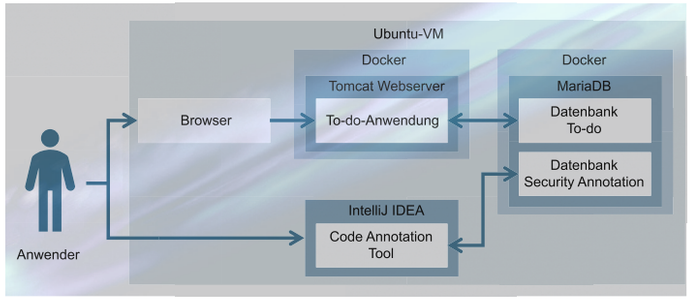


SECURITY ANNOTATION – SICHERHEITSSENSIBLEN CODE KENNZEICHNEN

Für Unternehmen alle Größen sind Daten über Prozesse, Personen oder Systeme wichtige Werte und damit schützenswerte Güter (engl. Assets). Werden solche Daten manipuliert oder geraten in falsche Hände, kann dies die Wirtschaftlichkeit und Arbeitsfähigkeit eines Unternehmens beeinträchtigen. Deshalb wurde die Security Annotation entwickelt, um KMU den Einstieg in die IT-Sicherheit zu erleichtern. Mit diesem Konzept ist es möglich, sicherheitssensiblen Quellcode dauerhaft zu kennzeichnen und den Assets sowie potenziellen Schwachstellen zuzuordnen. Die Annotationen sowie die verlinkten Zusatzinformationen werden Commit-spezifisch gespeichert. Dadurch wird eine auf den Sicherheitsstatus der gesamten Codebasis abgestimmte Dokumentation erzeugt. Diese Dokumentation ist sowohl für Entwickler als auch Projektmanager relevant, um die Softwareentwicklung mit dem Risikomanagement zu verbinden.

Um das Konzept zu erläutern und erfahrbar zu machen, wurde eine Erweiterung für die Entwicklungsumgebung IntelliJ erstellt, mit der die Security Annotationen einfach gesetzt werden können. Zudem wurde ein Projekt zur Demonstration entwickelt.

cloud.hs-augsburg.de/s/kZBbYaJJew5xfG8?

plugins.jetbrains.com/plugin/17541-code-annotation-tool-hitssse-

ANSPRECHPARTNER UND KONTAKT

Kontakt
Prof. Dr. Dominik Merli
Leiter HSA_innos
Institut für innovative Sicherheit
Tel. +49 821 5586-3459
Dominik.Merli@hs-augsburg.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
HSA_innos Institut für innovative Sicherheit
Hochschule Augsburg University of Applied Sciences
HSA_ias Institut für agile Softwareentwicklung
HITSSSE Höhere IT-Sicherheit durch Sichere Software Entwicklung
IT-Sicherheit IN DER WIRTSCHAFT
Mittelstand-Digital

Technische Hochschule Augsburg
Institut für innovative Sicherheit | HSA_innos
Am Technologiezentrum 8, MRM-Gebäude
86159 Augsburg
www.hsainnos.de

Stand: 09/2023 | Fotos: unsplash.com, THA | Gestaltung: wppt.de

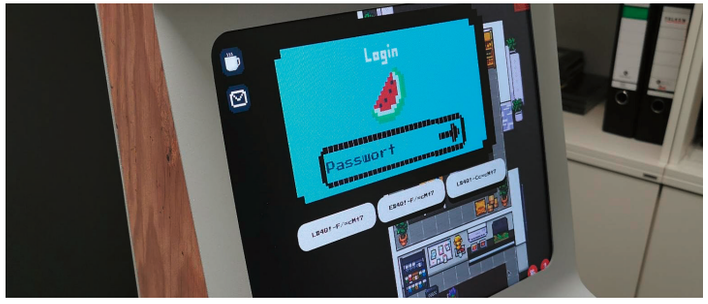
HSA_innos
Institut für innovative Sicherheit

Hochschule Augsburg University of Applied Sciences

HITSSSE – Höhere IT-Sicherheit durch Sichere Software Entwicklung

MEHR SICHERHEIT FÜR DEN MITTELSTAND

Immer mehr kleine und mittlere Unternehmen (KMUs) entwickeln Software für Infrastrukturen oder Produkte. Hierbei treffen oftmals hoher Zeitdruck und beschränkte personelle Ressourcen aufeinander. Deshalb spielt die Sicherheit der Entwicklungen teils kaum eine Rolle und gefährdet letztlich Unternehmen und ihre Kunden. Das Fördervorhaben „Höhere IT-Sicherheit durch Sichere Software Entwicklung“ (kurz: HITSSSE) soll diesen Zustand verbessern. Hierfür werden Handlungsempfehlungen sowie technische Hilfsmittel erstellt, um daraufhin generische Lösungsansätze für KMUs zu schaffen. Letztendlich soll es Unternehmen leichter fallen, einen sicheren Prozess für die Produkt- und Softwareentwicklung umzusetzen, der die IT-Sicherheit in Infrastrukturen und Produkten verbessert. Dafür adressiert HITSSSE sowohl technische Hürden als auch den Faktor Mensch.



SECURITY ADVENTURE – DER FAKTOR MENSCH

Ein großer Teil der Angriffe auf IT-Infrastrukturen ist auf den Faktor Mensch zurückzuführen. Phishing-Mails, Tailgating, CEO-Fraud, Baiting – diese und viele weitere Methoden machen sich die Schwachstelle „Mensch“ zu Nutze und können Angreifern den Zugang zu sensiblen Daten und Systemen ermöglichen. Verhindern lassen sich solche Angriffe mit der Arbeit am Menschen. Unternehmen sollten sie für Bedrohungen sensibilisieren und Akzeptanz für Sicherheitsmaßnahmen schaffen.

Um Unternehmen hierbei zu unterstützen, entwickelte Projekt HITSSSE ein Videospiel, das die Spielenden durch verschiedene sicherheitsrelevante Herausforderungen im Arbeitsalltag führt. Dabei hat es zwei Funktionen. Zum einen baut das Security Adventure Wissen auf, indem es spielerisch konkrete Themen aus dem breiten Feld der IT-Security Awareness oder der sicheren Softwareentwicklung aufarbeitet. Zum anderen soll so die Bereitschaft der Mitarbeitenden steigern, sich mit dem Thema IT-Sicherheit zu beschäftigen.

Das Spiel kann auf einem normalen PC betrieben werden. Zudem wird das Security Adventure auch in Form eines klassischen Spielautomaten angeboten. Gepaart mit dem Pixel-Look des Spiels, spricht dies sowohl die Nostalgie der Mitarbeitenden an und minimiert zugleich die Einstiegshürden.

CI-IN-A-BOX – VOLLSTÄNDIG GEKAPSELTE CI/CD INFRASTRUKTUR

Beim Versuch CI/CD Pipeline-Tools in die interne Infrastruktur einzubinden kann es oft zu Problemen kommen. Schuld sind häufig Konfigurationsprobleme, besonders wenn Embedded Hardware verwendet wird. Um diese Störungen zu verhindern, bietet die CI-in-a-Box eine vollständig gekapselte CI/CD Infrastruktur. Hiermit erhalten Softwareentwickler:innen eine sichere Plattform, um automatisierte CI/CD Pipeline Prozesse auszuprobieren und kennenzulernen.

Bei der Infrastruktur wird Wert auf Flexibilität, Reproduzierbarkeit und Robustheit gelegt. Deshalb ist die CI-in-a-Box kompakt und mobil – und damit flexibel und nach Bedarf einsetzbar. Zudem ist die zu nutzende Softwareumgebung mit einem Klick installierbar und ebenso einfach zurückgesetzt werden. Durch eine vorgeschaltete OPNsense wird ein internes Netzwerk errichtet. So kann die CI-in-a-Box separiert vom Unternehmensnetzwerk betrieben werden.

Für den einfachen Zugang zur CI-in-a-Box und der CI/CD Prozesse werden Beispielprojekte schwerpunktmäßig für den Embedded-Bereich bereitgestellt, die die Verwendung und Integration der Plattform unterstützen.