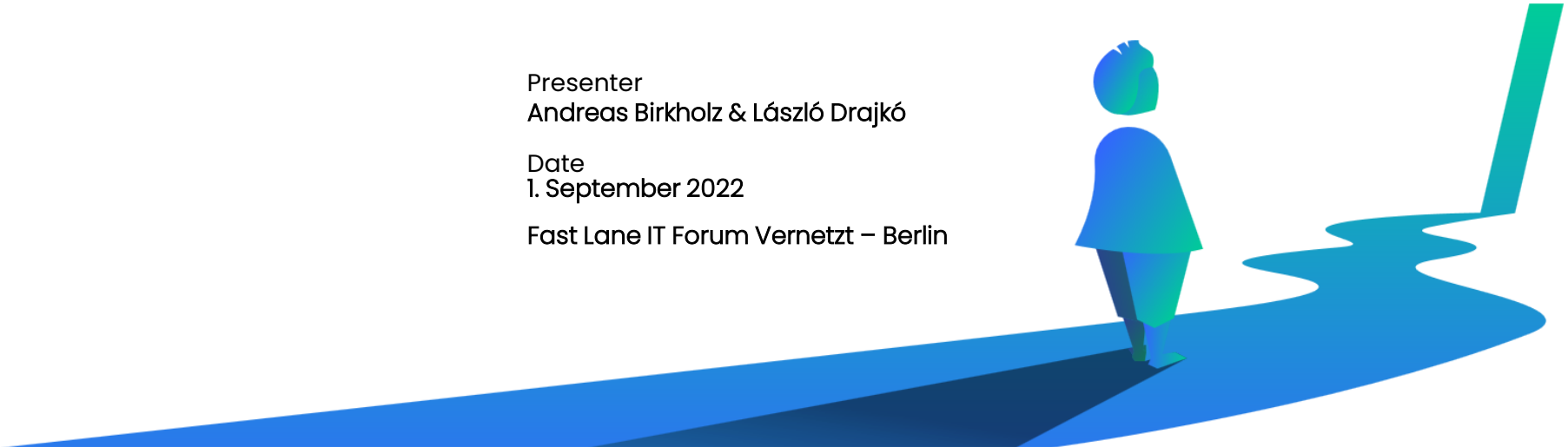
Was läuft falsch mit Cyber Security?

Die digitale Welt und unser Leben befinden sich seit Beginn der ersten Hackerangriffe auf einer Pechsträhne. Im Laufe der Zeit haben sich Cyber-Vorfälle zu den führenden Geschäftsrisiken und zur meist unterschätzten Bedrohung entwickelt. Wir gehen es an!

Presenter
Andreas Birkholz & László Drajkó

Date
1. September 2022

Fast Lane IT Forum Vernetzt – Berlin



Safety vs. Security

Sicherheit vs. Sicherheit


E
'OR 1=1;--

Problem: **Menschliche Fehler**

90+%

Über 90 % der Vorfälle resultieren aus bereits bekannten, aber wiederholt begangenen Fehlern im Code

Source: Focus on the Biggest Security Threats, Not the Most Publicized - Smarter With Gartner NVD - Data Feeds (nist.gov)

Cybersecurity – der große Orbit des menschlichen Versagens

Amateurliga: Die Nutzer – oder die, von denen wir wissen, dass Sie es nicht kennen

- Die Benutzer werden alles tun, um unsere IT-Systeme auf neue Art und Weise mit Malware zu infizieren
- Was kann man tun: den Nutzer informieren und ihm beibringen, was er NICHT tun soll
- Programme zur Sensibilisierung für Cybersicherheit

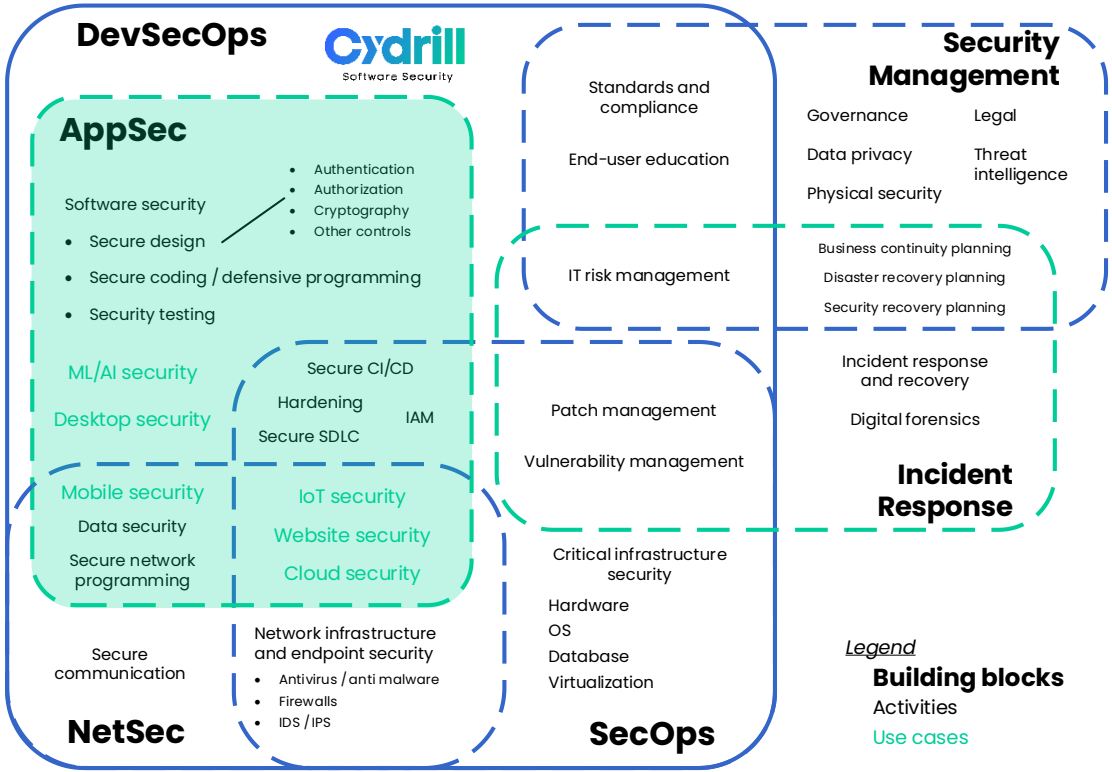
Champions League: Entwickler – oder diejenigen, bei denen wir es nicht einmal vermuten, kennen oder praktizieren möglicherweise keine präventiven Techniken

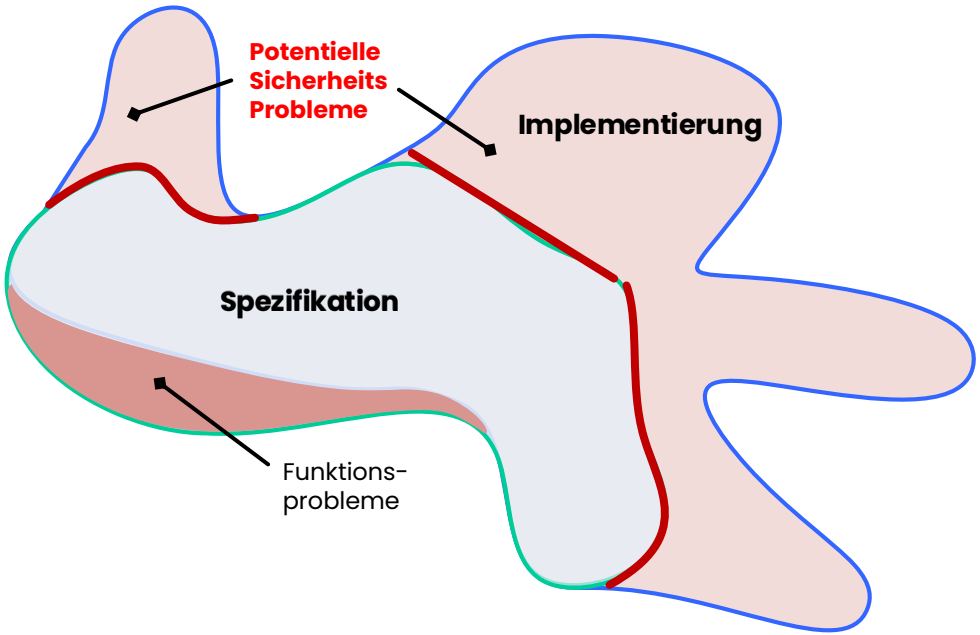
- **Tor für Hacker** - Die Erwartungen, die an die Entwickler herangetragen werden, konzentrieren sich fast ausschließlich auf die Funktionalität, so dass sie sich am wenigsten Gedanken darüber machen, ***was die Software außer dem***, was sie tun soll noch kann. Was kann man tun: lehren, wie man NICHT PROGRAMMIERT – Sichere Kodierung

Das Kernproblem ist AppSec, welches die meisten Ursachen der Probleme enthält.

Während der Großteil des Budgets für die Beseitigung der Folgen dieser Probleme verwendet wird →ist Sicherheit ein nachträglicher Gedanke

Empfehlung ist, ein Gleichgewicht zwischen der Bekämpfung der Ursachen und der Begrenzung der Folgen herzustellen.




Potentielle
Sicherheits
Probleme
Implementierung
Spezifikation
Funktions-
probleme

Interventionspunkte

Wunschvorstellung: Prozesse und Werkzeuge zur Lösung

- ‚*Code review*' Verfahren zur Fehlererkennung
- SAST, DAST: Statische und dynamische Code Analysatoren
- Sicherheitsprüfung und Penetration Test

→ Jemand anderes soll die Arbeit erledigen? Ethischer Hacker, Postsicherheit

Derzeitige Auswirkungen auf die Gemeinschaft: **26.8 Millionen „professionelle" Entwickler**

- Weniger als 1% haben jemals eine solche Ausbildung erhalten
- Nachfragedefizit, Mangel an angemessenen verfahren und Praktiken

→ Die Ursache des Problems

Software-Sicherheit, sichere Programmierung: **TEAM SPORT**

- Der Code ist so sicher, wie es die Ausbildung des schwächsten Programmierers vorgibt zu sein
- Es ist nicht möglich, jedem Programmiere einen SW- Tester zuzuweisen

→ Die Sicherheit liegt in den Händen **ALLER** beitragenden Entwickler

Jahr	Anzahl der Software-Entwickler
2018	23.9 Millionen
2021	26,8 **Millionen**
2023	27,7 **Millionen**
2024	28.7 **Millionen**
2030	45 **Millionen**

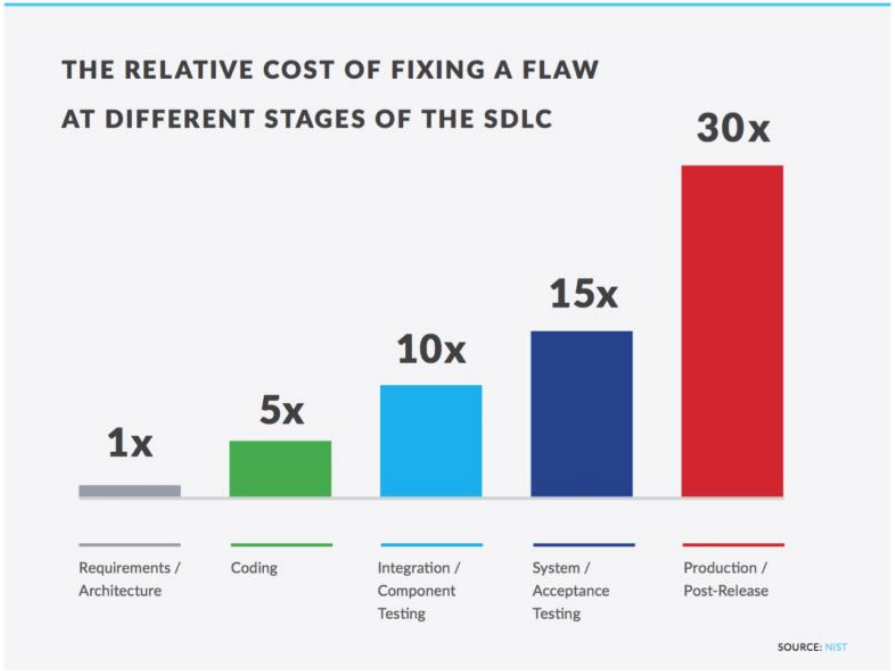
Quelle: future-processing.com

Finanzielle Rationalität

Die Entwicklung softwareintensiver Systeme ist eine komplexe Aufgabe – wie bei physischen Gebäuden erhöht die Durchführung von Änderungen in Abhängigkeit vom Grad der Fertigstellung die Komplexität der Korrektur..

Finanzieller Aspekt: Fehlerbehebungen sind sehr kostspielig, wenn sie zu spät entdeckt werden, und diese Kosten steigen mit der Zeit exponentiell an.

Branchenverschiebung: „Shift-Left" – Verschiebung der Kosten nach links auf der SDLC _ lebenszykluskurve. Ein in die Sicherheit investierter Euro ist besser, wenn er rechtzeitig ausgegeben wird



Quelle: National Institute of Standards & Technology nist.com

Der Weg

Der Weg: vom Bewusstsein zur Meisterschaft

Ablauf eines Cydrill Kurses:

- Erkennen eines Problems im Code
- Hacking-Techniken aufzeigen (LAB)
- Fokus auf Best Practices (LAB)
- Reale Beispiele, Fallstudien

Interaktive Übungen im “Natürlichen Lebensraum” eines Entwicklers

- Jährlich lizenziertes eLearning
- Periodische Fertigkeiten und Übungen
- Nachhaltigkeit “Sichere Programmierkenntnisse”
- Vergleich von Teams und Teammitgliedern
- Zertifizierungsstufen und Live- Scoring

Cyberrisiken vorhersehen

Mehr Sicherheit, Konformität und Wettbewerbsvorteile

- Der erste präventive Schritt besteht darin, den vorhandenen Wissenstand zu ermitteln – das „Schwarze Loch“ zu identifizieren
- Fahrplan für die Vorbereitung und Kompetenzentwicklung
- Übernahme, Umsetzung und Beibehaltung bewährter Verfahren
- Einhaltung der Cybersicherheitsvorschriften mit einem kontinuierlich aufrechterhaltenen Bereitschaftsniveau

CydrillSergeant – the award-winning learning experience that delivers

Our learning environment has been recognized by CIOReview Europe – Cydrill was awarded the reputable Top Gamification Solution Provider title in 2021. CydrillSergeant supports the team sport nature of secure coding to engage developers, both individually and in a team.

Top Gamification Solution Companies-gamification Companies (ciorevieweurope.com)

Cydrill: Emotionally Engaging Drills for Secure Coding (ciorevieweurope.com)

Cydrill

Cydrill is featured:

TOP 20 Companies shaping the cyber landscape

Recognized by

ENTERPRISE SECURITY

TOP CYBER SECURITY COMPANY IN EUROPE 2021

 Cydrill: Ensuring Proactive Security with Effective Coding Practices (enterprisesecuritymag.com)

Zusammenfassung

Problem: Die digitale Welt und unser Leben befinden sich seit Beginn der ersten Hackerangriffe auf einer Pechsträhne. Im Laufe der Zeit haben sich Cyber-Vorfälle zu den führenden Geschäftsrisiken und zur meist unterschätzten Bedrohung entwickelt.

Prozess: Maßnahmen zur Gewährleistung der Cybersicherheit haben sich im Nachhinein entwickelt um die Folgen zu minimieren, anstatt die Ursachen anzugehen. Über 90% der Schwachstellen waren bekannte menschliche Codierungsfehler, bevor diese gehackt wurden.

Potential: Stellen Sie sich vor, organische Sicherheit wird Zeile für Zeile in der Software aufgebaut, wobei die Code-Hygiene durch gemeinsame sichere Codierungs-Best-Practices in den Entwicklungsteams sichergestellt wird, um die Cybersicherheit zu gewährleisten und so die Ursache zu bekämpfen.

Vorschlag: durch kontinuierliches Lernen und regelmäßige Bereitschaftsübungen neue Fähigkeiten, auch bekannt als sichere Programmierkenntnisse, zu erwerben, um anfällige Programmiergewohnheiten mit Best Practices für das gesamte Entwicklungsteam zu ersetzen. Eine Blended-Learning-Reise aus Schulungs-, E-Learning- und Labs-Abonnements mit auf Live-Score-Messwerten basierenden Zertifikaten.

Cydrill |

Danke!

Presenter
Andreas Birkholz, andreasb@cydrill.com

Date

01. September 2022
Berlin