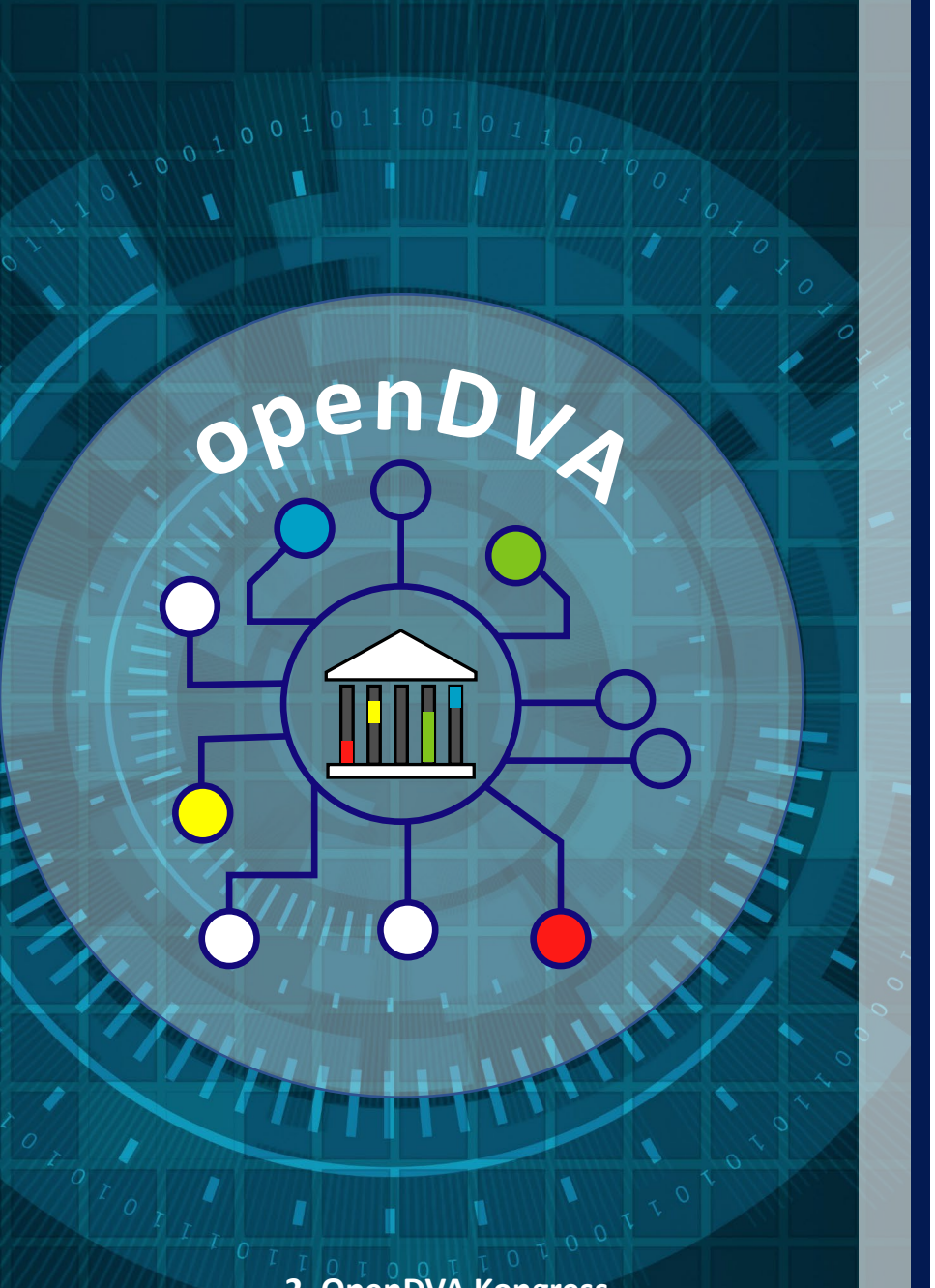


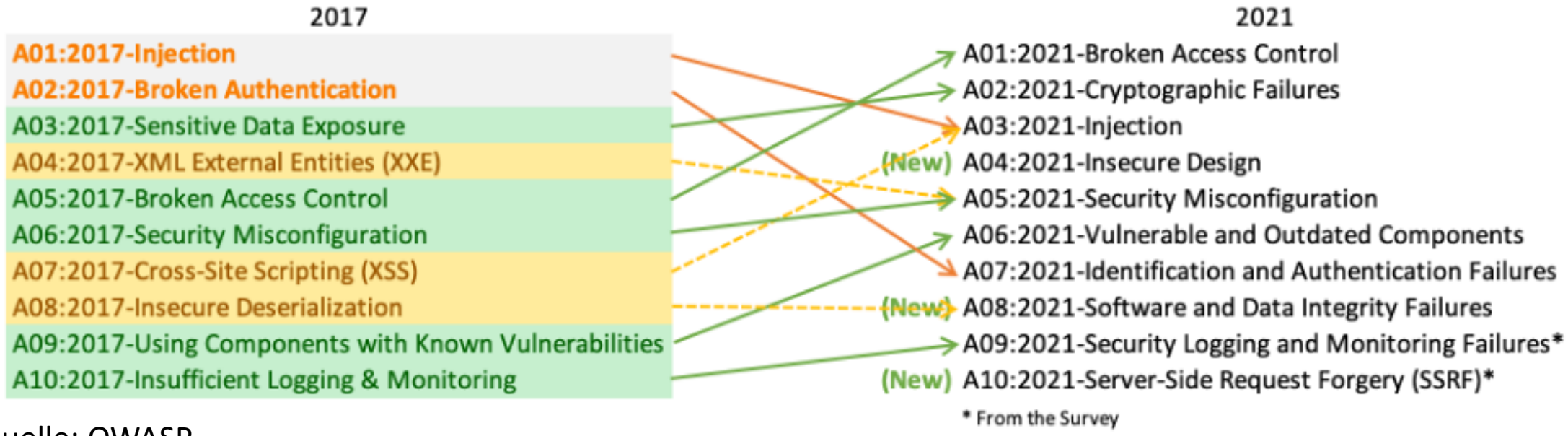
Citizen Development… aber sicher?

Clemens-Alexander Brust
DLR-Institut für Datenwissenschaften

2. OpenDVA Kongress
Dornburger Schlösser 03. - 04. Juni 2024

Trends in der Softwaresicherheit

– Unsicheres Design und „Denkfehler“ lösen Sicherheitslücken technischer Natur als wesentlichen Risikofaktor ab.



Quelle: OWASP

Trends in der Softwaresicherheit (2)

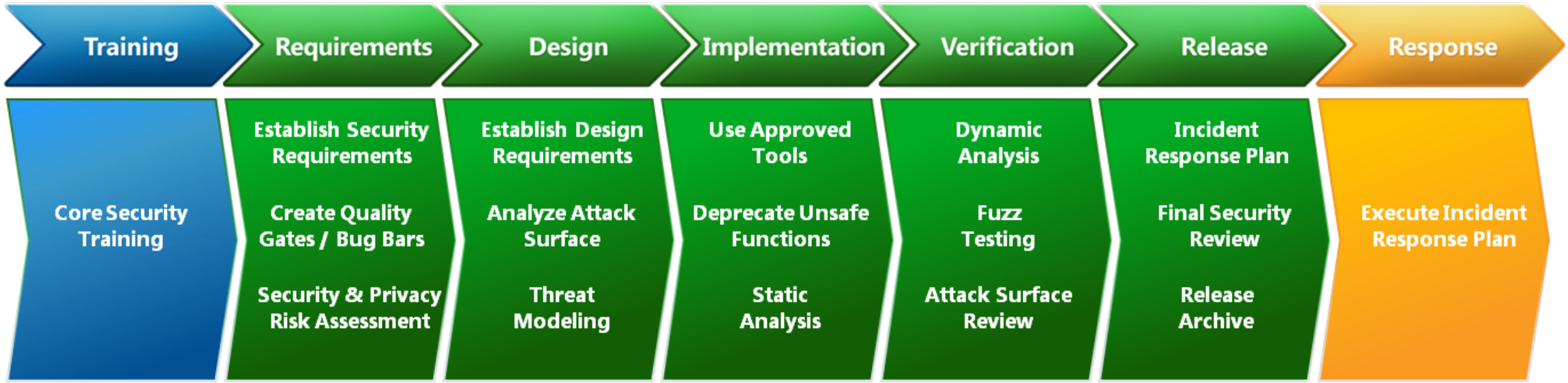
- Der Einsatz von Low-Code/No-Code-Plattformen verstärkt diesen Effekt weiter.
- Tätigkeit der Entwickelnden wird auf Design reduziert.
- Dazu bringen LC/NC-Plattformen neue einzigartige Risiken mit.

→ Was können wir tun?

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

Quelle: OWASP

Was können wir tun? (Generell)

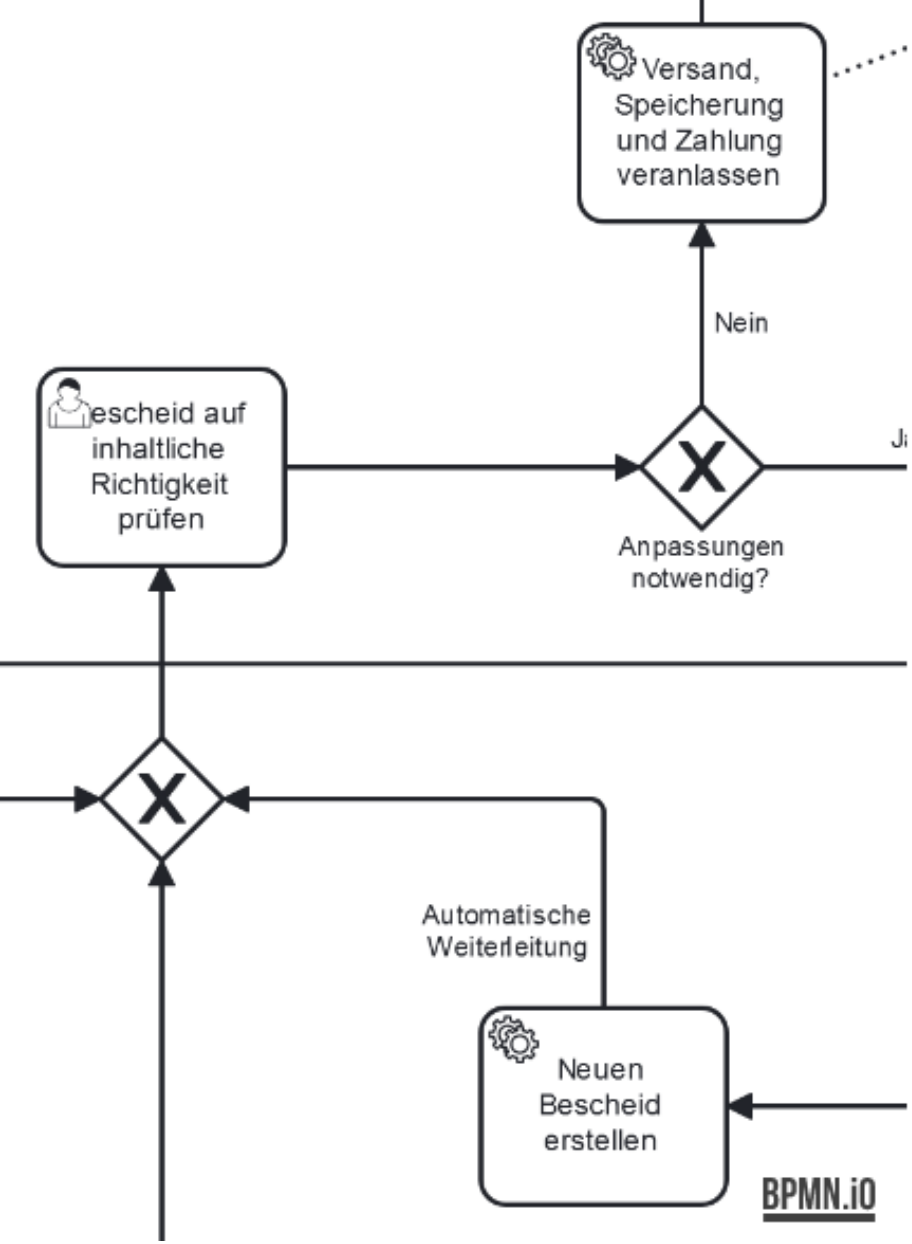


- "Shift Left": früher im Entwicklungsprozess ansetzen.
- Neben rein technischen sind vor allem organisationelle Maßnahmen angezeigt:
  - Schulung des Personals im Umgang mit der Plattform,
  - Sensibilisierung für häufige Bedrohungen, Best Practices.

Was können wir tun (simpLEX)

- Es einfach(er) machen, sichere Prozesse zu entwerfen.
- Nudging kann effektiver als Zwang sein ☺

- In der Entwicklungsumgebung selbst über Bedrohungen und Risiken einzelner Bausteine oder Verbindungen aufklären – konstruktiv!
- Für häufige unsichere Konstruktionen Gegenvorschläge anbieten, die mit einem Klick eingebaut sind.



32. Verantwortlichkeitsübergreifender Informationsfluss

Informationsfluss von "Leistungsbetreuende Person" nach "Teamleiter"

Dieser Informationsfluss reicht von einer Verantwortlichkeit zu einer anderen. Möglicherweise haben die Verantwortlichkeiten verschiedene Berechtigungen.

Empfehlungen:

- Übergebene Informationen explizit benennen

33. Prozess enthält Zyklus

Bürgergeld Lokalprozess

Dieser Prozess enthält mindestens einen Zyklus, wodurch die Ausführungsdauer evtl. unbeschränkt ist.

Empfehlungen:

- Prozess ohne Zyklen gestalten.
- Anzahl der Ausführungen durch Ausrollen der Zyklen begrenzen.
- Anzahl der Ausführungen durch Einfügen eines garantierten Abbruchkriteriums begrenzen.

Vielen Dank
für Ihre Aufmerksamkeit!

Clemens-Alexander Brust
DLR-Institut für Datenwissenschaften

clemens-alexander.brust@dlr.de

Gefördert durch:

Bundesministerium des Innern und für Heimat

aufgrund eines Beschlusses des Deutschen Bundestages

Kollaboration:

FRIEDRICH-SCHILLER-UNIVERSITÄT JENA

UNIVERSITÄT BIELEFELD
Fakultät für Linguistik und Literaturwissenschaft

CLAUSE

HOCHSCHULE KEHL
UNIVERSITY OF APPLIED SCIENCES
Verwaltung - Gestalten & Entwickeln

FUSION

JENA LICHTSTADT.

DLR Institute of Data Science

knowledge tools

InfAI
Institut für Angewandte Informatik

BÜRO FÜR PRAKTISCHE INFORMATIK
BFPI

SHI STEIN HARDENBERG INSTITUT

ÖZG

FITKO

Freistaat Thüringen Finanzministerium