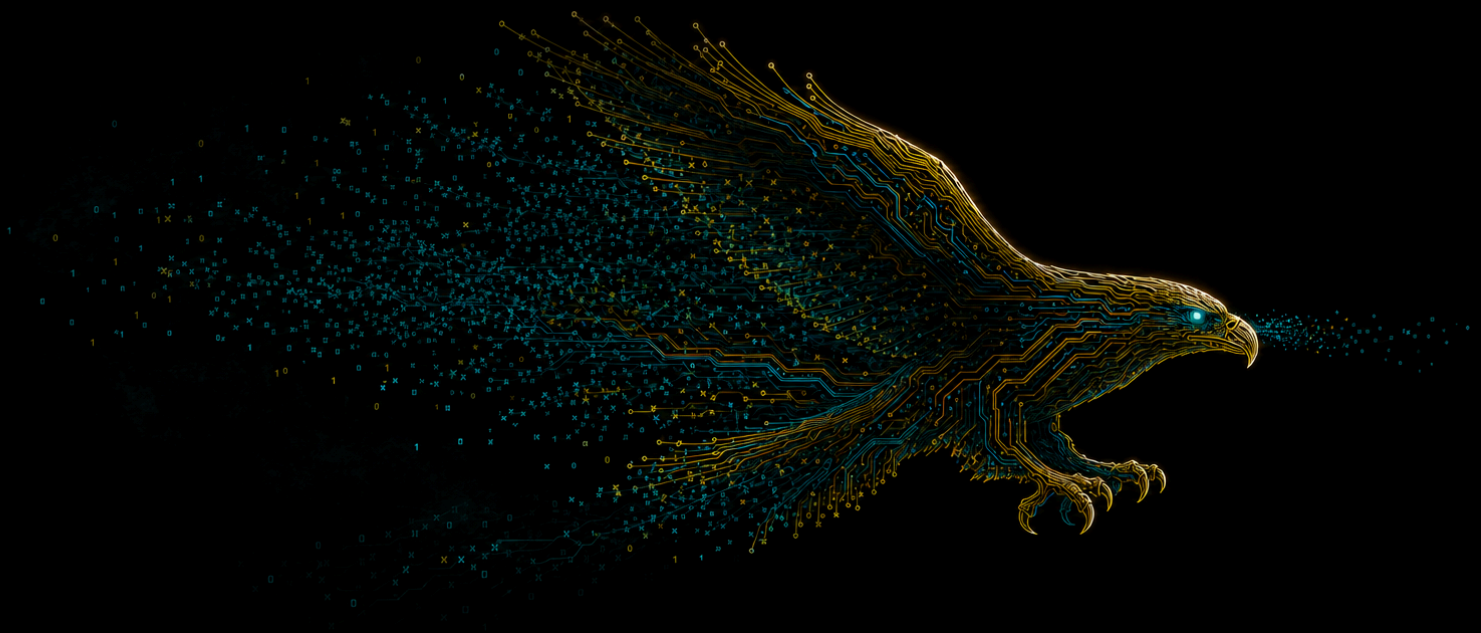
BASEC GMBH
BASECONSULTING
SCHWACHSTELLENMANAGEMENT

CASE STUDY · TRANSPORT

Sehen, bevor es jemand anders sieht

Wie ein Betreiber kritischer Verkehrsinfrastruktur ein strukturiertes Schwachstellenmanagement aufbaut, während er seine Betriebstechnik auf IP-basierte Vernetzung umstellt.

„Der Falke erkennt aus großer Höhe die kleinste Bewegung. Seine Stärke ist nicht das Tempo, sondern der Moment, in dem er sich entscheidet."



ZUM GELEIT

Das Prinzip des scharfen Blicks

Ein Falke jagt nicht durch Ausdauer. Er sitzt hoch, sieht weit und wartet, bis eine Bewegung im Feld wichtig genug ist. Dann greift er zu, gezielt, einmal. Alles andere zieht an ihm vorbei, ohne dass er Kraft verliert.

Schwachstellenmanagement funktioniert nach demselben Prinzip. Es gewinnt nicht, wer die längste Liste offener Findings führt, sondern wer erkennt, welche wenigen davon den Betrieb tatsächlich gefährden. Diese Case Study zeigt, wie ein Betreiber kritischer Verkehrsinfrastruktur diesen Blick aufgebaut hat, mitten in der Umstellung auf eine vernetzte Betriebstechnik.

INHALT

01 · ÜBER DEN KUNDEN

Ein Betreiber, auf dessen Verfügbarkeit sich ein Land verlässt

Unser Kunde ist ein Betreiber kritischer Verkehrsinfrastruktur mit mehreren zehntausend Mitarbeitenden. Er hält eine Infrastruktur in Betrieb, die täglich von sehr vielen Menschen genutzt wird, und digitalisiert sie gleichzeitig grundlegend.

Im Zentrum steht ein Programm, das die technologische Basis für die künftige vernetzte Betriebstechnik bildet. Diese Basis ist IP-basiert vernetzt. Damit erbt ein Bereich, der jahrzehntelang von der IT getrennt war, deren Bedrohungsmodell und braucht auch deren Schutzmechanismen.

KRITIS | IP-basierte Vernetzung | Schwachstellenmanagement | Hochreguliert

KUNDENPROFIL

BRANCHE	Transport + Verkehr (KRITIS)
GRÖSSE	Mehrere zehntausend Mitarbeitende
VORHABEN	Basis für vernetzte Betriebstechnik
RAHMEN	NIS2, ISO 27001, BSI IT-Grundschutz

BRANCHEN-KONTEXT

Verfügbarkeit ist in dieser Branche keine Kennzahl im Reporting, sondern die Betriebsgrundlage. Eine Sicherheitsmaßnahme, die den Betrieb behindert, wird nicht umgesetzt, sie muss also von Anfang an dazu passen.

02 · DER KONTEXT

Ein kritischer Bereich lernt das Internetprotokoll

Die Digitalisierung des Betriebs ist beschlossen, das Programm liefert dafür die technologische Grundlage. Mit der IP-basierten Vernetzung wächst die Bedeutung eines robusten Schwachstellenmanagements, und zwar schneller, als klassische Betriebsprozesse üblicherweise mitwachsen.

Der Anspruch war von Beginn an zweiseitig. Die technische Verfügbarkeit sollte auf höchstem Niveau garantiert bleiben. Gleichzeitig sollte die IT-Sicherheit proaktiv gesteuert werden, in einem hochkomplexen und stark regulierten Umfeld, in dem NIS2, ISO 27001 und der BSI IT-Grundschutz jeweils eigene Nachweise verlangen.

01

Vernetzt

IP-basierte Basis für die künftige Betriebstechnik.

02

Reguliert

NIS2, ISO 27001 und BSI IT-Grundschutz gleichzeitig im Blick.

03

Verfügbar

Höchste technische Verfügbarkeit als nicht verhandelbare Randbedingung.

■ vernetzt · reguliert · verfügbar ■

WAS PROAKTIV WIRKLICH HEISST

Die Lücke kennen, bevor jemand sie nutzt, und sie schließen können, ohne den Betrieb anzuhalten.

03 · DER SCHMERZPUNKT

Wachsende Komplexität, knappe Kapazität

Die Bedrohungslage entwickelt sich weiter, und sie tut es schneller als früher. **KI-gestützte Angriffsszenarien** senken den Aufwand für Angreifer und erhöhen damit die Anforderungen an die Verteidigung. Für das Team des Kunden bedeutete das zusätzliche Last bei knapp bemessenen personellen Ressourcen.

Parallel wuchs die Komplexität der IT-Landschaft. Mehr Komponenten, mehr Abhängigkeiten, mehr Schnittstellen. Genau in dieser Kombination geht der Überblick verloren: Man weiß, dass es Schwachstellen gibt, aber nicht mehr verlässlich, welche zuerst zählt.

DAS KERNRISIKO

Ohne belastbare Priorisierung arbeitet ein Team an den Findings, die zuerst gemeldet wurden, nicht an denen, die den größten Schaden verhindern. Die zentrale Herausforderung bestand darin, trotz begrenzter Kapazitäten eine ganzheitliche Kontrolle zu etablieren, die die Integrität der Infrastruktur jederzeit sicherstellt.

BRANCHEN-INSIGHT · KAPAZITÄT + PFLICHT

92 %

der in Deutschland befragten Fachkräfte berichten laut ISC²-Studie 2025 von mindestens einem Sicherheitsvorfall, der auf Kompetenzdefizite zurückging. Fehlende Kompetenz im Team ist keine Projektbesonderheit, sondern Rahmenbedingung.

KRITIS

Betreiber kritischer Infrastruktur tragen erhöhte Nachweispflichten. Für sie ist Schwachstellenmanagement eine regulatorische Anforderung, keine Ermessensfrage.

04 · DIE ZIELSETZUNG

Kontrolle, die ohne zusätzliche Köpfe skaliert

Mehr Personal war keine realistische Option. Das Zielbild musste also mit der vorhandenen Kapazität funktionieren. Vier Leitziele gaben die Richtung vor.

01
Bewertet
Die technologische Infrastruktur vollständig beurteilen, nicht stichprobenhaft.

02
Geregelt
Verbindliche IT-Richtlinien für sicherheitsrelevante und netzwerktechnische Bereiche.

03
Reduziert
Erkannte Risiken gezielt mindern, Fehler aus den Testphasen systematisch beheben.

04
Dokumentiert
Komponenten lückenlos dokumentieren, Auslieferung standardisieren.

AUS ZIELEN WIRD EIN WEG

01 **Bewertet** → 02 **Geregelt** → 03 **Reduziert** → 04 **Dokumentiert**

05 · UNSER ANSATZ

Erst bewerten, dann zugreifen

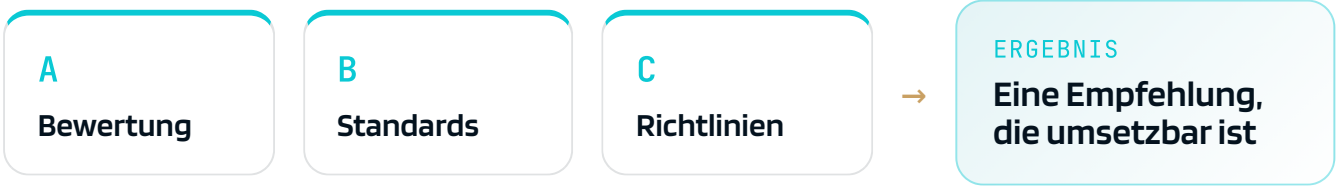
Wir haben nicht mit Maßnahmen angefangen, sondern mit einer umfassenden Bewertung der technologischen Infrastruktur. Erst wenn klar ist, welche Komponenten in den Applikationen stecken, welche Version läuft und welche Anforderung dafür gilt, lässt sich eine Empfehlung geben, die auch trägt.

◆ Methodik · Bewertung + Richtlinien + Risikominderung

ZWEI REGELWERKE GLEICHZEITIG

Die Empfehlungen waren sowohl auf die aktuellen Sicherheitsstandards als auch auf die **spezifischen Unternehmensrichtlinien** abgestimmt. Der zweite Punkt ist der undankbarere: Eine Empfehlung, die im Standard vorbildlich ist, aber gegen die interne Richtlinie läuft, verbrennt Zeit und Vertrauen.

VOM BEFUND ZUR BELASTBAREN EMPFEHLUNG



UNSER PRINZIP

Wer alles gleich wichtig behandelt, behandelt nichts wichtig. Priorisierung ist die eigentliche Leistung im Schwachstellenmanagement.

06 · DIE UMSETZUNG

In fünf Schritten vom Befund zum Regelbetrieb

01 Infrastruktur bewertet — belastbares Lagebild

Umfassende Beurteilung der technologischen Infrastruktur als Grundlage für jede weitere Entscheidung.

02 Komponenten empfohlen — standard- + richtlinienkonform

Fundierte Empfehlungen für die technischen Komponenten innerhalb der Applikationen.

03 IT-Richtlinien entwickelt — klarer Handlungsrahmen

Richtlinien für sicherheitsrelevante und netzwerktechnische Bereiche, entwickelt und implementiert.

04 Risiken gemindert — Findings behoben

Systematische Behebung der Fehler aus den Testphasen, verbunden mit gezielter Risikominderung.

05 Dokumentation + Lieferpakete — Transparenz + Wartbarkeit

Lückenlose Dokumentation der technischen Komponenten und standardisierte Lieferpakete je Systemumgebung.

HÜRDE + LÖSUNG

Knappe personelle Ressourcen ließen sich nicht durch mehr Aufwand kompensieren. Standardisierte Lieferpakete und verbindliche Richtlinien haben die wiederkehrende Arbeit aus dem Einzelfall genommen.

07 · DIE LÖSUNG

Ein Board, das Priorität herstellt

Am Ende steht ein Verfahren, das jede Schwachstelle denselben Weg nimmt: **erfassen, bewerten, entscheiden, beheben, dokumentieren**. Das klingt selbstverständlich und ist es in einer hochkomplexen Landschaft gerade nicht, weil Befunde aus verschiedenen Quellen mit verschiedenen Maßstäben eintreffen.

SCHWACHSTELLEN-BOARD · VERFAHREN — Im Regelbetrieb

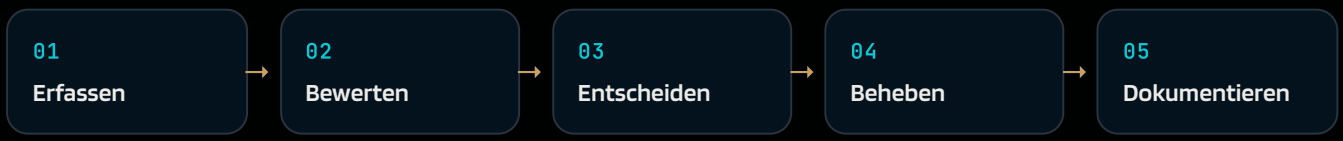
BEREICH	GRUNDLAGE	TAKT	STATUS
Komponentenbewertung	Standards + Richtlinien	je Release	etabliert
IT-Richtlinien	Sicherheit + Netztechnik	verbindlich	implementiert
Findings aus Tests	Testprotokolle	je Zyklus	behoben
Risikominderung	Bewertung + Priorität	laufend	gesteuert
Lieferpakete	Systemumgebungen	je Umgebung	standardisiert

PROJEKT-TICKER | Bewertet → **priorisiert** → behoben → dokumentiert → **als Lieferpaket über**

etabliert gesteuert

▪ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP



DER ENTSCHEIDUNGSPUNKT

Zwischen Bewertung und Behebung wird festgelegt, was sofort geschlossen, was terminiert und was bewusst als Restrisiko getragen wird. Diese Entscheidung ist dokumentiert und damit prüfbar, gegenüber dem Audit und gegenüber der eigenen Organisation.

08 · ERGEBNIS + WIRKUNG

Ein Verfahren, das den Überblick hält

Struktur etabliert

Der Kunde verfügt über ein effizientes und strukturiertes Schwachstellenmanagement.

Personen-unabhängig

Die Prozesse laufen unabhängig von einzelnen Personen weiter.

Nachweis gesichert

Compliance-Anforderungen und Bedrohungslage lassen sich mit denselben Prozessen bedienen.

NACHHALTIGE WIRKUNG

Der langfristige Mehrwert liegt in den etablierten Prozessen. Sie ermöglichen es dem Kunden, aktuellen Compliance-Anforderungen und einer dynamischen Bedrohungslage souverän zu begegnen. Die Dokumentation der Komponenten und die standardisierten Lieferpakete haben Transparenz und Wartbarkeit nachhaltig verbessert, auch für alles, was nach dem Projekt kommt.

09 · STIMME DES KUNDEN

> **Mit der IP-basierten Vernetzung ist die Sicherheitsfrage in einen Bereich gerückt, der bisher anders gedacht wurde. Wir brauchten kein weiteres Werkzeug, sondern ein Verfahren, das uns sagt, welche Lücke zuerst zählt. Genau das haben wir heute, und es läuft, ohne dass wir dafür zusätzliche Kapazität aufbauen mussten.**

Projektleitung, Betreiber kritischer Verkehrsinfrastruktur

10 · KEY ACHIEVEMENTS

Was bleibt

- Technologische Infrastruktur umfassend bewertet, belastbares Lagebild geschaffen
- Fundierte Empfehlungen für die technischen Komponenten der Applikationen
- Sicherheitsstandards und interne Unternehmensrichtlinien gemeinsam berücksichtigt
- IT-Richtlinien für sicherheitsrelevante und netzwerktechnische Bereiche implementiert
- Fehler aus den Testphasen systematisch behoben, Risiken gezielt gemindert
- Technische Komponenten lückenlos dokumentiert
- Standardisierte Lieferpakete je Systemumgebung etabliert
- Effizientes, strukturiertes Schwachstellenmanagement im Regelbetrieb

FAZIT · AUS BEFUNDEN WIRD STEUERUNG

Aus knapper Kapazität und wachsender Komplexität wurde ein Verfahren, das Priorität herstellt.

WIE DER FALKE ÜBER DEM FELD

Der Wert liegt im Blick, der das Wesentliche findet, und in der Ruhe, alles andere ziehen zu lassen.

11 · FAZIT

Der Blick entscheidet, nicht die Liste.

Kritische Infrastruktur wird nicht dadurch sicher, dass man jede Schwachstelle kennt, sondern dadurch, dass man die richtige zuerst schließt. Bewertung, verbindliche Richtlinien und dokumentierte Entscheidungen haben aus einem überlasteten Team eine Funktion gemacht, die ihre Landschaft steuert, statt ihr nachzulaufen.

AUSBLICK

Das Verfahren trägt die weitere Digitalisierung mit. Neue Komponenten laufen durch dieselbe Bewertung, neue Umgebungen durch dieselben Lieferpakete.

ÜBERTRAGBAR

Der Ansatz aus Bewertung, Richtlinien und standardisierter Dokumentation lässt sich auf andere KRITIS-Betreiber übertragen, die ihre Betriebstechnik auf IP-basierte Vernetzung umstellen.

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, Schwachstellenmanagement und ISMS**.

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