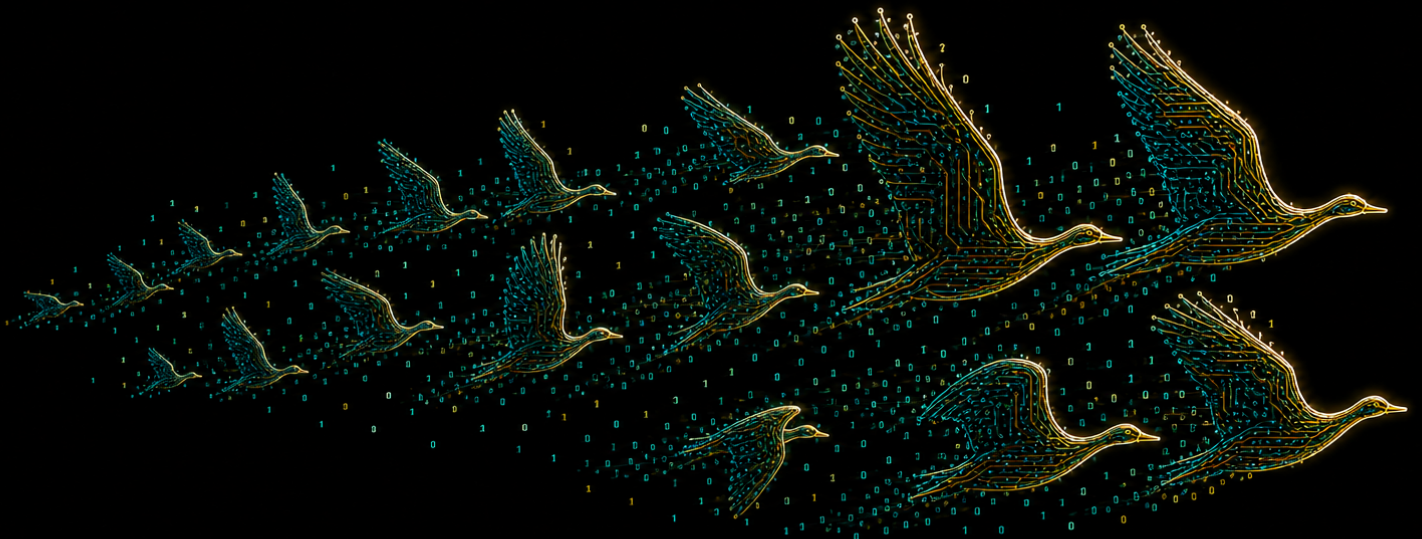


— CASE STUDY · TRANSPORT

Auf Kurs, auch im Gegenwind

Wie ein Transport- und Verkehrsunternehmen die Sicherheitsvorgaben für eine geschäftskritische Anwendung erfüllt, und das Projekt trotz halbiertem Budget und Team termingerecht ans Ziel bringt.

„Ein Zugvogel hält Kurs, auch wenn Sturm und Gegenwind ihn abzudrängen versuchen, er korrigiert früh und erreicht sein Ziel.“



— ZUM GELEIT

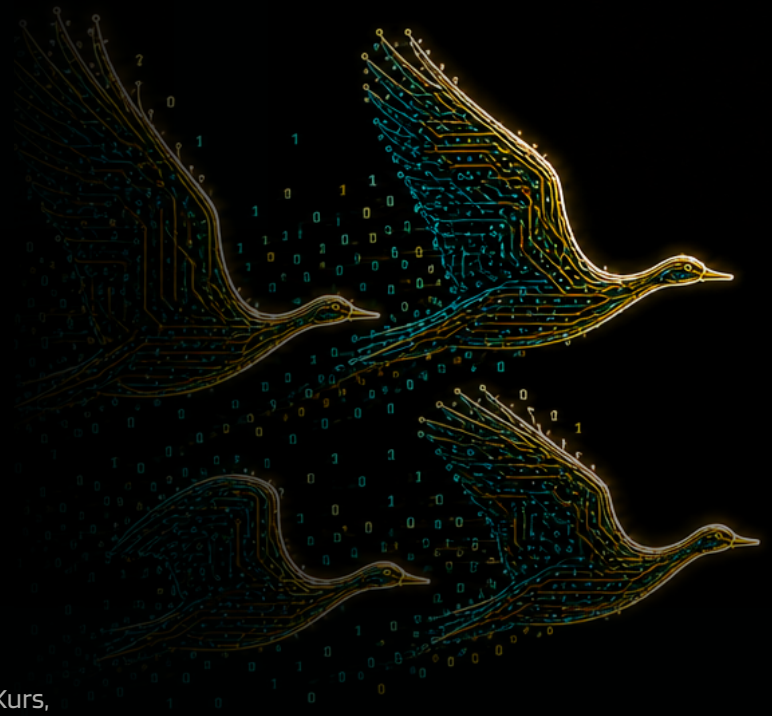
Das Prinzip vorausschauender Sicherheit

Ein Zugvogel hält über tausende Kilometer präzise Kurs, auch wenn Sturm und Gegenwind ihn abzudrängen versuchen. Er korrigiert früh, nutzt jede Strömung und erreicht sein Ziel, ohne die Richtung zu verlieren.

Genau darin liegt das Prinzip vorausschauender Sicherheit: Sicherheit ist kein Kurswechsel am Ende, sondern die Orientierung, die von Beginn an mitfliegt. Diese Case Study zeigt, wie ein Projekt unter härtestem Gegenwind, halbiertem Budget und halbiertem Team, auf Kurs blieb und sicher ans Ziel kam.

— INHALT

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



01 · ÜBER DEN KUNDEN

Ein Betreiber, dessen Software den Betrieb trägt

Unser Kunde ist ein großes Unternehmen im Transport- und Verkehrssektor, ein Betreiber kritischer Infrastruktur (KRITIS) mit mehreren zehntausend Mitarbeitenden. In einer Organisation dieser Größe entstehen laufend interne Anwendungen, die Entwicklungs- und Managementprozesse steuern.

Eine davon war ursprünglich als reine Kosteneinsparung gedacht: ein paar einfache Performanceberichte. Doch das Vorhaben wuchs, von einem kleinen Startprojekt zu einem zwölfköpfigen Team, und aus den Berichten wurde unbemerkt ein übergreifendes Performancemanagement-Tool für alle Entwicklungsprojekte.

KRITIS

Transport + Verkehr

SSDLC offen

NIS2

KUNDENPROFIL

BRANCHE	Transport + Verkehr · KRITIS
GRÖSSE	Mehrere zehntausend MA
AUSGANGSOBJEKT	Internes Performance-Tool
REIFEGRAD	100 % Funktion · Sicherheit offen

BRANCHEN-KONTEXT

Seit dem 6. Dezember 2025 gilt in Deutschland das NIS2-Umsetzungsgesetz ohne Übergangsfrist, auch für den Sektor Transport und Verkehr, mit klaren Pflichten bis in die Lieferkette und die eingesetzte Software hinein.

02 · DER KONTEXT

Aus einem Bericht wurde unbemerkt eine Applikation

Was als schlankes Reporting begann, war innerhalb eines Jahres zu einer vollwertigen Applikation geworden, genutzt zur Steuerung sämtlicher Entwicklungsprojekte. Damit änderte sich alles: Eine produktiv genutzte Anwendung dieser Tragweite muss zwingend Sicherheitsvorgaben und die Richtlinien für sichere Softwareentwicklung (SSDLC) erfüllen, genau das war bis dahin nicht im Fokus.

01

Gewachsen

Vom einfachen Bericht zum unternehmensweiten Steuerungstool für alle Entwicklungsprojekte.

02

Ungesichert

Fokus zu 100 % auf Funktionalität, Sicherheit und SSDLC bislang nicht berücksichtigt.

03

Produktivkritisch

Ohne Sicherheitsnachweise keine Freigabe für den Produktivbetrieb.

■ gewachsen · ungesichert · nicht produktionsreif ■

DER WENDEPUNKT

In dieser Phase kam unser Consultant ins Projekt: Bestehende Entwicklungen entsprachen nicht den Sicherheitsanforderungen und mussten neu betrachtet und angepasst werden.

03 · DER SCHMERZPUNKT

Sicherheit einbauen, ohne die Entwicklung anzuhalten

Die akute Herausforderung bestand darin, tief in einen laufenden Entwicklungsprozess einzugreifen, ohne dass die Entwicklung zum Erliegen kommt. Die Entwickler mussten den zwingenden Charakter der Sicherheitsanforderungen, **Control Self Assessment (CSA)** und SSDLC, nicht nur akzeptieren, sondern verstehen und umsetzen.

Mitten in dieser Phase kam die zweite, härtere Krise: eine plötzliche Halbierung des Budgets, bei laufender Entwicklung und offenen Sicherheitsanforderungen.

DAS KERNRISIKO

Ohne etablierten SSDLC hätte die Applikation die strengen internen Sicherheitsvorgaben nicht erfüllt und hätte nicht produktiv genommen werden dürfen. Der bisherige Aufwand wäre entwertet gewesen.

BRANCHEN-INSIGHT · BEDROHUNGSLAGE

10×

Ein erst in der Produktion entdeckter Sicherheitsmangel kostet um eine Größenordnung mehr als einer, der schon im Design behoben wird (Shift-Left-Prinzip).

~119 / Tag

neue Schwachstellen wurden laut BSI-Lagebericht 2025 täglich bekannt, ein Anstieg um 24 % gegenüber dem Vorjahr.

04 · DIE ZIELSETZUNG

Sicherheit, die von Anfang an mitfliegt

Das Zielbild war nicht, Sicherheit nachträglich aufzusetzen, sondern sie als festen Bestandteil der Entwicklung zu verankern, Security by Design. Vier Leitziele gaben den Kurs vor.

01

Verstehen

Bei den Entwicklern echtes Verständnis für CSA und SSDLC schaffen, statt Vorgaben nur zu verordnen.

02

Integrieren

Sicherheitsanforderungen in den laufenden Entwicklungsprozess einweben, ohne ihn zu stoppen.

03

Nachweisen

Alle Sicherheits-Assessments und Risikobewertungen belastbar dokumentieren, als Grundlage der Produktivfreigabe.

04

Befähigen

Das Team in die Lage versetzen, Sicherheit künftig eigenständig mitzudenken.

AUS ZIELEN WIRD EIN KURS

01

Verstehen

02

Integrieren

03

Nachweisen

04

Befähigen

05 · UNSER ANSATZ

Gemeinsam Kurs finden, statt Kurs *vorschreiben*

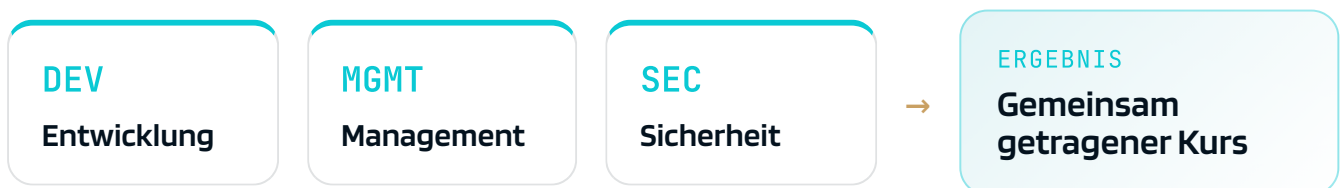
Wir wählten einen stark kommunikativen und pragmatischen Ansatz. In gemeinsamen Workshops betrachteten wir die Sicherheitsthemen direkt mit den Entwicklern, um die bestmöglichen Umsetzungswege zu finden. Das Ziel: den Prozess strikt einhalten, den Entwicklern aber genug Freiraum lassen, die Anforderungen praktikabel umzusetzen.

◆ Methodik · SSDLC + CSA

GEMEINSAM GEBAUT, NICHT VERORDNET

Aus einer aufgezwungenen Pflicht wurde ein gemeinsam getragener Kurs, entscheidend dafür, dass Sicherheit auch unter Zeitdruck nicht als **Bremse**, sondern als Teil der Entwicklung verstanden wurde.

DREI PERSPEKTIVEN, EIN KURS

**UNSER PRINZIP**

Sicherheit wird nicht über die Köpfe der Entwickler hinweg verordnet, sondern mit ihnen gebaut. Nur was verstanden ist, wird im Alltag auch gelebt.

06 · DIE UMSETZUNG

Kurs halten, auch als der Wind drehte

01 Bestandsaufnahme

Sichtung aller aktuellen Themen und Abgleich mit den CSA- und SSDLC-Vorgaben.

Lücken-Landkarte

02 Prozessintegration

Anpassung der Entwicklungsprozesse und Workshops zur Sensibilisierung des Teams.

gelebter Prozess

03 Krisenmanagement · Scope-Change

Nach der Budgethalbierung wurde das Projekt neu bewertet (ein Monat Verzögerung) und der Scope auf ein MVP reduziert: die ursprünglichen automatisierten Berichte.

Fokus auf MVP

04 Neustrukturierung

Das Projektteam wurde von zwölf auf fünf Personen verkleinert und die Projektleitung ausgetauscht.

schlagkräftiges Kernteam

05 Endspurt

In den verbleibenden zwei Monaten (statt der geplanten zehn) wurden alle Sicherheits-Assessments, die sichere Umsetzung und der komplette Sicherheitsprozess inklusive Risikobewertung auf den neuen Scope finalisiert.

sichere Freigabe

HÜRDE + LÖSUNG

Budget und Ressourcen halbiert, Laufzeit auf zwei Monate verkürzt. Gelöst durch einen radikalen, aber kontrollierten Fokus auf das MVP und eine hocheffiziente Anpassung der Sicherheitsprozesse an den verkleinerten Scope.

Sicherheit an jedem Gate, nicht erst am Ende

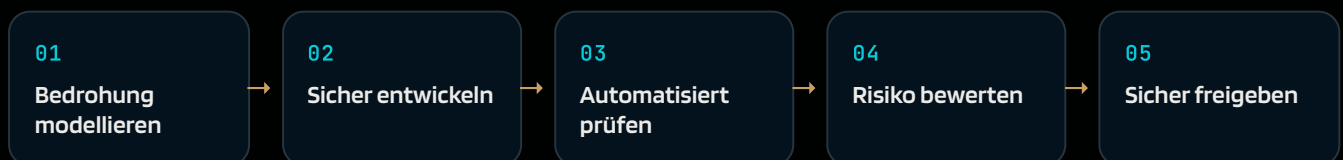
Am Ende stand ein Prozess, in dem Sicherheit an jedem Schritt fest verankert ist. Statt einer nachgelagerten Prüfung durchläuft jede Änderung definierte **Security-Gates**, von der Bedrohungsanalyse im Design bis zur Freigabe.

SICHERHEITS-GATES IM PROZESS			● Gate-Status
PHASE	SECURITY-GATE	METHODE	STATUS
Design	Bedrohungsanalyse	CSA	● bestanden
Implementierung	Secure Coding	Review	● bestanden
Build / Test	Security-Assessment	Scan	● bestanden
Release	Risikobewertung	Freigabe	● MVP live

PROJEKT-TICKER | Scope-Change: Budget halbiert → MVP-Fokus → Team 12 → 5 → Sicherheitspro

● Gate bestanden ● sicher freigegeben · MVP live ■ Schematische Darstellung des Wirkprinzips

WIRKPRINZIP DER SICHERHEITS-GATES



VOM NACHGEDANKEN ZUM BESTANDTEIL

Aus einer nachgelagerten Prüfung ist ein Prozess geworden, in dem Sicherheit an jedem Schritt fest verankert ist, von der Bedrohungsanalyse im Design bis zur geprüften Freigabe.

Termingerecht geliefert, trotz halbiertem **allem**

**2 statt 10
Monate**

Fristgerechte Lieferung nach der
Scope-Anpassung.

**CSA
erfüllt**

Vollständige Einhaltung der Si-
cherheitsanforderungen, MVP si-
cher live.

12 → 5

Team um rund 60 % verkleinert,
ohne Sicherheitsabstriche.

NACHHALTIGE WIRKUNG

Trotz massiver personeller und finanzieller Einschnitte wurde das definierte MVP zum Stichtag mit allen geforderten Sicherheitsanforderungen übergeben. Wichtiger noch: Das Entwicklerteam wurde befähigt, Sicherheit von vornherein mitzudenken, ohne an Produktivität zu verlieren.

09 • STIMME DES KUNDEN

"

Als Budget und Team halbiert wurden, stand das Projekt auf der Kippe. Dass wir am Ende termingerecht und mit allen Sicherheitsanforderungen live gegangen sind, verdanken wir einem klaren Kurs, der Sicherheit nicht als Bremse, sondern als festen Teil der Entwicklung verstanden hat.

Projektleitung, Unternehmen im Transport- und Verkehrssektor

10 · KEY ACHIEVEMENTS

Was bleibt

- ✓ MVP termingerecht und mit allen Sicherheitsanforderungen produktiv gesetzt
- ✓ Sicherheitsanforderungen (CSA/SSDLC) fest im Prozess verankert (Security by Design)
- ✓ Fristgerechte Lieferung in zwei statt zehn Monaten
- ✓ Vollständige Einhaltung der CSA-Sicherheitsanforderungen
- ✓ Entwicklerteam befähigt, Sicherheit eigenständig mitzudenken
- ✓ Radikaler Scope-Fokus sicher durch Budget- und Teamhalbierung getragen
- ✓ Sicherheit als Teil der Entwicklung etabliert, nicht als nachgelagerte Bremse

FAZIT · AUS KRISE WIRD KURS

Ein Projekt, das auf der Kippe stand, wurde nicht nur gerettet, sondern auf einen tragfähigen Kurs gebracht, mit Sicherheit als festem Bestandteil der Entwicklung.

WIE DER ZUGVOGEL IM GEGENWIND

Der Betreiber hält heute den Kurs, auch unter Druck, korrigiert früh und verliert das Ziel nicht aus den Augen.

Aus Krise wird Kurs.

Vorausschauende Sicherheit macht aus einem Projekt in der Krise einen tragfähigen Kurs. Sicherheit ist heute kein Anhängsel am Ende der Entwicklung, sondern fliegt von Beginn an mit, und macht das Team fähig, auch in schwerem Wetter sicher anzukommen.

AUSBLICK

Security by Design ist im Entwicklungsalltag verankert, Sicherheit wird von Beginn an mitgedacht, nicht nachträglich geprüft.

ÜBERTRAGBAR

Der Ansatz lässt sich auf weitere geschäftskritische Anwendungen und Projekte im Unternehmen 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, Sichere Software-Entwicklung (SSDLC)**.



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.