Fortschrittszentrum
LERNENDE SYSTEME

EIN KI-QUICK-CHECK DES KI-FORTSCHRITTSZENTRUMS

CIDAAS RISIKOMANAGEMENT

KONTAKT

Fraunhofer IAO

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

Sebastian Kurowski
sebastian.kurowski@iao.fraunhofer.de

IN ZUSAMMENARBEIT MIT

cidaas

Widas ID GmbH

Sadrick Widmann

Ausgangssituation

Risikoanalysen beinhalten die Auswahl von Gegenmaßnahmen und die Abschätzung von Ereignisschweren und Eintrittswah scheinlichkeiten. Eine regelmäßige Durchführung solcher Analysen kann dabei die Informationssicherheit eines Unternehmens maßgeblich steigern. Sie ist jedoch auch mit erheblichen Ressourcen und Personalaufwand verbunden.

Lösungsidee

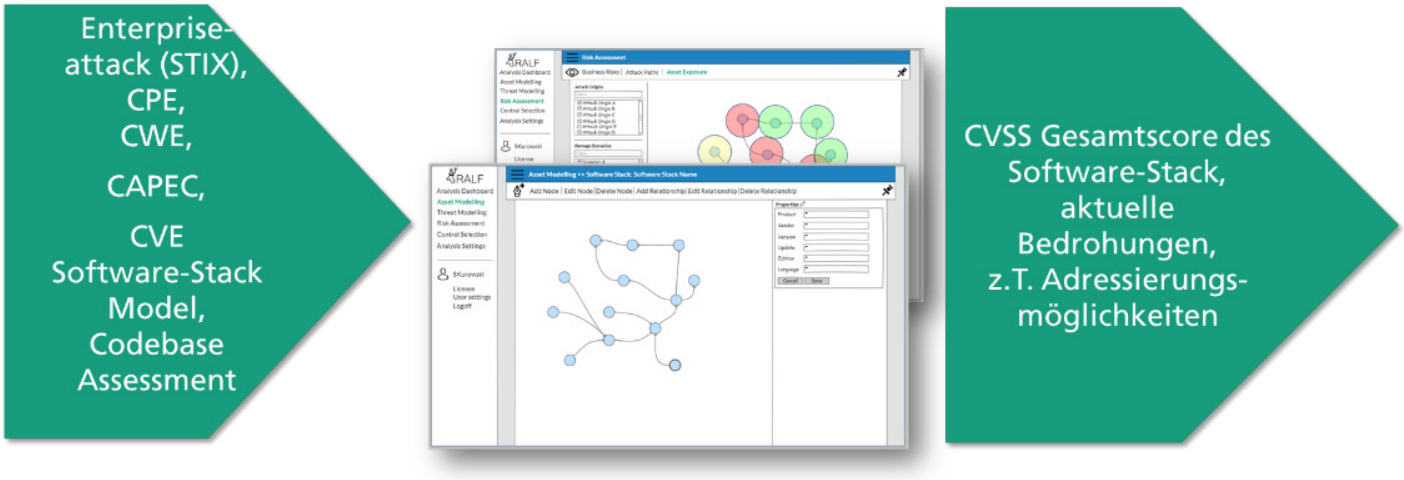
Ein automatisierter Red Teaming inspirierter Analyseansatz auf Grundlage von Bedrohungskonsolidierungen, gekoppelt mit einem lernenden System zur Berücksichtigung betriebswirtschaftlicher Grenzen bei der Maßnahmenauswahl, ermöglicht eine regelmäßige ressourcensparende Durchführung von Risikoanalysen.

Nutzen

Die Informationssicherheit kann dabei erheblich gesteigert werden, indem auch auf neuartig auftretende Bedrohungen Rücksicht genommen werden kann. So können beispielsweise neu auftretende Bedrohungen auf Grundlage von Remote Code Execution Schwachstellen bereits in der Analyse Berücksichtigung finden, bevor diese beispielsweise durch Malwareausnutzung relevant werden.

CIDAAS RISIKOMANAGEMENT

EIN KI-QUICK-CHECK DES KI-FORTSCHRITTSZENTRUMS



Umsetzung der KI-Applikation

Eine entsprechende Anwendung benötigt jedoch eine Datengrundlage zur Ermittlung möglicher Bedrohungen und Angriffs-patterns für Netzwerkinfrastrukturen, Softwarestacks und Codebases. Eine solche Datengrundlage konnte durch die Konsolidierung mehrerer Datenbanken zu Schwachstellen, Bedrohungen, Angriffs-mustern, Plattformen und Verwundbarkei-ten erreicht werden.

Die Anwendung der Bedrohungsmuster kann nun über Graphennetze ermöglicht werden. Anschließend können Maßnah-men auf Grundlage der anwendbaren Bedrohungen abgeleitet werden. Über das Feedback der Anwender kann nun mit Hilfe inferentiellen Lernens die Maßnahmenaus-wahl verbessert werden, so dass diese sich zunehmend besser auf das anwendende Unternehmen anpasst.

Fortschrittszentrum LERNENDE SYSTEME

EIN KI-QUICK-CHECK DES KI-FORTSCHRITTSZENTRUMS

Fraunhofer IAO

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

Fraunhofer IPA

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA

Kooperationspartner:

CyberValley

Gefördert durch:

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT. ARBEIT UND WOHNUNGSBAU

Ansprechpartner:

Dr. Matthias Peissner
Telefon +49 711 970-2311
matthias.peissner@iao.fraunhofer.de

Prof. Dr. Marco Huber
Telefon +49 711 970-1960
marco.huber@ipa.fraunhofer.de

www.ki-fortschrittszentrum.de

ÜBER DAS KI-FORTSCHRITTSZENTRUM »LERNENDE SYSTEME«

Das KI-Fortschrittszentrum »Lernende Systeme« unterstützt Firmen dabei, die wirtschaftlichen Chancen der Künstlichen Intelligenz und insbesondere des Maschinellen Lernens für sich zu nutzen. In anwendungsnahen Forschungsprojekten und in direkter Kooperation mit Industrieunternehmen arbeiten die Stuttgarter Fraunhofer-Institute für Arbeitswirtschaft und Organisation IAO sowie für Produktionstechnik und Automatisierung IPA daran, Technologien aus der KI-Spitzenforschung in die breite Anwendung der produzierenden Industrie und der Dienstleistungswirtschaft zu bringen. Finanzielle Förderung erhält das Zentrum vom Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg.

Europas größte Forschungskooperation auf dem Gebiet der KI

Das KI-Forschungszentrum ist Forschungspartner des Cyber Valley, einem Konsortium aus den renommierten Universitäten Tübingen und Stuttgart, dem Max-Planck-Institut für intelligente Systeme und einigen führenden Industrieunternehmen. In gemeinsamen Forschungslabors werden Grundlagenforschung und anwendungsorientierte Entwicklung zu aktuellen wie auch zukünftigen Bedarfen behandelt und vorangetrieben.

Menschzentrierte KI

Alle Aktivitäten des Zentrums verfolgen das Ziel, eine menschzentrierte KI zu entwickeln, der die Menschen vertrauen und die sie akzeptieren. Nur wenn Menschen mit neuen Technologien intuitiv interagieren und vertrauensvoll zusammenarbeiten, kann ihr Potenzial optimal ausgeschöpft werden. Daher konzentrieren sich die Forschungsaktivitäten unter anderm auf die Themen Erklärbarkeit, Datenschutz, Sicherheit und Robustheit von KI-Technologien.