WAS (BISHER) FEHLT UM APPS SICHER ZU ENTWICKELN?

PROZESSE, WERKZEUGE UND SCHULUNGEN FÜR SICHERE APPS BY DESIGN

PVM 2019: Projektmanagement und Vorgehensmodelle

Katharina Altemeier, Matthias Becker, Stefan Dziwok, Thorsten Koch und Sven Merschjohann

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

EFRE.NRW
Investitionen in Wachstum
und Beschäftigung

Dieses Vorhaben wurde aus Mitteln des Europäischen Fonds für regionale Entwicklung (EFRE) gefördert.

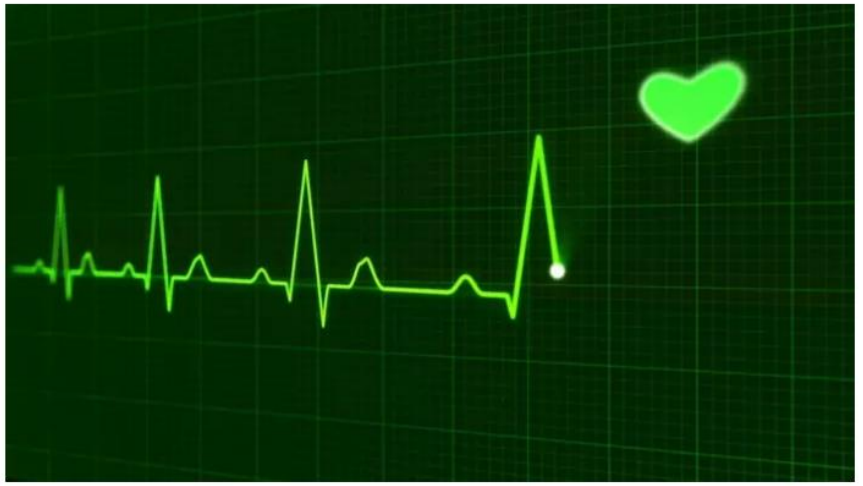
Motivation

Unsichere Software kann Leben gefährden

Beispiel: Medizintechnik

Herzschrittmacher von St. Jude Medical: Firmware-Patches gegen Sicherheitslücken

31.08.2017 15:17 Uhr – Olivia von Westernhagen vorlesen



Versierte Hacker können Herzschrittmacher der Marke Abbott angreifen, um Befehle auszuführen und Patientendaten zu stehlen. Implantatträgern wird ein baldiger Arztbesuch empfohlen, um wichtige Firmware-Updates zu installieren.

Quelle: https://www.heise.de/newsticker/meldung/Herzschrittmacher-von-St-Jude-Medical-Firmware-Patches-gegen-Sicherheitsluecken-3817954.html, 31.08.2017

Unsichere Software kann schützenswerte Daten gefährden

Beispiel: Vivy Gesundheits-App

30.10.2018 16:28 Uhr | Security

Vivy: Gravierende Sicherheitsmängel in Krankenkassen-App aufgedeckt

Die App, die bei Millionen von Versicherten und 16 Kassen im Einsatz ist, hatte schwerwiegende Sicherheitsmängel. Die Verantwortlichen sehen das anders.

Von **Fabian A. Scherschel** 221

Sicherheitsforscher sind mit der Absicherung der digitalen Krankenakte der App Vivy nicht zufrieden. (Bild: dpa, Michael Kappeler)

https://www.heise.de/security/meldung/Vivy-Gravierende-Sicherheitsmaengel-in-Krankenkassen-App-aufgedeckt-4207260.html

www.youtube.com/watch?v=82Hfh1AItiQ

Allianz · Barmenia Versicherungen · Gothaer · DAK Gesundheit · IKK classic · IKK Nord · IKK Südwest · Bertelsmann BKK · BKK Diakonie · BKK_DÜRKOPP ADLER · mhplus · pronova BKK · BKK Stadt Augsburg · BKK Gildemeister Seidensticker · HEIMAT KRANKENKASSE · BKK HMR · BKK MO · BITMARCK

AppSecure.nrw

Das Thema Sicherheit wird zunehmend reguliert…

Beispiele KRITIS, DSGVO, IEC 62443

Verordnete Sicherheit

Neue gesetzliche Anforderungen an den Schutz kritischer Infrastrukturen

WISSEN | RECHT

Joerg Heidrich 19.08.2016

BSI, IT-Sicherheit, IT-Sicherheitsgesetz, KRITIS, Kritische Infrastrukturen, NIS-Richtlinie

Nachdem Deutschland mit seinem IT-Sicherheitsgesetz im vergangenen Jahr vorausgegangen war, hat nun die EU eine Richtlinie zur Förderung der Cybersicherheit verabschiedet. Die neuen Regelungen stellen Betreiber von digitalen Diensten auch hierzulande vor erhebliche Herausforderungen.

Quelle: https://www.heise.de/ct/ausgabe/2016-18-Neue-gesetzliche-Anforderungen-an-den-Schutz-kritischer-Infrastrukturen-3293714.html

HOME / IEC-NORMEN / IEC 62443-4-1:2018

größer

IEC 62443-4-1:2018

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

Ausgabedatum: **2018-01**
Edition: **1.0**
Sprache: **EN - englisch**
Seitenzahl: **54** VDE-Artnr.: **225304**

Inhaltsverzeichnis

Quelle: https://www.vde-verlag.de/iec-normen/225304/iec-62443-4-1-2018.html

PASSWÖRTER GELEAKT

Datenschützer prüft Sanktionen gegen Knuddels

Das Datenleck beim Chatanbieter Knuddels ruft nun auch die Aufsichtsbehörden auf den Plan. Nach der Datenschutz-Grundverordnung sind hohe Bußgelder möglich.

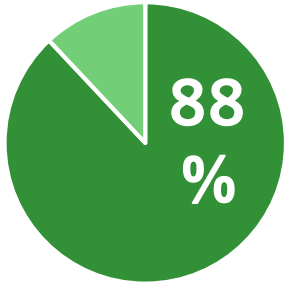
11. September 2018, 10:22 Uhr, Friedhelm Greis

Quelle: https://www.golem.de/news/passwoerter-geleakt-datenschuetzer-prueft-sanktionen-gegen-knuddels-1809-136501.html

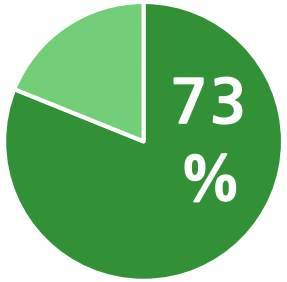
AppSecure.nrw

Warum ist sichere Software-Entwicklung ein wichtiges Thema?

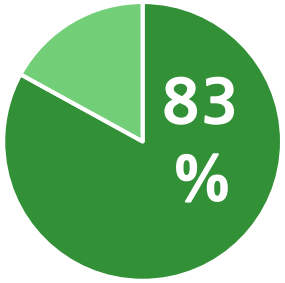
Beispiel: „Security-Lücken durch falsche Nutzung von Krypto-Bibliotheken“



der Android-Apps mit mindestens einer Krypto-Fehlbenutzung[1]



der 2,7 Mio. Artefakte in Maven Central benutzen Java-Standard-Krypto-Bibliothek falsch[3]



der Kryptographie-bezogenen Lücken wegen Fehlbenutzung[2]

Selbst namhafte Anbieter benutzen TLS-Bibliotheken falsch[4]

[1] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel. An empirical study of cryptographic misuse in android applications. CCS 2013.
[2] D. Lazar, H. Chen, X. Wang, and N. Zeldovich. Why does cryptographic software fail?: A case study and open problems. APSys 2014.
[3] S. Krüger, J. Spaeth, K. Ali, E. Bodden, M. Mezini. Large-Scale Study of Non-Trivial Misuses of the Java Cryptography Architecture. In Preparation
[4] S. Fahl, M. Harbach, T. Muders, M. Smith, L. Baumgärtner, B Freisleben. Why Eve and Mallory Love Android: An Analysis of SSL (In)Security. CCS 2012.

Problemstellung und Zielsetzung

Zur Problemstellung …

Was sind die Herausforderungen in der sicheren Softwareentwicklung?

AppSecure.nrw

Zur Zielstellung…

Wir wollen Entwickler*innen bei der Erstellung sicherer Software unterstützen

AppSecure.nrw

Online-Umfrage

Online-Umfrage zu »Secure Software Engineering in Unternehmen der DACH-Region«

Durchführung einer Studie zum Thema IT-Security, um Probleme und Bedarfe zu verstehen

Ziel der Online-Umfrage

- Herausforderungen und Bedarfe (inkl. subjektiver Einschätzung) bzgl. sicherer Softwareentwicklung im Arbeitsumfeld ermitteln
- Zielgruppe: alle Personen, die an der Entwicklung aktiv beteiligt sind: Anforderung, Konzept, Implementierung, Test, Betrieb
- Maßnahmen ableiten und innerhalb des Projekts praxisnahe Lösungen entwickeln

365

Teilnehmer

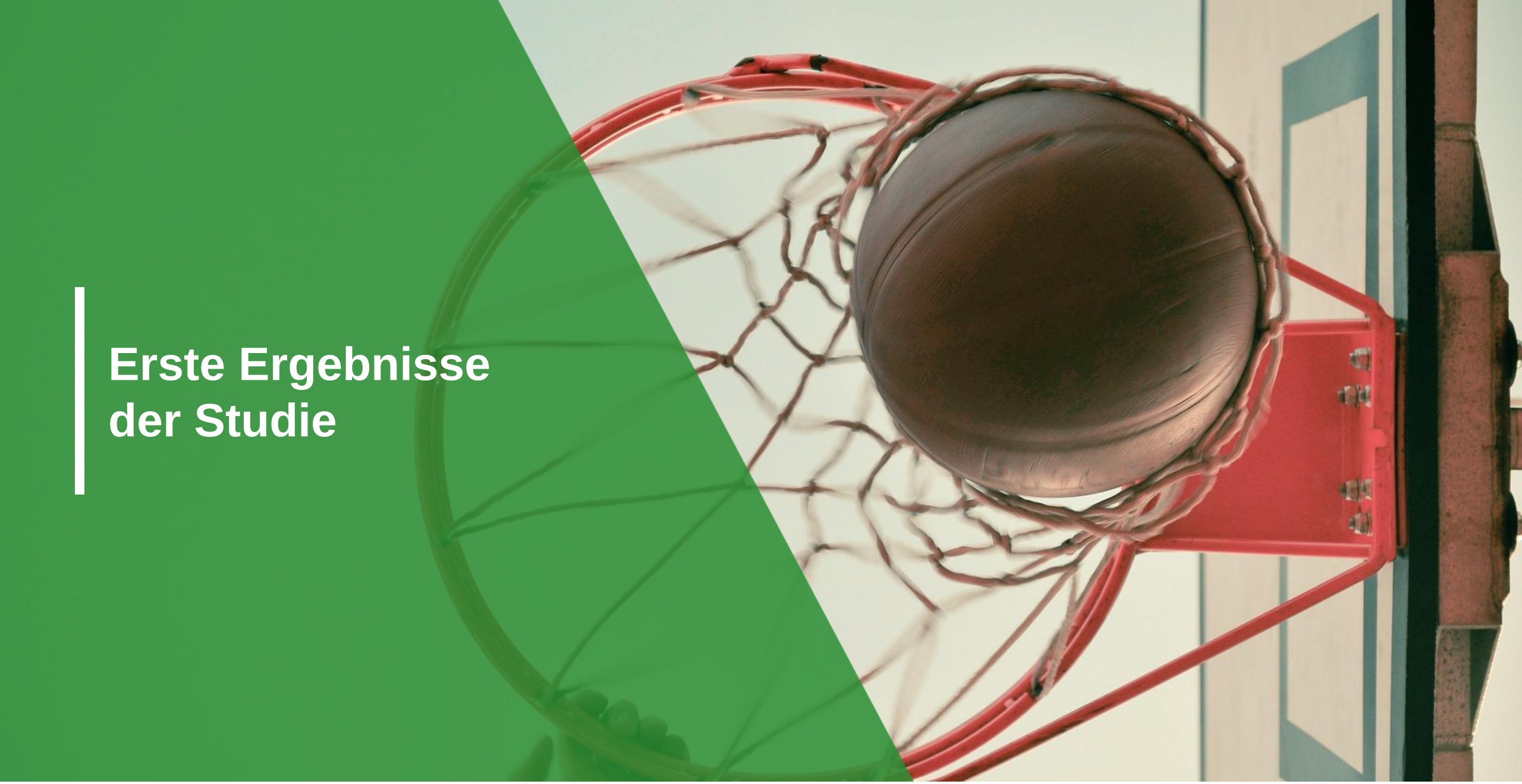
Zeitraum

11.06.– 09.08.19

Multiplikatoren

Heise, Bitkom, Digital-in-NRW
It‘s OWL

Erste Ergebnisse der Studie



Teilnehmer der Studie

Position

- 80% der Teilnehmer sind Software-Entwickler
- 15% der Teilnehmer sind Produkt-Owner und Führungskräfte
- 5% der Teilnehmer sind Security Analysten

Berufserfahrung

- 60% der Teilnehmer haben über 10 Jahre Berufserfahrung
- 18% der Teilnehmer haben zwischen 6 – 10 Jahren Berufserfahrung
- 22% der Teilnehmer haben weniger als 5 Jahre Berufserfahrung

Größe des Unternehmens

- 44% der Teilnehmer arbeiten in Unternehmen mit 1.000 Beschäftigten
- 15% der Teilnehmer arbeiten in Unternehmen mit 251 – 1.000 Beschäftigten
- 41% der Teilnehmer arbeiten in KMUs

Top-Branchen

- Versicherung + Finanzen
- Gesundheit
- Industrie

Key-Facts zum Stand der Softwareentwicklung

1 Die Awareness für das Thema Security in der Softwareentwicklung ist bei der Mehrheit der Teilnehmer vorhanden.

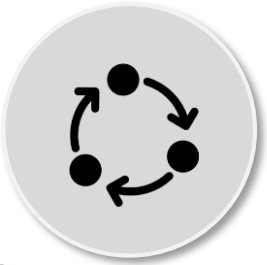
- 61% der Teilnehmer empfindet, dass nicht genügend Zeit in SSE investiert wird.
- 66% der Teilnehmer achten während des Anforderungsmanagements auf Security.
- 77% der Teilnehmer achten während des Entwurfs auf Security.
- 73% der Teilnehmer achten während der Implementierung auf Security.
- 73% der Teilnehmer stimmt zu, dass jedes Teammitglied über eine hohe SSE Kompetenz verfügen sollte.

Key-Facts zum Stand der Softwareentwicklung

2 **Methoden aus dem Secure Software Engineering (Vorlagen, Tools, Prozesse) werden nicht angewendet und sind größtenteils auch nicht bekannt.**

- Die knappe Mehrheit der Teilnehmer (56%) hat keine klar definierten Prozesse.
- 62% der Teilnehmer haben keine Vorlagen bzw. Standards für Security Anforderungen.
- 67% der Teilnehmer haben keine Vorlagen bzw. Standards für einen sicheren Entwurf.
- 34% der Teilnehmer haben Vorlagen bzw. Standards für die Erstellung von sicherem Code.
- 74% der Teilnehmer geben an, dass es kein finales Security Review vor dem Release gibt.

Key-Facts zum Stand der Softwareentwicklung



3 **Bessere Prozesse würden den meisten Teilnehmer dabei helfen den Aspekt Security bei ihrer täglichen Arbeit besser umsetzen zu können.**

- Die knappe Mehrheit der Teilnehmer (56%) hat keine klar definierten Prozesse.
- 83% der Teilnehmer geben an, dass die gegenwärtigen Prozesse im Anforderungsmanagement genauer und verständlicher sein sollten.
- 80% der Teilnehmer geben an, dass die gegenwärtigen Prozesse im Entwurf genauer und verständlicher sein sollten.
- 85% der Teilnehmer geben an, dass die gegenwärtigen Prozesse in der Implementierung genauer und verständlicher sein sollten.

Key-Facts zum Stand der Softwareentwicklung

4 **Bessere Tools würden den meisten Teilnehmer dabei helfen den Aspekt Security bei ihrer täglichen Arbeit besser umsetzen zu können.**

- 56% der Teilnehmer haben keine passende Sammlung an Werkzeugen.
- 66% der Teilnehmer geben an, dass bessere Werkzeuge helfen würden die Aufgaben im Anforderungsmanagement besser zu erfüllen.
- 66% der Teilnehmer geben an, dass bessere Werkzeuge im Entwurf bei der Erfüllung der Aufgaben helfen würden.
- 81% der Teilnehmer geben an, dass bessere Werkzeuge während der Implementierung bei der Erfüllung der Aufgaben helfen würden.

Key-Facts zum Stand der Softwareentwicklung

4 Die heutigen Kompetenzen reichen nicht aus um sichere Software zu entwickeln

- 73% der Teilnehmer stimmen zu, dass jedes Teammitglied über eine hohe SSE Kompetenz verfügen sollte.
- 64% der Teilnehmer denken, dass die heutigen Kompetenzen des Teams nicht ausreichen passende Security Anforderungen zu definieren.
- 59% der Teilnehmer geben an, dass die aktuellen Kompetenzen im Team nicht ausreichen, um einen sicheren Entwurf zu definieren.
- 66% der Teilnehmer geben an, dass die aktuellen Kompetenzen im Team nicht ausreichen, um eine sichere Implementierung zu gewährleisten.

Key-Facts zum Stand der Softwareentwicklung

Zusammenfassung

1. Die Awareness für das Thema Security in der Softwareentwicklung ist bei der Mehrheit der Teilnehmer vorhanden.
2. Methoden aus dem Secure Software Engineering (Vorlagen, Tools, Prozesse) werden nicht angewendet und sind größtenteils auch nicht bekannt.
3. Bessere Prozesse würden den meisten Teilnehmer dabei helfen den Aspekt Security bei ihrer täglichen Arbeit besser umsetzen zu können.
4. Bessere Tools würden den meisten Teilnehmer dabei helfen den Aspekt Security bei ihrer täglichen Arbeit besser umsetzen zu können.
5. Die heutigen Kompetenzen reichen nicht aus um sichere Software zu entwickeln.

Nächste Schritte

Nächste Schritte

Zusammenfassung

Zusammenfassung

Wie wollen wir Entwickler*innen bei der Erstellung von sicherer Software unterstützen?

Wie erreichen wir unsere Ziele im Projekt?

- Durchführung einer Studie zum Thema IT-Security, um Probleme und Bedarfe zu verstehen
- Erarbeitung von werkzeuggestützten Security-by-Design Methoden
- Konzipierung und Erprobung von Security Schulungen
- Verbesserung der Benutzbarkeit von Open-Source Werkzeugen

Diese Vorteile schafft AppSecure.nrw für die sichere Softwareentwicklung:

Daten- & Angriffs-sicherheit → Kompetente Entwickler → Vertrauen in die Software → Kosten-effiziente Entwicklung → Wettbewerbs-vorteil

AppSecure.nrw

AppSecure.nrw

Apps von Grund auf sicher entwickeln

MEHR INFORMATIONEN

www.appsecure.nrw
Twitter: @AppSecureNRW

KONTAKT

Thorsten Koch
Wissenschaftlicher Mitarbeiter
Fraunhofer IEM
Zukunftsmeile 1
33102 Paderborn

Telefon: +49 5251 5465-127
thorsten.koch@iem.fraunhofer.de
www.iem.fraunhofer.de