

— CASE STUDY · INFORMATION UND KOMMUNIKATION

Aus vielen Fäden ein tragendes Netz

Wie ein IT-Dienstleister der öffentlichen Hand alle vertraglich geforderten Sicherheitskonzepte nach BSI IT-Grundsatz erstellt, arbeitsteilig, unter Zeitdruck, und zehn Tage vor der Frist übergibt.

„Ein Pilzmyzel verbindet auf kilometerweiten Flächen, was einzeln verstreut liegt, und macht aus vielen Wurzeln ein einziges, tragendes Netz.“



— ZUM GELEIT

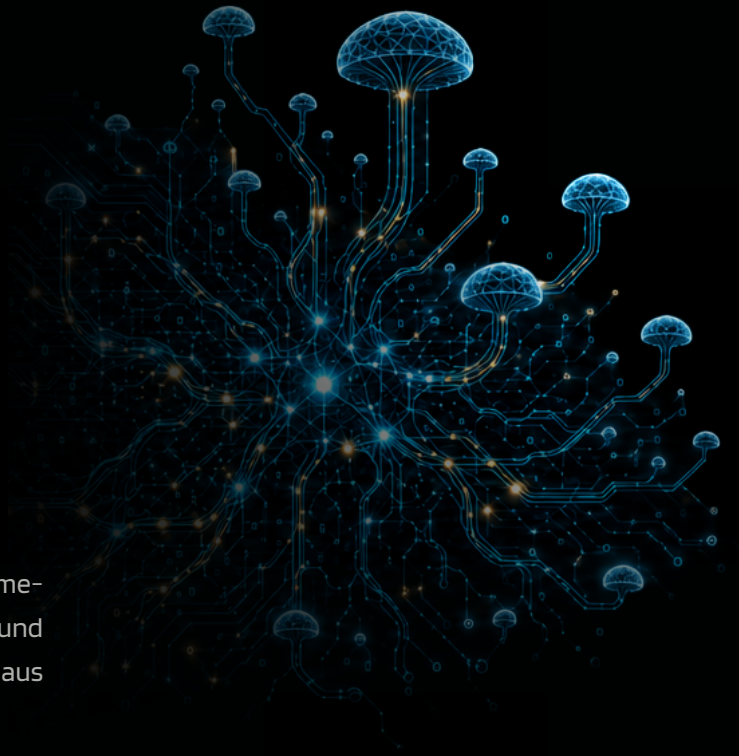
Das Prinzip des tragenden Netzes

Unter dem Waldboden verbindet ein Pilzmyzel auf kilometerweiten Flächen Bäume und Pflanzen. Es sammelt und verteilt, tauscht Nährstoffe und Warnungen, und macht aus vielen einzelnen Wurzeln ein einziges, tragendes Netz.

Genau das braucht ein belastbares Sicherheitskonzept: Informationen, die über viele Systeme verstreut liegen, müssen zusammengeführt werden, bis ein lückenloses Bild entsteht. Diese Case Study zeigt, wie aus fragmentierten Daten und einem knappen Zeitfenster vollständige, fristgerechte Konzepte wurden.

— INHALT

- 01 Der Kunde
- 02 Ausgangslage
- 03 Die Herausforderung
- 04 Zielbild
- 05 Unser Ansatz
- 06 Umsetzung
- 07 Die Lösung · Konzept-Board
- 08 Ergebnis + Wirkung
- 09 Stimme des Kunden
- 10 Erfolge · Fazit · Kontakt



01 · ÜBER DEN KUNDEN

Ein Dienstleister, auf den sich die öffentliche Hand verlässt

Unser Kunde ist ein IT-Dienstleister der öffentlichen Hand mit mehreren tausend Mitarbeitenden. Gegenüber seinen öffentlichen Auftraggebern unterliegt er einer strengen vertraglichen Verpflichtung: detaillierte Sicherheitskonzepte (SiKos) nach BSI IT-Grundschutz zu erstellen und kontinuierlich aktuell zu halten.

Diese Konzepte sind kein Selbstzweck. Sie weisen nach, dass die individuelle Infrastruktur jedes Endkunden den Anforderungen des IT-Grundschutzes entspricht, und sie müssen strikt den vorgegebenen Vorlagen folgen.

IT-Dienstleister

Öffentliche Hand

BSI IT-Grundschutz

SiKo

KUNDENPROFIL

BRANCHE	Information + Kommunikation
GRÖSSE	Mehrere tausend Mitarbeitende
AUFTRAG	SiKo nach BSI IT-Grundschutz
VERPFLICHTUNG	Vertraglich, öffentliche Hand

BRANCHEN-KONTEXT

Als Dienstleister für die öffentliche Hand steht der Kunde in der Lieferkette kritischer Verwaltungsprozesse, seine Sicherheitsnachweise sind Voraussetzung dafür, dass Behörden ihre Aufgaben verlässlich erfüllen können.

02 · DER KONTEXT

Ein Auftrag, der keine Verzögerung *verträgt*

Der Auslöser war konkret: Akute Personalengpässe und ein bereits entstandener zeitlicher Verzug machten externe Unterstützung zwingend erforderlich, um die vertraglichen Fristen überhaupt noch einhalten zu können. Erschwerend kam hinzu, dass jedes Konzept die individuelle Infrastruktur des jeweiligen Endkunden exakt widerspiegeln musste, kein Konzept glich dem anderen.

01

Verpflichtet

Vertragliche SiKo-Pflicht nach BSI IT-Grundsatz gegenüber der öffentlichen Hand.

02

Verzögert

Personalengpass und bereits entstandener zeitlicher Verzug.

03

Verstreut

Benötigte Informationen fragmentiert über viele Plattformen.

■ verpflichtet · verzögert · verstreut ■

KEIN KONZEPT WIE DAS ANDERE

Die Konzepte mussten strikt nach vorgegebenen Vorlagen auf Basis des BSI IT-Grundsatzes erstellt werden, jedes eine eigene, individuelle Ausarbeitung.

03 • DER SCHMERZPUNKT

Zwei Monate, viele Quellen, ein Feiertagsfenster

Die absolute Deadline für die Erstellung und Übergabe der Konzepte betrug lediglich **zwei Monate**. Gleichzeitig waren die benötigten Informationen stark fragmentiert und über verschiedene Plattformen verstreut, jeder Baustein musste aus mehreren Quellen zusammengetragen werden.

Zusätzlich fielen die zwingend notwendigen Abstimmungstermine mit dem internen Sicherheitsbereich, zur Klärung spezifischer BSI-IT-Grundschatzbausteine, genau in die kritische Zeit kurz vor den Feiertagen.

DAS KERNRISIKO

Ohne fristgerechte Lieferung drohte die Nichterfüllung vertraglicher Verpflichtungen gegenüber den öffentlichen Auftraggebern, mit möglichen Vertragsstrafen und einem erheblichen Vertrauensverlust.

BRANCHEN-INSIGHT • BSI IT-GRUNDSCHUTZ

111

Bausteine umfasst das BSI IT-Grundschatz-Kompodium (Edition 2023), auf rund 1.500 Seiten, jedes Konzept bildet die relevanten davon ab.

~120.000

Cybersecurity-Fachkräfte fehlen laut ISC²-Studie 2024 in Deutschland, Engpässe wie dieser sind die Regel.

04 • DIE ZIELSETZUNG

Vollständig, fristgerecht, ohne Qualitätsverlust

Das Zielbild ließ keine Kompromisse bei der Qualität zu, wohl aber beim Weg dorthin. Vier Leitziele gaben die Richtung vor.

01

Zusammenführen

Die verstreuten Informationen aus allen Plattformen zu einem vollständigen Bild aggregieren.

02

Normkonform

Jedes Konzept strikt nach Vorlage und BSI IT-Grundschutz erstellen.

03

Individuell

Die spezifische Infrastruktur jedes Endkunden exakt abbilden.

04

Fristgerecht

Alle Konzepte innerhalb des Zwei-Monats-Fensters liefern.

AUS ZIELEN WIRD EIN WEG

01

Zusammenführen

02

Normkonform

03

Individuell

04

Fristgerecht

05 · UNSER ANSATZ

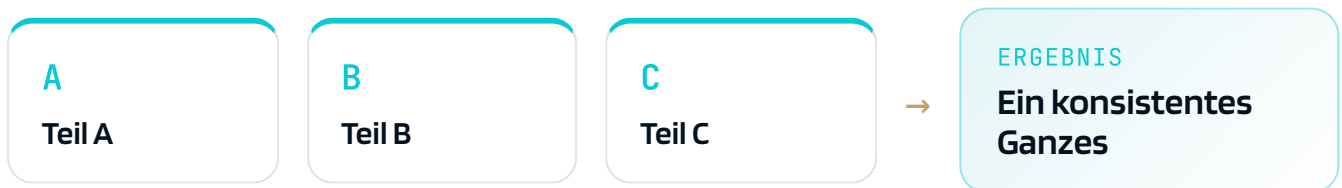
Viele Hände, ein zusammenhängendes Netz

Wie ein Myzel, das viele Wurzeln zu einem Netz verbindet, wählten wir einen stark arbeitsteiligen, parallelen Ansatz mit hohem persönlichem Einsatz. Um das enge Zeitfenster zu halten, wurden die zu erstellenden Sicherheitskonzepte strategisch auf die Basec-Berater aufgeteilt, jede und jeder übernahm einen klar umrissenen Teil.

◆ Methodik · Arbeitsteilung + BSI IT-Grundschutz

GETEILT, ABER VERBUNDEN

Die einzelnen Teile durften nicht auseinanderdriften. Über enge Abstimmung blieb jederzeit sichtbar, wie sie zusammengehören, damit am Ende ein **lückenloses, konsistentes Ganzes** entsteht.

AUFGETEILT, DANN ZUSAMMENGEFÜHRT**UNSER PRINZIP**

Geteilte Arbeit, geteiltes Wissen: Wer parallel arbeitet, aber eng verbunden bleibt, wird schnell, ohne dass die Konzepte auseinanderfallen.

06 • DIE UMSETZUNG

In vier Schritten vom Fragment zum Konzept

01 Informationsbeschaffung

Aggregation der über verschiedene Plattformen verstreuten Daten zu einer belastbaren Grundlage.

vollständige Datenbasis

02 Kollaboration

Gemeinsame Besprechung und Bearbeitung der zentralen Infrastruktur-Komponenten in engen Sessions mit dem internen Sicherheitsbereich.

BSI-Bausteine geklärt

03 Dezentrale Ausarbeitung

Die spezifischen, dezentralen Kundenkomponenten wurden von den Beratern individuell ausgearbeitet und in die Konzepte integriert.

Konzepte je Endkunde

04 Finalisierung + Übergabe

Zusammenführung aller Konzepte zu einem konsistenten Ganzen, bereit zur internen Prüfung und Einreichung.

fristgerechte Übergabe

HÜRDE + LÖSUNG

Die terminliche Enge kurz vor den Feiertagen gefährdete die Informationsbeschaffung massiv. Kompensiert durch Flexibilität und bewussten Mehraufwand der Berater, sodass alle BSI-Bausteine rechtzeitig geklärt wurden.

Ein Board, das alle Konzepte zusammenhält

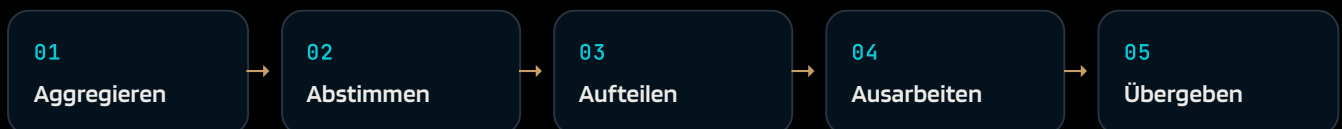
Kern der Lösung war ein gemeinsames **Überblicksbild**: Welches Konzept ist wem zugeordnet, welche BSI-Bausteine sind geklärt, was ist bereits übergabereif? So arbeiteten alle Berater parallel, ohne den Zusammenhang zu verlieren.

SICHERHEITSKONZEPTE · STATUS			● Board-Status
KONZEPTBEREICH	ZUSTÄNDIG	FRIST	STATUS
Zentrale Infrastruktur	Team A	2 Monate	● Übergeben
Netzkomponenten	Team B	2 Monate	● Übergeben
Fachverfahren	Team C	2 Monate	● Übergeben
Endkunden-Systeme	Team D	2 Monate	● in Prüfung

PROJEKT-TICKER | Verstreute Daten aggregiert → BSI-Bausteine geklärt → Konzepte arbeitsteil

● Übergeben · abgeschlossen ● in Prüfung ■ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP DER ZUSAMMENARBEIT



AUS VIELEN TEILEN EIN GANZES

Aus fragmentierten Daten und parallel arbeitenden Händen wurde ein lückenloses, konsistentes Konzeptwerk, vollständig und fristgerecht übergeben.

Vollständig geliefert, vor der Frist

10 Tage früher

Alle Konzepte vor Ablauf der straffen Zwei-Monats-Frist übergeben.

100 % BSI-konform

Alle geforderten Sicherheitskonzepte nach BSI IT-Grundschutz vollständig erarbeitet.

Engpass abgefedert

Vertragliche Pflichten ohne Qualitätsverlust erfüllt.

NACHHALTIGE WIRKUNG

Alle geforderten Sicherheitskonzepte wurden vollständig erarbeitet und finalisiert. Der Kunde konnte die Dokumente intern prüfen und erfolgreich bei seinen öffentlichen Auftraggebern einreichen. Der Personalengpass wurde effektiv abgefedert, und der Dienstleister verfügt nun wieder über aktuelle, compliant Dokumentationen, ohne dass die Qualität gelitten hätte.

09 • STIMME DES KUNDEN

"

Als Personalengpässe unsere vertraglichen Fristen für die Sicherheitskonzepte gefährdeten, brauchten wir schnelle und verlässliche Unterstützung. Dass alle Konzepte nach BSI IT-Grundsatz vollständig und sogar vor der Frist vorlagen, hat uns geholfen, unsere Verpflichtungen ohne den geringsten Qualitätsverlust zu erfüllen.

Sicherheitsbereich, IT-Dienstleister der öffentlichen Hand

10 · KEY ACHIEVEMENTS

Was bleibt

- ✓ Alle geforderten Sicherheitskonzepte nach BSI IT-Grundschutz vollständig erarbeitet
- ✓ Übergabe zehn Tage vor Ablauf der straffen Zwei-Monats-Frist
- ✓ Verstreute Informationen aus vielen Plattformen zu vollständigen Konzepten zusammengeführt
- ✓ Individuelle Endkunden-Infrastruktur in jedem Konzept exakt abgebildet
- ✓ Kritische BSI-Bausteine trotz Feiertagsfenster rechtzeitig geklärt
- ✓ Personalengpass ohne Qualitätsverlust abgefedert
- ✓ Vertragliche Verpflichtungen gegenüber öffentlichen Auftraggebern erfüllt

FAZIT · AUS FRAGMENTEN WIRD EIN GANZES

Aus verstreuten Daten und parallel arbeitenden Händen wurden vollständige, konsistente Konzepte, fristgerecht und ohne Qualitätsverlust.

WIE DAS MYZEL IM WALDBODEN

Aus vielen einzelnen Wurzeln wird ein tragendes Netz, das verbindet, was einzeln verstreut liegt, bis ein Ganzes entsteht.

Aus Fragmenten wird ein Ganzes.

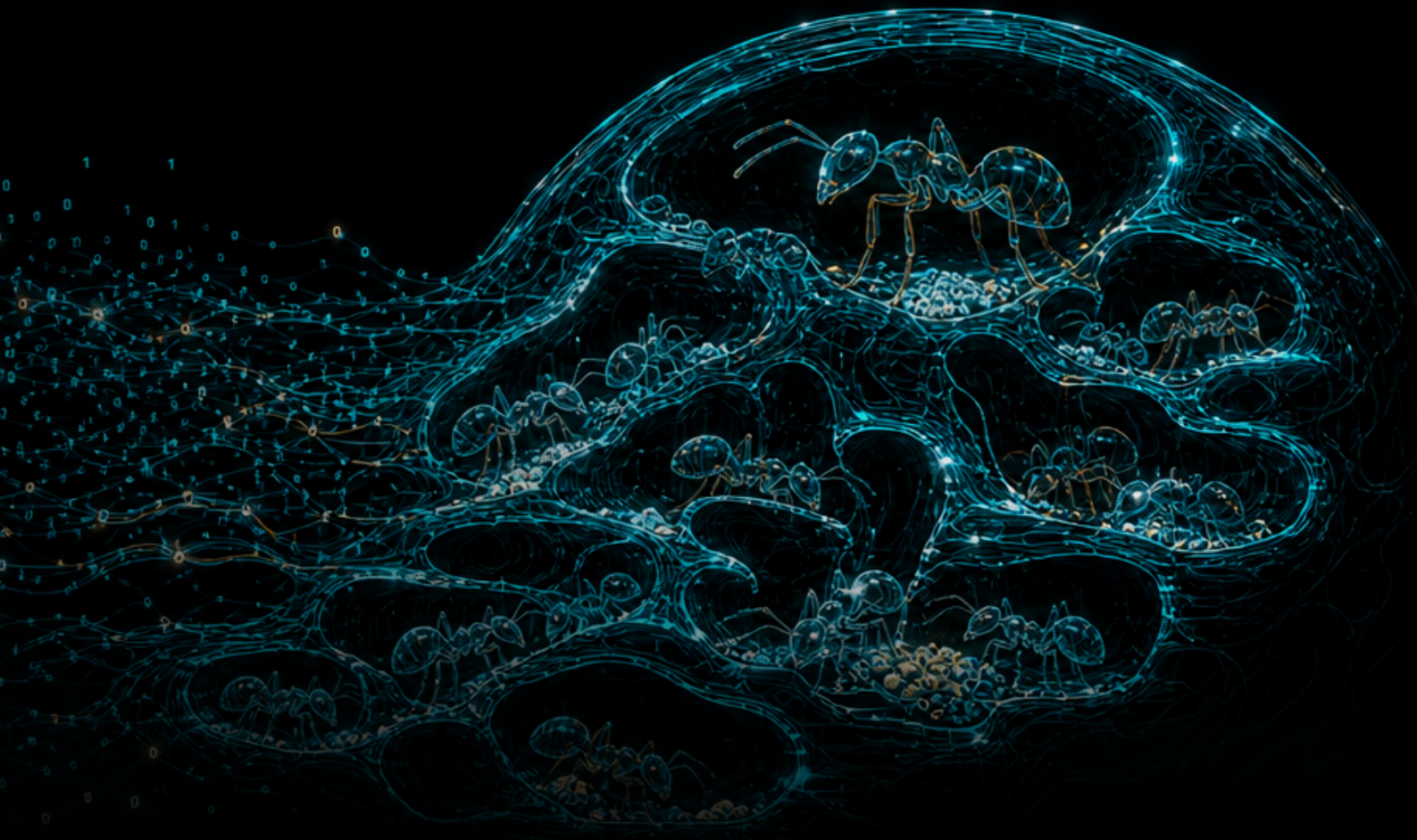
Verstreute Informationen, ein knappes Zeitfenster, kompromisslose Qualitätsanforderungen: Solche Aufgaben löst man nicht durch Tempo allein, sondern durch kluge Arbeitsteilung und enge Verbindung, so werden aus vielen Händen vollständige, fristgerechte Konzepte.

AUSBLICK

Die Dokumentationen sind wieder aktuell und compliant, eine belastbare Basis für die kontinuierliche Fortschreibung.

ÜBERTRAGBAR

Der arbeitsteilige Ansatz nach BSI IT-Grundschutz lässt sich auf weitere Konzeptwerke und Dienstleister der öffentlichen Hand 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, 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.