorisiert. Mit gemeinsamem Bild nach Wirkung. Aus vielen Einzelentscheidungen wurde ein Verfahren.

08 · ERGEBNIS + WIRKUNG

Handlungsfähig, und zwar dauerhaft

Engpass gelöst

Der Kunde verfügt über die nötigen Kapazitäten, um Architekturaufgaben effizient und professionell abzuarbeiten.

Zeit gewonnen

Architekturanfragen durchlaufen einen standardisierten Weg und sind dadurch deutlich schneller entschieden.

Niveau gehalten

Plattform und Grundschutz-Konformität stabilisieren das Sicherheitsniveau dauerhaft.

NACHHALTIGE WIRKUNG

Die Arbeitslast ist im Team nachhaltig verteilt, statt an einzelnen Personen zu hängen. Entscheidungen sind reproduzierbar, Freigaben nachvollziehbar, der Grundschutz laufend belegbar. Der Dienstleister kann heute Anfragen aus vielen Abteilungen bearbeiten, ohne dass jede einzelne zur Grundsatzdiskussion wird.

09 · FACHLICHE EINORDNUNG

> **Ein Engpass an Architekten ist selten nur ein Personalproblem. Er ist ein Strukturproblem, das sich als Personalproblem zeigt. Wer nur Köpfe nachlegt, kauft Zeit. Wer gleichzeitig das Prüfraster standardisiert und die Daten zusammenführt, verändert, wie eine Organisation entscheidet, und das hält, wenn die externe Unterstützung endet.**

Andreas Dietrich · Director Cyber-Security · Basec GmbH

10 · KEY ACHIEVEMENTS

Was bleibt

- Team um qualifizierte IT-Security-Architekten verstärkt, Rückstau abgebaut
- Security-Plattform aufgebaut, die Schwachstellen, Vorfälle und Bewertungen zusammenführt
- Netzwerk- und Firewall-Freigaben geordnet koordiniert und dokumentiert
- Anforderungen mehrerer Abteilungen harmonisiert, hohe Verfahrensdichte bewältigt
- Standardisierte Architektur-Reviews auf Basis der TOGAF®-Prinzipien eingeführt
- Schwachstellenbewertung nach den Standards von OWASP und FIRST verankert
- Infrastruktur laufend nach BSI IT-Grundschutz geprüft und erweitert
- Arbeitslast im Team nachhaltig verteilt, Sicherheitsniveau dauerhaft stabilisiert

FAZIT · AUS EINZELFÄLLEN EIN VERFAHREN

Aus verstreuten Werkzeugen und Einzelfallentscheidungen wurde ein Verfahren, das trägt.

WIE DAS NEST IM GEÄST

Nicht das einzelne Material entscheidet, sondern die Ordnung, in die es eingebaut wird.

11 · FAZIT

Struktur ist die längere Antwort.

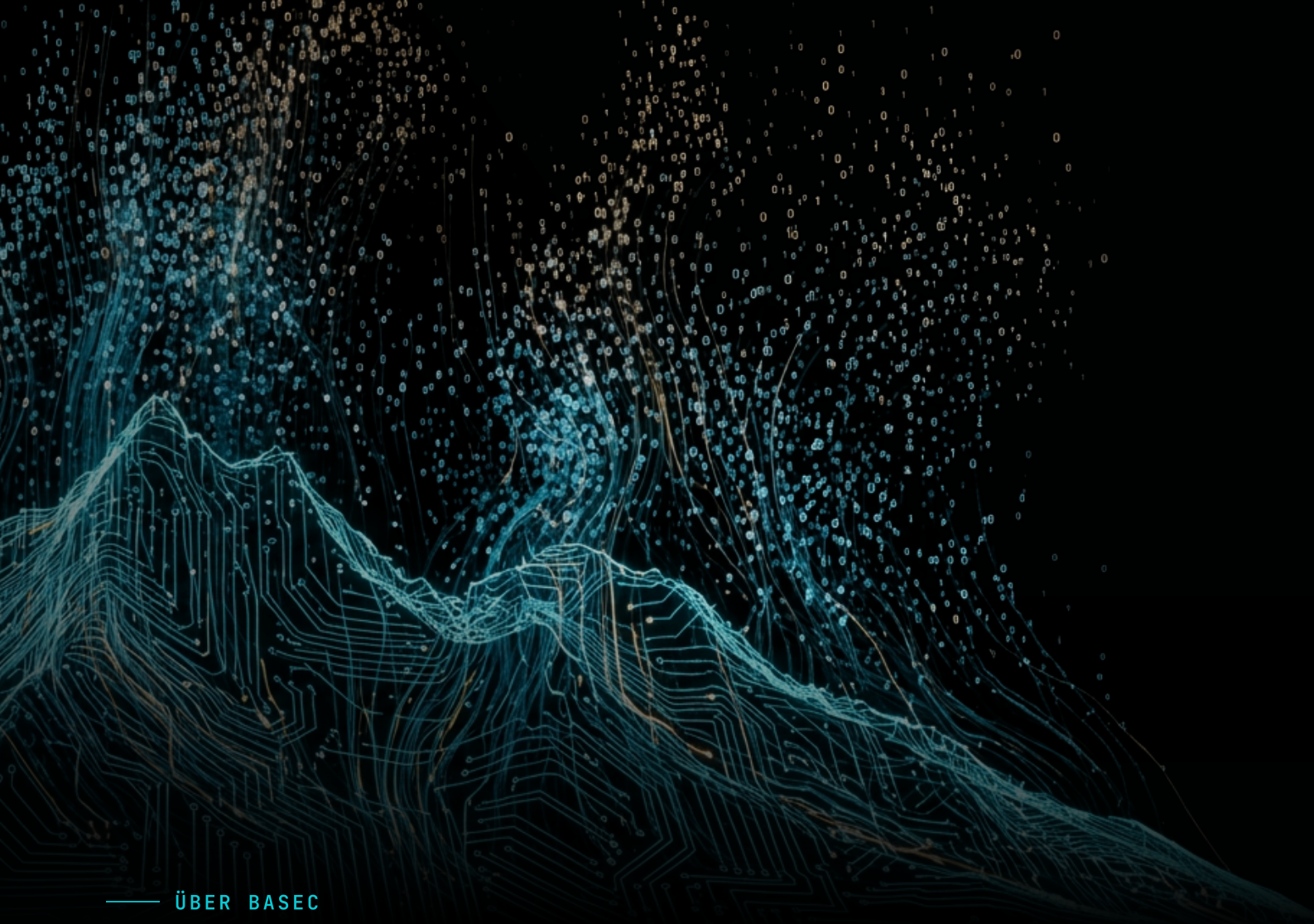
Personalengpässe lassen sich mit Kapazität überbrücken. Uneinheitliche Entscheidungen lassen sich damit nicht heilen. Erst als Prüfraster, Datenbasis und Freigabeprozess zusammenkamen, wurde aus einer entlasteten Abteilung eine Architekturfunktion, die den Grundschutz aus eigener Kraft nachweisen kann.

AUSBLICK

Die Reviews laufen im Standardbetrieb, die Plattform wächst mit den Verfahren. Die Fortschreibung des Grundschutzes ist Routine geworden.

ÜBERTRAGBAR

Der Ansatz aus standardisierten Reviews, konsolidierter Datenbasis und koordinierten Freigaben lässt sich auf andere Dienstleister mit hoher Verfahrensdichte 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 und BSI IT-Grundschutz**.

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.