Schwachstellen vor den Hackern finden: Automatisierte Sicherheitstests von IT-Systemen

Prof. Dr. Marc Rennhard
Leiter Institut für angewandte Informationstechnologie (InIT)
ZHAW School of Engineering

Thurgauer Technologietag, 22. März 2019

IT-Sicherheit in Ausbildung und Forschung an der ZHAW SoE

Zürcher Hochschule
für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- Ausbildung BSc Informatik
  - Spezialisierung in IT-Sicherheit durch breites Angebot an Modulen
  - Ca. 60 Studierende / Jahr
  - Weitere Vertiefung möglich im Rahmen des Master of Science in Engineering
- Weiterbildung CAS Angewandte IT-Sicherheit
  - Starker Fokus auf techn. IT-Sicherheit, neu ab Sep. 2019
- F&E Projekte in Zusammenarbeit mit Firmen
  - 20 grössere F&E Projekte im Bereich IT-Sicherheit in den letzten 10 Jahren
  - Innosuisse (ex KTI), EU-Projekte, direkt finanziert

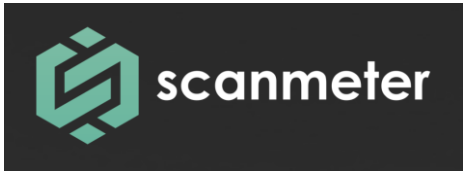
Automatisierte Sicherheitstests von IT-Systemen

Zürcher Hochschule
für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

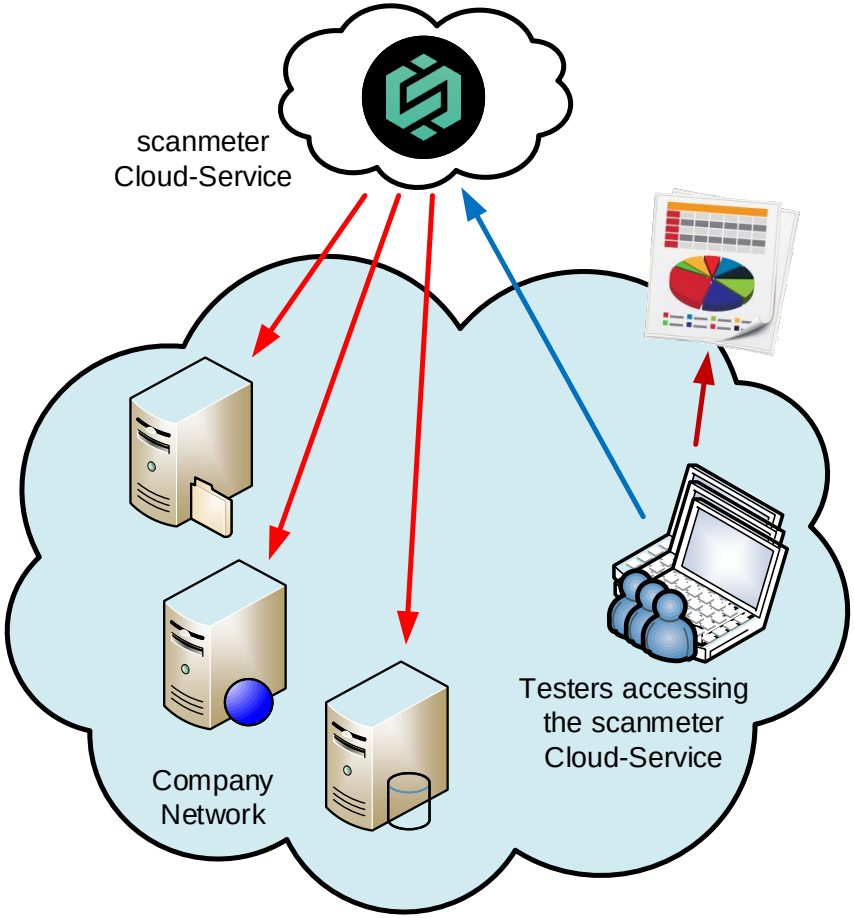
- Manuelle Sicherheitstests von IT-Systemen können zwar gute Ergebnisse produzieren, sie sind aber teuer, langsam und schlecht reproduzierbar

- Automatisierte Tests können Abhilfe bieten
  - Vielzahl von Tools zur Analyse von Code, Systemen und Applikationen
  - Vorhandene Tools sind zwar gut, aber komplex in der Verwendung und heterogen bzgl. Leistungsfähigkeit

- Basierend auf dieser Ausgangslage: Gemeinsames F&E Projekt mit Consecom AG (KTI Projekt)
  - Ziel: Entwicklung eines Service, um Benutzbarkeit und Leistungsfähigkeit von automatisierten Sicherheitstests deutlich zu erhöhen

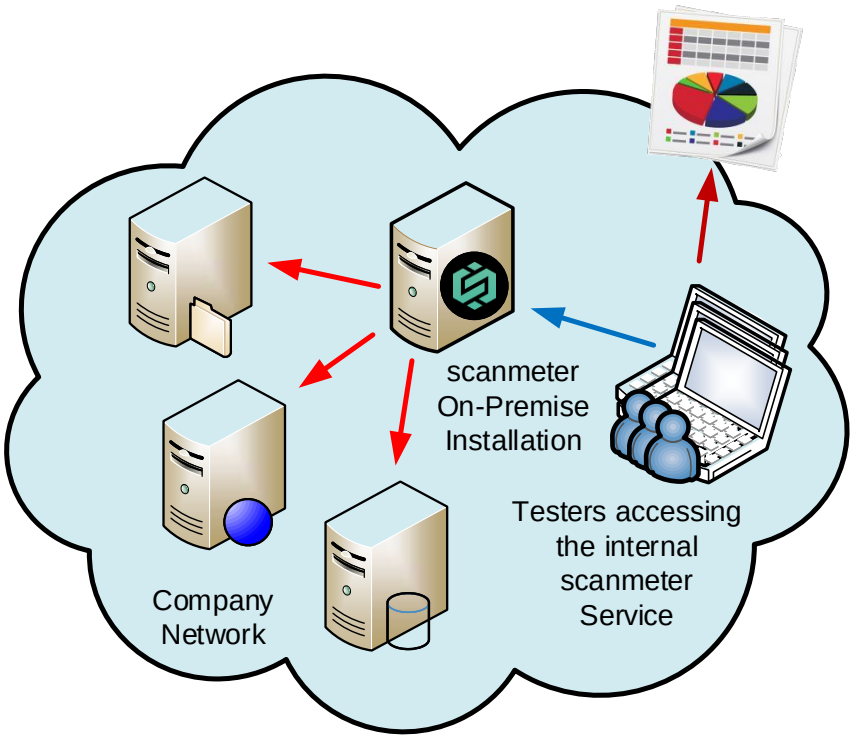


Verwendung von scanmeter



scanmeter Cloud-Service

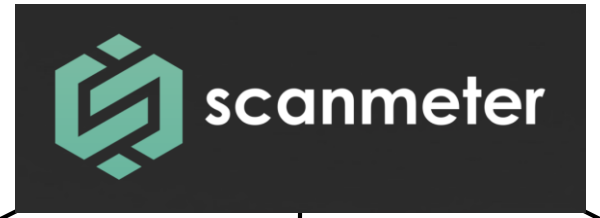
- Sicherheitstest der nach aussen exponierten Systeme und Applikationen



scanmeter On-Premise Installation

- Sicherheitstest der internen und nach aussen exponierten Systeme und Applikationen
- Integration in Software-Entwicklungsprozess

Zentrale Eigenschaften von scanmeter



Integration einer Vielzahl frei verfügbarer Testing Tools

- Rund 20 Tools aus versch. Bereichen
- Code-Analyse, System-Scans, Webapp-Scans

Neuartige Ansätze zur Optimierung des Testprozesses

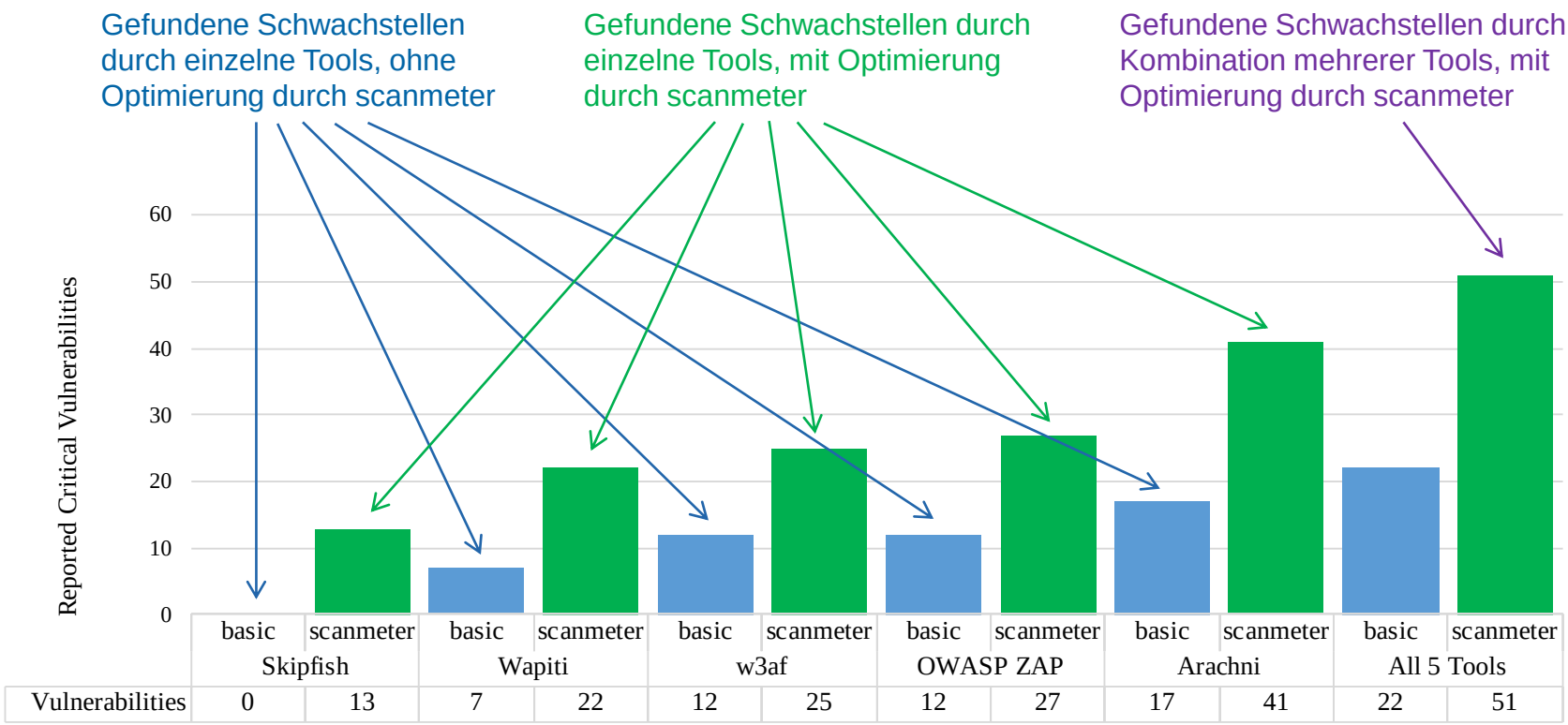
- Erhöhung der Testabdeckung
- Robuste Tests von authentisierten Bereichen

Aggregation der Reports der einzelnen Tools in einen einheitlichen Gesamtreport

- Eliminierung Duplikate
- Beliebige Vergleiche über Testläufe

Evaluation am Beispiel von Schwachstellen in Webapplikationen

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie



- Testset: 7 absichtlich verwundbare Webapplikationen, basierend auf unterschiedlichen Frameworks & Technologien

Esposito, Damiano; Rennhard, Marc; Ruf, Lukas; Wagner, Arno, Exploiting the potential of web application vulnerability scanning, in Proceedings of ICIMP 2018.

Zusammenfassung und Ausblick

- Projektziele erreicht
  - scanmeter findet nachweislich mehr Schwachstellen im Vergleich zur direkten Verwendung von Testing Tools und verbessert die Benutzbarkeit
  - scanmeter erhöht damit den Automatisierungsgrad von Sicherheitstests

- scanmeter wurde kurz nach dem Projektende (Mitte 2018) vom Firmenpartner am Markt lanciert (https://scanmeter.io)

- Seit Februar 2019: Folgeprojekt läuft (finanziert durch Innosuisse), um scanmeter in verschiedenen Dimensionen zu erweitern

Institut für angewandte Informationstechnologie

Zürcher Hochschule für Angewandte Wissenschaften
School of Engineering
InIT Institut für angewandte Informationstechnologie

- Das InIT deckt mit seinen 5 Forschungsschwerpunkten ein breites Spektrum der Informationstechnologie ab
  - IT-Sicherheit, Software Engineering, Usability & Accessibility, Künstliche Intelligenz, Natural Language Processing, Cloud Computing,...

- Weitere Infos: https://www.zhaw.ch/init

- Kontakt: marc.rennhard@zhaw.ch

- Neu ab Sep. 2019: CAS Angewandte IT-Sicherheit
  - https://weiterbildung.zhaw.ch/de/school-of-engineering/programm/cas-angewandte-it-sicherheit.html