T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

Security by Design scheitert nicht an Technik, sondern am Willen zur Veränderung

Alexandra Palandrani & Nicole Adloff, Securenication GmbH

These



Security by Design ist ein technisches Problem.

These



Security by Design ist ein technisches Problem.



Ausgangslange

Warum wird Sicherheit so oft nachträglich ergänzt?

Standards. Frameworks.
Tools. Guidelines.

Die Methoden sind da.
Die Technik ist da.

Und trotzdem …

- Sicherheit wird ans Projektende verschoben
- Risiken werden erst spät sichtbar
- Verantwortlichkeiten bleiben unklar

Die zentrale Frage ist daher nicht: Können wir sichere Systeme bauen?
Sondern: Sind wir bereit, dafür anders zu arbeiten?

Inhalte

1 Der Mythos: Security by Design ist ein technisches Problem

2 Sicherheit trifft Realität: Entwickler, Informationssicherheit & Management

3 Vom Security Gatekeeper zum Enabler

4 Warum Security by Design in der Praxis scheitert

5 Abschluss

1 Der Mythos: Security by Design ist ein technisches Problem



Der Mythos: Security by Design ist ein technisches Problem

Was ist Security by Design eigentlich?

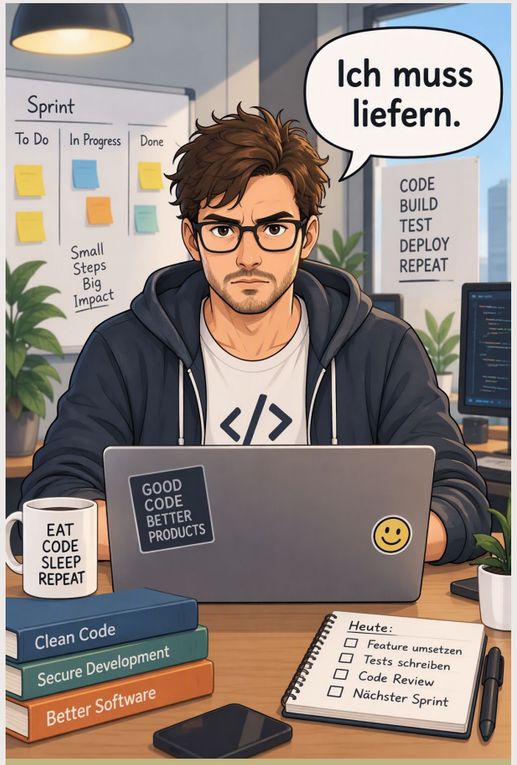
*Security by Design ist der Ansatz, Sicherheit von **Anfang** an als **festen Bestandteil** von Produktion, Prozessen und Entscheidungen zu verankern.*



2 Sicherheit trifft Realität: Entwickler, Informationssicherheit & Management

Sicherheit trifft Realität: Entwickler, Informationssicherheit & Management

Drei Perspektiven



Time to market

Möglichst wenig Reibung



Risikoreduktion

Möglichst hohe Sicherheit



Business Value

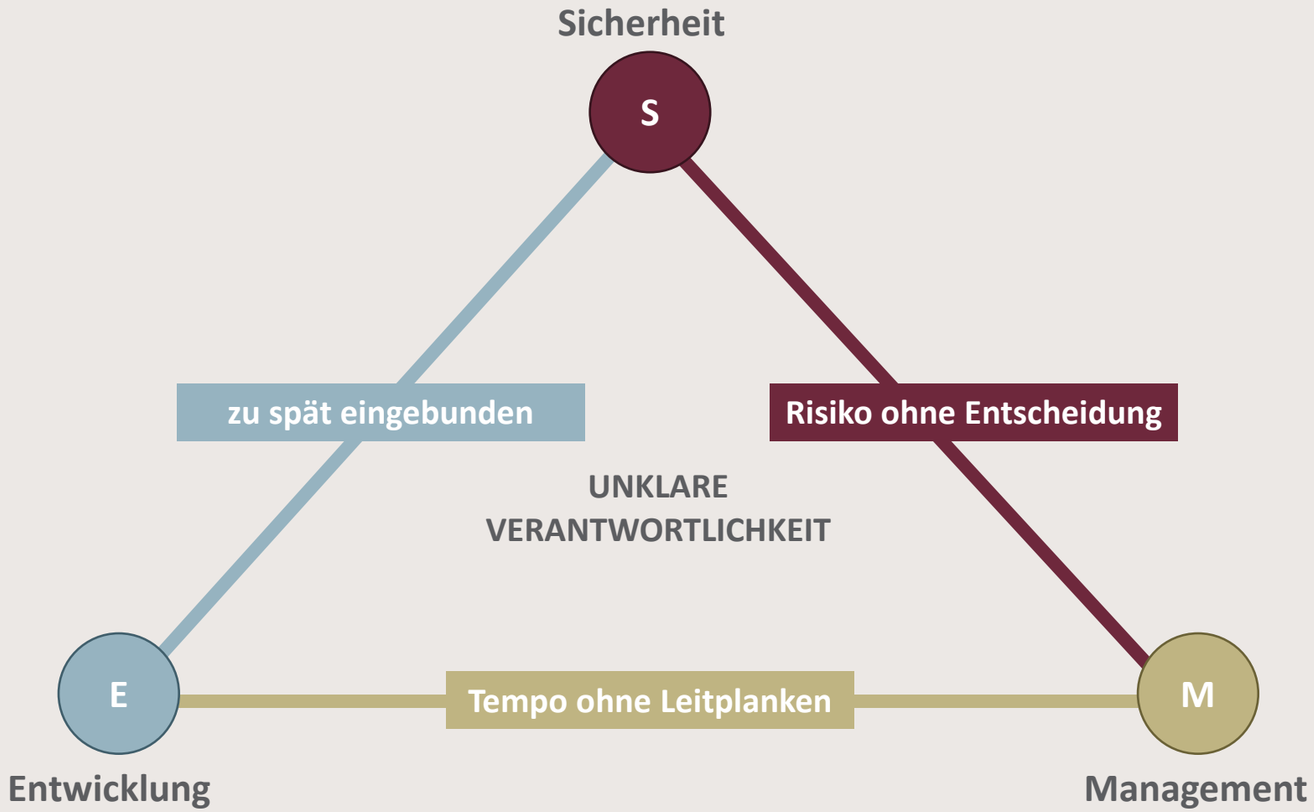
Möglichst hohe Effizienz

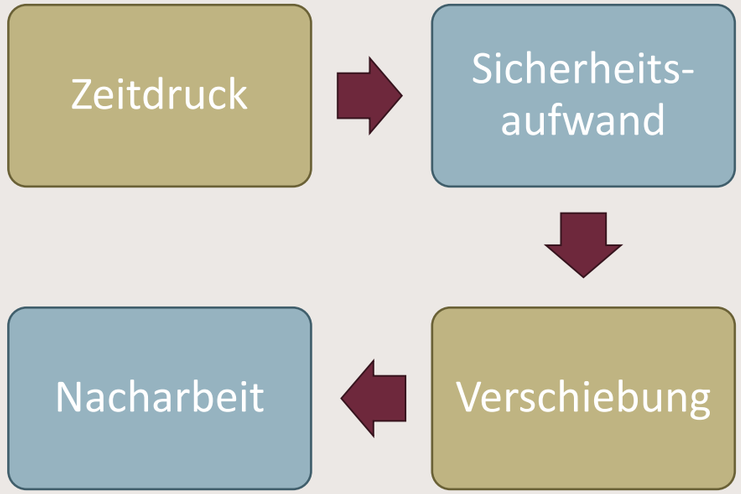
Die Herausforderung: aus individuellen Zielsystemen ein gemeinsames Ziel machen

Sicherheit trifft Realität: Entwickler, Informationssicherheit & Management

Wo Zusammenarbeit kippt

Verantwortung wird geschoben, wenn Entscheidungen spät, teuer oder unklar werden.





3 Vom Security Gatekeeper zum Enabler



Vom Security Gatekeeper zum Enabler
Symptome und Ursachen

SYMPTOME

- Sicherheit wird erst kurz vor dem Go Live betrachtet
- Entwickler sehen Sicherheit als Zusatzaufwand
- Fachbereiche priorisieren Geschwindigkeit
- Sicherheitsteams agieren als Kontrollinstanz



URSACHEN

- Silodenken zwischen Sicherheit, IT und Business
- Konkurrierende Ziele
- Fehlende Verantwortlichkeiten und Kompetenzen
- Angst vor zusätzlichem Aufwand
- Angst vor Veränderung bei etablierten Prozessen und Routinen
- Sicherheit wird als Bremse oder Verhinderer wahrgenommen
- Erfolgsmessung an Lieferterminen und Umsetzungsgeschwindigkeit, nicht am erreichten Sicherheitsniveau
- Veränderungen erzeugen kurzfristig Kosten, während der Nutzen erst langfristig entsteht

„Jeder ist verantwortlich“ bedeutet häufig „Niemand fühlt sich verantwortlich“.

Vom Security Gatekeeper zum Enabler

Nicht weniger Kontrolle, sondern bessere Steuerung

Der Rollenwechsel: von nachgelagerter Kontrolle zu früher, kontinuierlicher Unterstützung.

GATEKEEPER

- Prüfung am Projektende
- Anforderungen als Überraschung
- Fokus auf Abweichungen
- Sicherheit als Freigabehürde und Engpass
- Individuelle Freigaben
- Befunde und Eskalationen

ENABLER

- ✓ Beratung ab der Idee
- ✓ Sicherheitsstandards
- ✓ Anforderungen als Leitplanken
- ✓ Fokus auf umsetzbare Lösungen
- ✓ Sicherheit als Teil guter Engineering-Praxis
- ✓ Automatisierte Checks
- ✓ Coaching & Musterlösungen
- ✓ Sicherheit als Beschleuniger

Nicht weniger Kontrolle, sondern bessere, frühere und wirksamere Kontrolle.

Vom Security Gatekeeper zum Enabler
Vier Hebel für eine anschlussfähige Sicherheit

Sicherheit wird wirksam, wenn sie in die Arbeitsrealität der Teams passt.

01 Verantwortung	Klare Verantwortlichkeiten in Produkt, Entwicklung und Sicherheit.
02 Integration	Sicherheit in Anforderungen, Architektur, Backlog und Definition of Done.
03 Automatisierung	Wiederholbare Kontrollen dort automatisieren, wo es sinnvoll ist.
04 Anreize & Führung	Sicherheitsziele priorisieren, vorleben und in Entscheidungen berücksichtigen.

Wenn Sicherheit immer zusätzliche Arbeit bedeutet, wird sie immer als zusätzliche Arbeit behandelt.

4 Warum Security by Design in der Praxis scheitert

Warum Security by Design in der Praxis scheitert

6 Sätze, an denen Security by Design stirbt













Warum Security by Design in der Praxis scheitert
Fallbeispiel 1 - Dokumentation

DIE ANFORDERUNG

Die Dokumentation zur Anwendung wird regelmäßig, mindestens jährlich, auf Aktualität überprüft und bei Bedarf ergänzt.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Dies erfolgt mindestens einmal jährlich im Rahmen des Jahresabschlusses.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

Die Antwort ist aktuell etwas formal schwach formuliert. Ein Prüfer liest das Wort „Dies“ jedoch als ungenau.

PROBLEMATISCH

- Fokus auf Formulierung und mögliche Prüferreaktionen
- Die tatsächlich fehlende Information wird nicht klar benannt
- Der Fachbereich soll die „richtige Sprache“ verwenden
- Der Zweck der Rückfrage bleibt unklar
- Der Eindruck entsteht: Es geht um prüfungssichere Antworten, nicht um wirksame Sicherheit

DIE EIGENTLICHE FRAGE

Werden alle relevanten Dokumente regelmäßig überprüft und ist die Verantwortung dafür eindeutig festgelegt?

Warum Security by Design in der Praxis scheitert
Fallbeispiel 1 - Dokumentation

DIE ANFORDERUNG

Die Dokumentation zur Anwendung wird regelmäßig, mindestens jährlich, auf Aktualität überprüft und bei Bedarf ergänzt.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Dies erfolgt mindestens einmal jährlich im Rahmen des Jahresabschlusses.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

Die Antwort ist aktuell etwas formal schwach formuliert. Ein Prüfer liest das Wort „Dies“ jedoch als ungenau.

WIE HÄTTE DIE RÜCKMELDUNG BESSER AUSSEHEN KÖNNEN?

Aus Ihrer Antwort verstehen wir, dass die Dokumentation der Anwendung XXX mind. jährlich auf Aktualität geprüft wird. Bitte bestätigen Sie uns diese Annahme.

Nicht: „Die Formulierung ist formal schwach.“

Sondern: „Uns fehlt noch eine konkrete Information, um die Umsetzung nachvollziehen zu können.“

Warum Security by Design in der Praxis scheitert
Fallbeispiel 2 - Verschlüsselung

DIE ANFORDERUNG

Werden Datensicherungen der Anwendungsdaten verschlüsselt gespeichert?

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Die Datensicherungen werden verschlüsselt. In der Software selbst wird nicht verschlüsselt, da es sich um eine Anwendung zur Archivierung handelt.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

Bitte die Hochkommata entfernen.
Bitte den letzten Buchstaben entfernen.
Sonst OK.

PROBLEMATISCH

- Die Rückmeldung korrigiert Zeichen, aber bewertet nicht das Risiko
- Die fachliche Aussage wird nicht eingeordnet
- Der Schutzbedarf der verarbeiteten Informationen bleibt unberücksichtigt
- Mögliche kompensierende Maßnahmen werden nicht betrachtet
- Es entsteht kein zusätzliches Verständnis für Verschlüsselung

DIE EIGENTLICHEN FRAGEN

- Welche Informationen werden verarbeitet?
- Welche kryptografischen Verfahren werden eingesetzt?
- Wie werden Datensicherungen übertragen und gibt es für die unterschiedlichen Stadien jeweils Verschlüsselungsverfahren (at-rest, in-transit, in-use)?

Warum Security by Design in der Praxis scheitert
Fallbeispiel 2 - Verschlüsselung

DIE ANFORDERUNG

Werden Datensicherungen der Anwendungsdaten verschlüsselt gespeichert?

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Die Datensicherungen werden verschlüsselt. In der Software selbst wird nicht verschlüsselt, da es sich um eine Anwendung zur Archivierung handelt.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

Bitte die Hochkommata entfernen.
Bitte den letzten Buchstaben entfernen.
Sonst OK.

WIE HÄTTE DIE RÜCKMELDUNG BESSER AUSSEHEN KÖNNEN?

Vielen Dank für die Erläuterung. Wir verstehen die Antwort so, dass die Datensicherungen verschlüsselt werden, innerhalb der Anwendung selbst jedoch keine Verschlüsselung eingesetzt wird. Für die Bewertung benötigen wir noch eine kurze Einordnung, welche schützenswerten Informationen verarbeitet werden und wie das daraus entstehende Risiko behandelt wird. Falls eine Verschlüsselung technisch nicht möglich ist, können auch geeignete kompensierende Maßnahmen beschrieben werden.

Nicht der perfekte Satz schützt die Informationen, sondern die wirksame Maßnahme.

Warum Security by Design in der Praxis scheitert
Fallbeispiel 3 - Passwortanzeige

DIE ANFORDERUNG

Das eingegebene Passwort wird nicht im Klartext angezeigt.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Eingegebene Passwörter werden nicht in Klartext angezeigt.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

„Passworte“ → Der korrekte Plural ist „Passwörter“.
„angegeben“ → Das Wort aus der Anforderung heißt „angezeigt“.

PROBLEMATISCH

- Erhält der Anwendungsverantwortliche Rückmeldungen aufgrund von Grammatik- oder Rechtschreibfehler, werden unnötig Ressourcen zur Korrektur genutzt.
- Weiterhin kann die Zusammenarbeit zwischen der 2nd Line und der 1st Line negativ beeinflusst werden und das Bewusstsein für Informationssicherheit in der 1st Line sinken.

DIE EIGENTLICHE FRAGE

Fall keine sonstigen Informationen fehlen, ist keine Rückfrage erforderlich.

Warum Security by Design in der Praxis scheitert
Fallbeispiel 3 - Passwortanzeige

DIE ANFORDERUNG

Das eingegebene Passwort wird nicht im Klartext angezeigt.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Eingegebene Passwörter werden nicht in Klartext angezeigt.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

„Passworte“ → Der korrekte Plural ist „Passwörter“.
„angegeben“ → Das Wort aus der Anforderung heißt „angezeigt“.

WIE HÄTTE DIE RÜCKMELDUNG BESSER AUSSEHEN KÖNNEN?

OK



Sprachliche Präzision ist wichtig. Sie sollte aber kein Selbstzweck sein.

Warum Security by Design in der Praxis scheitert
Fallbeispiel 4 - Incident Management

DIE ANFORDERUNG

Das IT-Asset ist in den Prozess zur Behandlung von Sicherheitsvorfällen eingebunden.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

... wird in einem solchen Fall vorgenommen …

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

... Sie beschreiben einen Zustand in der Zukunft, gefordert wird jedoch der IST-Zustand …

PROBLEMATISCH

Die Rückmeldung klingt, als müsse lediglich die Formulierung geändert werden.

FACHLICH KORREKT ERKANNT

- Sicherheitsvorfälle bzw. entsprechende Prozesse müssen vorab berücksichtigt werden
- Melde-, Eskalations- und Kommunikationswege müssen festgelegt sein
- Die Anwendung muss wirksam in den Incident-Management-Prozess eingebunden sein

Warum Security by Design in der Praxis scheitert
Fallbeispiel 4 - Incident Management

DIE ANFORDERUNG

Das IT-Asset ist in den Prozess zur Behandlung von Sicherheitsvorfällen eingebunden.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

... wird in einem solchen Fall vorgenommen …

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

... Sie beschreiben einen Zustand in der Zukunft, gefordert wird jedoch der IST-Zustand …

WIE HÄTTE DIE RÜCKMELDUNG BESSER AUSSEHEN KÖNNEN?

Aus der Antwort verstehen wir, dass bei der Anwendung XXX der Incident-Management-Prozess angewendet wird, sollte ein entsprechender Fall eintreten.
Die Anforderung geht jedoch einen Schritt weiter: Bereits vor Eintritt eines Sicherheitsvorfalls muss festgelegt sein, wie ein möglicher Vorfall erkannt, gemeldet, bewertet und eskaliert wird.
Bitte prüfen Sie, ob für die Anwendung ein entsprechender Meldeweg definiert ist. Falls dies noch nicht der Fall ist, können wir gemeinsam klären, wie die Anwendung in den bestehenden Prozess eingebunden werden kann.

▶ Die fachliche Lücke verständlich machen.

Warum Security by Design in der Praxis scheitert
Fallbeispiel 5 – komplexe Fragestellungen

DIE ANFORDERUNG

Für das IT-Asset ist sicherzustellen, dass jegliche Informationsobjekte, die für die Governance relevant sind, entsprechend zugeordnet sind.

ANTWORT DES ANWENDUNGSVERANTWORTLICHEN

Die Informationsobjekte sind ausgefüllt.

RÜCKMELDUNG DER INFORMATIONSSICHERHEIT

OK

PROBLEMATISCH

- Ausgefüllt ≠ zugeordnet
- Ob die Anforderung korrekt verstanden wurde, ist unklar.

DIE EIGENTLICHE FRAGE

Wurde die Anwendung im GRC-Tool XXX mit den relevanten Prozessen, IT-Komponenten und Informationskategorien verknüpft?

Warum Security by Design in der Praxis scheitert

Was lernen Fachbereiche aus solchen Rückmeldungen?

- Hochkommata entfernen
- Passworte → Passwörter
- Nicht verstandene Fragen

Haben wir danach ein sichereres System oder nur einen besseren Assessment-Eintrag?

Warum Security by Design in der Praxis scheitert

Was zeigen die Beispiele?

01	**FORM STATT RISIKO**	Sprachliche Korrekturen verdrängen die eigentliche Sicherheitsfrage.
02	**ANWEISUNG STATT ERKLÄRUNG**	Der Fachbereich erfährt, was geändert werden soll, aber nicht, warum.
03	**PRÜFUNG STATT DIALOG**	Das Assessment wird als Abnahmeprüfung und nicht als gemeinsamer Erkenntnisprozess erlebt.
04	**WORDING STATT UMSETZUNG**	Eine sprachlich perfekte Antwort kann eine fehlende oder unwirksame Maßnahme verdecken.

Die Folge:
Menschen optimieren Antworten, anstatt Sicherheit zu gestalten.
Die Motivation, überhaupt zu antworten, sinkt.

5 Abschluss

Abschluss
3 Botschaften zum Mitnehmen

Security by Design wird nicht beschlossen. Sie wird im Alltag sichtbar.

1	**KEIN TECHNOLOGIEPROJEKT**	Tools unterstützen. Sie ersetzen keine Priorisierung.
2	**EIN FÜHRUNGS- UND KULTURPROJEKT**	Verantwortung, Anreize und Vorbilder prägen Verhalten.
3	**VERHALTEN VOR REGELWERK**	Akzeptierte Verantwortung wirkt stärker als zusätzliche Vorgaben.

Wir scheitern nicht daran, sichere Systeme zu bauen.
Wir scheitern daran, die Organisation zu verändern, die diese Systeme baut.

Abschluss

Was Sie bereits nach dem T.I.S.P./T.P.S.S.E CM anders machen können:

01	**EINEN VERANTWORTLICHEN BENENNEN**	Nicht: „Sicherheit ist zuständig“, sondern eine konkrete Entscheidung.
02	**EINEN PROZESSPUNKT VORZIEHEN**	Sicherheitsfrage vor Budget- oder Architekturentscheidung platzieren.
03	**EINEN SICHEREN STANDARD BAUEN**	Ein häufiges Problem einmal lösen und als Standard bereitstellen.
04	**EINEN ANREIZ VERÄNDERN**	Nicht nur Liefertermine, sondern sichere Lieferfähigkeit sichtbar machen.

Veränderung wird glaubwürdig, wenn sie im nächsten Arbeitsablauf sichtbar wird.

Abschluss

Security by Design beginnt nicht mit einem Tool. Es beginnt mit einer Entscheidung.

Vielen Dank!



Alexandra Palandrani

Director – Assurance & Readiness
Securenication GmbH

E-Mail alexandra.palandrani@securenication.de

SE | CURE | NI | CA | TIO N

[siː¦kjʊəʁnɪˈkeɪʃən] Substantiv, feminin

Wird genutzt, um ein Unternehmen zu beschreiben, das robuste Strukturen aufbaut, Transformation steuert und Intelligenz verantwortungsvoll einsetzt – und dies in der charakteristischen Qualität einer High-End-Boutique.



Nicole Adloff

Senior Consultant – Assurance & Readiness
Securenication GmbH

E-Mail nicole.adloff@securenication.de