mgm

München/HQ Dresden

mgm security partners

mgm security partners deckt das komplette Dienstleistungsspektrum rund um die Web Application Security ab. Wir beraten in allen Fragen der Sicherheit von Webanwendungen und mobilen Apps, führen Penetrationstests und Codeanalysen durch und entwickeln Sicherheitslösungen.

Wir machen Software sicher!

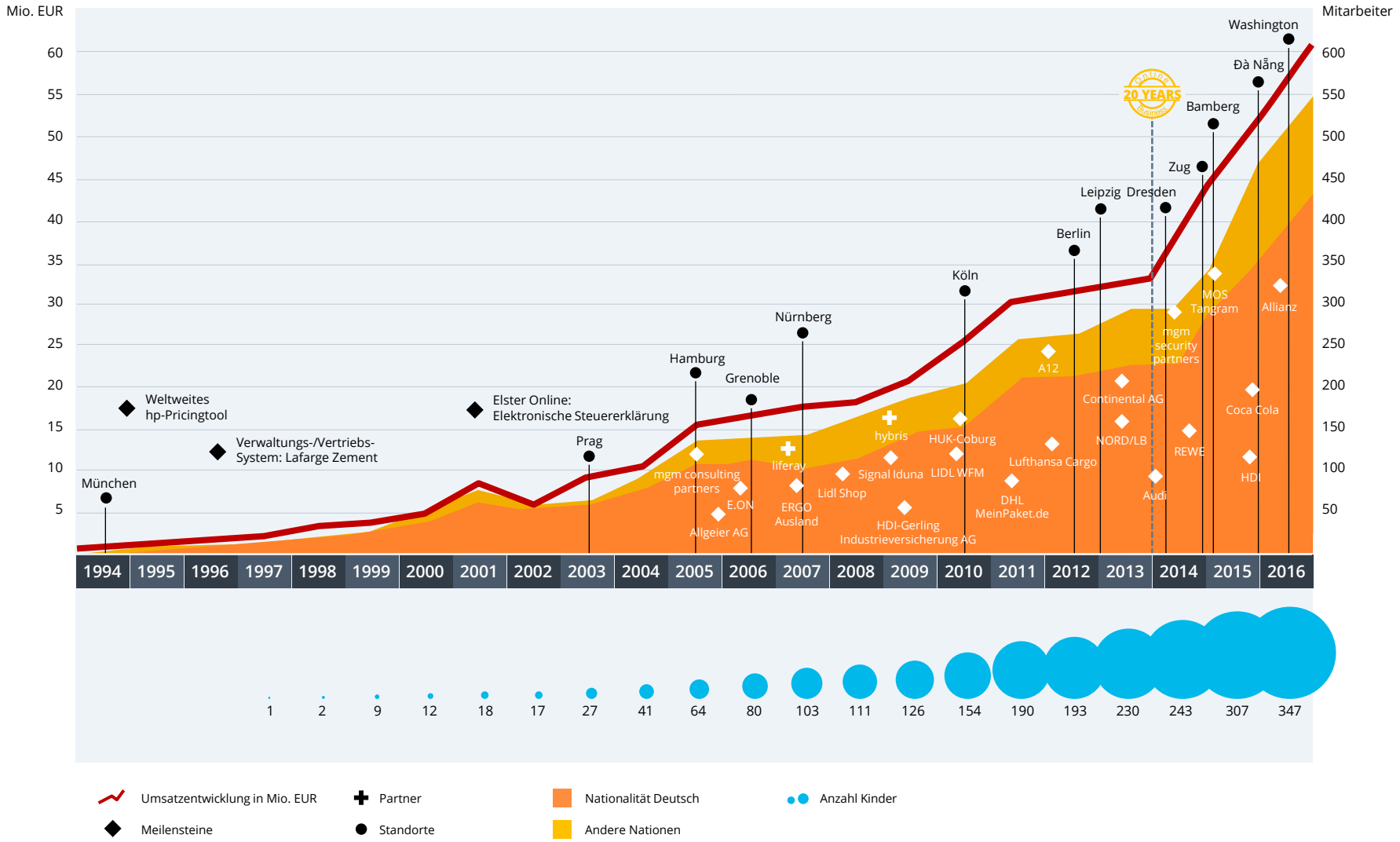
23 Jahre mgm-Gruppe

mgm technology partners

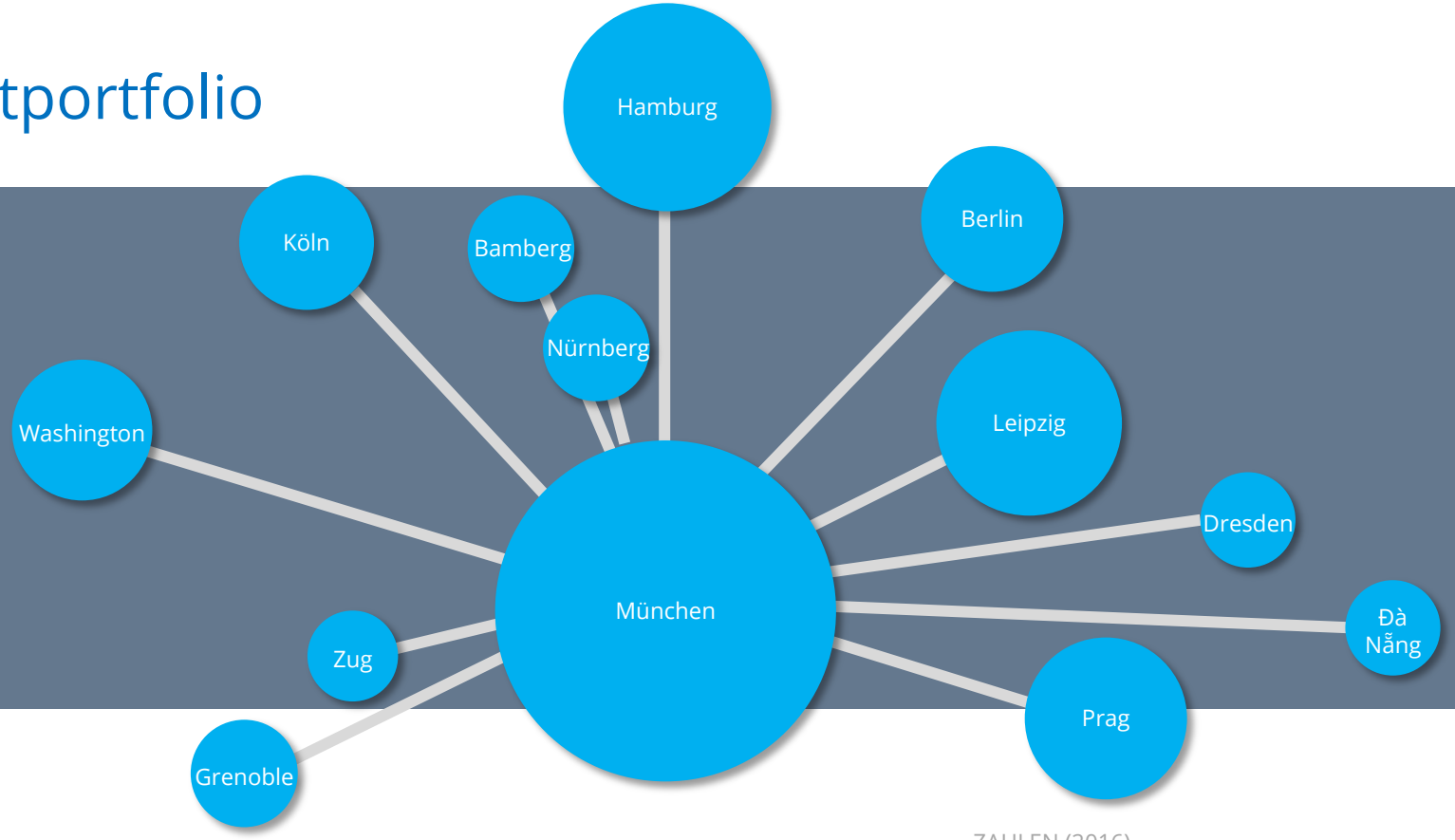
mgm consulting partners

mgm security partners

Mitglied der ALLGEIER



mgm-Gruppe: Das Gesamtportfolio



mgm

	PROFIL	ZAHLEN (2016)
mgm technology partners	Zuverlässige IT-Projektumsetzung für hochskalierbare Webapplikationen: Für E-Commerce, E-Government, Insurance	1994 gegründet 463 Mitarbeiter an 13 Standorten 47,3 Mio. € Umsatz
mgm consulting partners	Management-Beratung auf Augenhöhe: Für Versicherungen, Energieversorger, Handel und IT-Dienstleister.	2005 gegründet 54 Mitarbeiter an 5 Standorten 9,7 Mio. € Umsatz
mgm security partners	Web Application Security von Anfang an: Sicherheitslösungen, Penetrationstests und Codeanalysen	2008 gegründet 26 Mitarbeiter an 2 Standorten 3,9 Mio. € Umsatz

Mitglied der
ALLGEIER

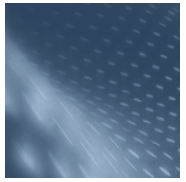
Leistungen

Penetrationstests

Sicherheitsanalysen durch simulierte Angriffe und Analyse des Anwendungsverhaltens von außen.

Security Workshops

Workshops legen in der frühen Phase des Softwareprojekts den Grundstein für nachhaltige Sicherheit.



Sourcecodeanalyse

Auffinden von Schwachsstellen direkt im Code mittels manueller und toolgestützer Inspektion oder komplett automatisch.

Inhouse-Schulungen

Wir geben unser spezialisiertes Wissen an Softwareentwickler, Sicherheitsleute und Manager weiter.

Mobile App Security

Sicherheit durch Analyse des Zusammenwirkens von Client, Server und Kommunikation.

Consulting

Von der Einführung einer Softwaresecurity-Strategie bis zur Integration von Security-Tests in die Deployment-Prozesse.

Penetrationstests

Wir untersuchen Ihre Webanwendungen, mobilen Apps und Webserver mit dem Mittel des Penetrationstests (simulierte Hackerangriffe) auf Schwachstellen. Sie erhalten von uns umfassende, nachvollziehbare Berichte, die für den Fachverantwortlichen eine Entscheidungsgrundlage und den Entwickler konkrete Handlungsanweisungen enthalten.

Umfassend

Die Untersuchung deckt alle 5 Ebenen im Klassifizierungsschema zur Organisation von Sicherheit in Webanwendungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ab und folgt den Empfehlungen des Open Web Application Security Projects (OWASP).

Zuverlässig

Der in unserem Wissenspool hinterlegte Erfahrungsschatz und die hohe Expertise unserer Tester sorgen für höchste Zuverlässigkeit bei der Schwachstellensuche.

Effizient

Dank unserer Erfahrung und durch den Einsatz leistungsfähiger Werkzeuge erreichen wir eine hohe Effizienz – und können entsprechend günstig anbieten.

Security Workshops

Der Security Architekturworkshop stellt die wirksamste und gleichzeitig kostengünstigste Maßnahme dar, um Sicherheit tief in der Anwendung zu verankern.

Der Grundstein für inhärente und nachhaltige Sicherheit einer Anwendung wird in der Designphase gelegt. Dennoch ist es häufig so, dass Softwareentwickler und Architekten sich in dieser Phase ausschließlich auf die klassischen Softwarequalitätsmerkmale konzentrieren und Sicherheitsgesichtspunkte nur am Rande betrachten oder gleich ganz in die Sicherheitsanalyse nach Fertigstellung verlagern. Was dabei herauskommt, ist nachträglich aufgesetzte, schwer zu beherrschende Sicherheit.

Unser Angebot eines Security Architekturworkshops schafft hier Abhilfe. Erfahrene Softwareentwickler setzen sich mit Ihren Architekten zusammen und sorgen dafür, dass “Security by Design” entsteht, u.a. durch Einbeziehung von

- Datensicherungskonzepten
- Ein- und Ausgabevalidierung
- Trust Boundaries
- Sicheren Entwurfspattern
- Security Libraries
- Secure Coding Guidelines
- und durch die Aktivierung der “Bordmittel”, die die jeweiligen Programmierframeworks auf ihre eigene Art und Weise mitbringen.

Mobile App Security

Die Anforderungen an eine schwachstellenfreie Programmierung sind damit ebenso hoch wie bei klassischen Webanwendungen, aufgrund der höheren Komplexität aber zumeist weit schwieriger zu erfüllen.

Apps erwecken den Anschein, dass sie sehr viel geschlossener und damit weniger angreifbar sind als browserbasierte Anwendungen. Doch der Schein trügt, ein Angreifer kann mit seinen Werkzeugen sowohl das Innere der App als auch die Kommunikation und die Eintrittspunkte in die serverseitige Anwendung offen legen.

Wir untersuchen Apps ganzheitlich. Abhängig von der Art der App und dem Schutzbedarf der Daten kommen einzelne oder alle der im Folgenden genannten Maßnahmen zur Anwendung:

Serverseitige Webanwendung

Es werden umfassende Web Application Security Blackbox Penetrationstests auf die Serveranwendung gemäß Beschreibung in diesem Dokument durchgeführt.

Kommunikation

Die Kommunikation wird entschlüsselt und mit geeigneten Testtools umfassend analysiert.

Architektur

Sind an die App aufgrund ihrer Funktionalität, der Sensitivität der Daten oder des Schutzbedarfs höhere Sicherheitsanforderungen gestellt, so wird eine plattformspezifische Architekturanalyse durchgeführt. Dabei wird anhand der technischen Feinspezifikation (oder ähnlichen Beschreibungen) geprüft, ob die Webanwendung die Security-Guidelines des Herstellers beachtet, d.h. die sicherheitsgebenden Plattformeigenschaften dem Schutzbedarf angemessen auf Daten und Funktionen anwendet.

Selektive oder umfassende Codeanalyse

Sind an die App höhere Sicherheitsanforderungen gestellt und legen die Resultate des Penetrationstests oder der Architekturanalyse dies nahe, so wird eine Codeanalyse durchgeführt. Dabei werden im Code all die Stellen und Verarbeitungen untersucht, welche sensitive Daten und Funktionen betreffen. Insbesondere wird die sichere Datenablage von sensitiven Daten auf dem Gerät betrachtet.

In speziellen Fällen mit besonderem Schutzbedarf wird eine umfassende Codeanalyse durchgeführt.

Missbrauchsszenarien und Benutzerfehler

Es werden typische Bedrohungen für Smartphone-Anwendungen betrachtet und das Risiko bewertet, dem die jeweilige App ausgesetzt ist – etwa durch vorsätzliche Handlungen (z.B. Diebstahl) oder Benutzerfehler (z.B. Verlieren).

Sourcecodeanalyse

Die Sourcecodeanalyse deckt Fehlprogrammierungen, die Auswirkungen auf die Sicherheit haben, direkt im Quellcode auf. Sie kann während der Entwicklung durchgeführt werden und führt den Entwickler an die Wurzel des Problems.

Sourcecodeanalyse vs. Penetrationstest

Automatische Sourcecodeanalyse und Penetrationstests haben beide ihre Stärken – auf den richtigen Einsatz kommt es an! Hier einige Merkmale dieser Ansätze:

Automatische Sourcecodeanalyse

- Systematischer, umfassender Ansatz
- Die Beschreibung der gefundenen Schwachstellen und die Maßnahmenempfehlungen sind in der Sprache des Entwicklers
- Abdeckung der Analyse ist nachvollziehbar, zumeist Vollabdeckung
- Liefert Aussagen bereits während der Entwicklung
- Komponententests sind möglich
- Leistet einen effektiven Beitrag zur Schulung der Entwickler
- Sicherheitswissen wird Teil des Projektes bzw. der ganzen Organisation, nicht einzelner Personen
- Findet Schwachstellen, die ein Penetrationstest nicht auffinden kann

Penetrationstest/Externe Analyse

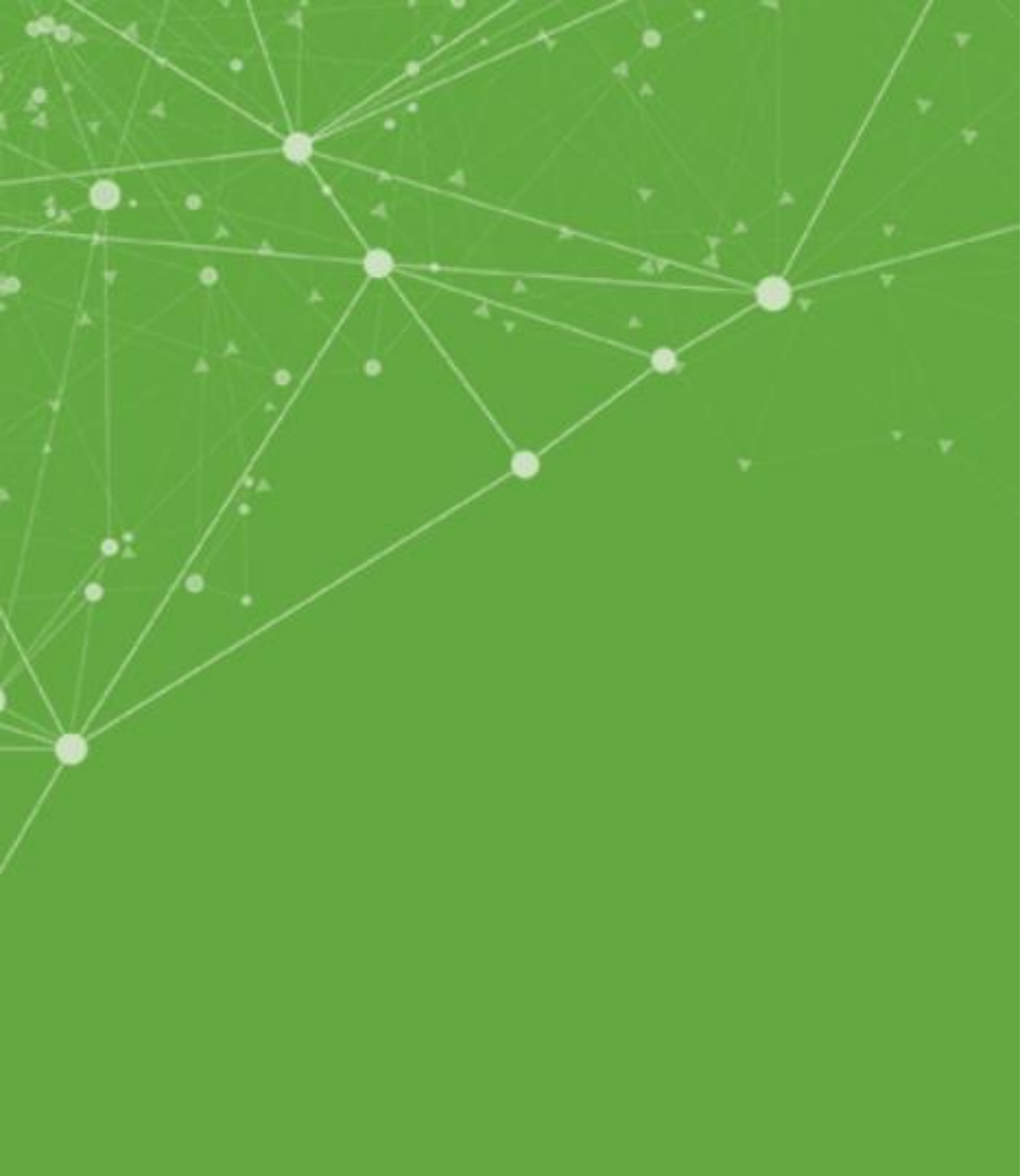
- Bezieht das Gesamtsystem (Webserver etc.) in die Untersuchung mit ein
- Leichte Durchführbarkeit
- Findet Schwachstellen, die eine Sourcecodeanalyse nicht oder nicht sicher auffinden kann

Manuelle Sourcecodeanalyse

Dort, wo eine manuelle Sourcecodeanalyse auf Sicherheitsprobleme gewünscht oder erforderlich ist, bieten wir mit unserem Verfahren SCA-Quick-Wins einen schlanken und leistungsfähigen Ansatz.

Automatische statische Codeanalyse

Abgestimmt auf Ihre Anforderungen setzen wir eines der am Markt verfügbaren Tools zur statischen Codeanalyse ein – auch Static Application Security Testing (SAST)-Tool genannt – und bereiten die Ergebnisse in einer für Verantwortliche und Entwickler leicht verstehbaren Form auf.



Inhouse-Schulungen

Wir geben unsere über 10-jährige Erfahrung in der Entwicklung sicherer Webanwendungen und der Herstellung von Web Application Security an Softwareentwickler, Sicherheitsverantwortliche und Manager weiter.

Aus der Praxis für die Praxis!
Unsere Trainer sind keine Lehrer, sondern aktiv tätige Experten mit langjähriger Erfahrung im unterrichteten Fachgebiet.

Immer auf dem neuesten Stand!
Die Seminare werden ständig der aktuellen Entwickung angepasst – sowohl was neue Angriffsvarianten als auch Lösungsansätze betrifft.

Unsere Security Trainings

Awarenesstraining

- Führt die Folgen unzureichender Web Application Security vor Augen
- Liefert eine Übersicht über Herangehensweisen
- Plakative, realitätsnahe Beispiele
- 2- bis 4-stündiger Vortrag oder 1-Tages-Training

Best Practices für sichere Web-Anwendungen

- Darstellung von Bedrohungen, Schwachstellen und Angriffstechniken
- Konkrete, an der Ursache ansetzende Gegenmaßnahmen (Secure Coding)
- Anpassbar: Abdeckung der OWASP-Top 10 oder weit darüber hinaus
- Umfassende Lösungsansätze für nachhaltig sichere Webanwendungen

Secure Coding mit Java EE

- Konkrete Secure Coding Guidelines für Java
- Framework-bezogene Sicherheitsmaßnahmen
- Einsatz von Security-Libraries
- Verwendung der OWASP Enterpreise Security ALI (ESAPI)

Advanced Web Application Security Testing

- Einführung in das Testen von Webanwendungen aus der Angreiferperspektive (Penetrationstest)
- Erlernen fortgeschrittener Techniken
- Einsatz der Tools burp suite (freie Version) und sqlmap

Individualschulungen

Wir bieten alle unsere Schulungen individuell auf Ihre Bedürfnisse zugeschnitten oder in Form von Workshops an, mit denen wir Sie bei der Herstellung der Web Application Security, dem Secure Design Ihrer Anwendung oder der Schwachstellen-behebung unterstützen – zum Beispiel auf Basis einer erfolgten Sicherheitsanalyse.

Consulting

Wir beraten auf der Basis von mehr als 10 Jahren praktischer Projekt- und Systemerfahrung und überschauen alle Aspekte, Ansatzpunkte und Maßnahmen von Sicherheit auf Anwendungsebene

Die Web Application Security bietet ein sehr breites und mittlerweile auch unübersichtliches Spektrum an Möglichkeiten zur Herstellung von Sicherheit. Ein Patentrezept oder ein für alle Unternehmen gleichermaßen gültiges Vorgehen existiert nicht.

Es gilt, die für die eigene Situation am besten passenden Herangehensweisen zu finden und diese in eine unternehmensweite Software Security Strategie münden zu lassen.

Wir nutzen moderne Methoden und Vorgehensmodelle, um Unternehmen, Abteilungen oder Teams bei der Findung der richtigen Strategie und dem Aufbau umfassender Software- und Anwendungssicherheit zu unterstützen:

OpenSAMM, das frei verfügbare *Software Assurance Maturity Model*, mit dem auf sytematische Weise der Ist-Stand in Sachen Web Application Security analysiert, geeignete weitere Maßnahmen identifiziert und in ihrer Strenge und Ausprägung definiert sowie einem Verbesserungsprozess unterworfen werden können.

BSIMM (*Building-Security-In Maturity Model*) ist OpenSAMM sehr ähnlich. Wir setzen es vornehmlich ergänzend dazu ein, da es in einigen Bereichen eine größere Klarheit besitzt.

Roadmap-Workshop

Einen guten Einstieg in die Thematik bietet in den meisten Fällen unser **Roadmap-Workshop**. Er beinhaltet die folgenden vier Schritte:

1. **Bestandsaufnahme**
   Ergebnis: Ein Softwareinventar liegt vor und die einzelnen Bestandteile sind Risikoklassen zugeordnet.
2. **Planung**
   Ergebnis: Der Vorgehensplan (“Roadmap”) liegt vor.
3. **Umsetzung Phase 1**
   Bei Altanwendungen geht es primär darum, Sicherheitsprobleme festzustellen und auf möglichst wirtschaftliche Weise Gegenmaßnahmen anzuwenden. Bei Neuanwendungen ist das Problem an der Wurzel zu lösen und es sind organisatorische und den Software Development Lifecycle (SDLC) verbessernde Maßnahmen umzusetzen.
4. **Weitere Phasen**
   Je nach den individuellen Anforderungen und Sicherheitszielen werden weitere Umsetzungsphasen geplant. Der typische zeitliche Planungshorizont liegt in der Größenordnung von 3 Jahren

Papers

HTML 5 Security (Artikel in iX 1/2013)

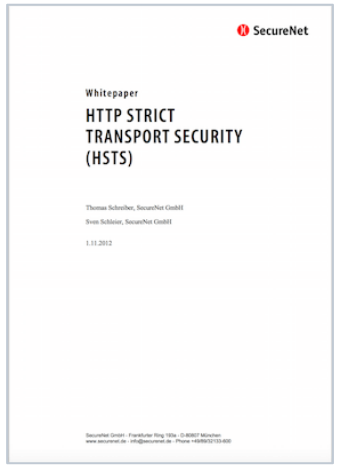
Beim kommenden Webstandard HTML5 haben sich die Entwickler in Sachen Sicherheit viel Mühe gegeben. Doch mit den neuen Features wächst auch die Komplexität und damit die Angriffsfläche. Eine Übersicht über verbleibende und neue Risiken sowie die Anwendungssicherheit erhöhende Konzepte von HTML5.

iX-Extra: Sicherheit bei Webapplikationen beginnt mit der Entwicklung

Der iX-Artikel gibt einen Überblick über den Stand der Web Application Security und Ansatzpunkte zur Herstellung sicherer Webanwendungen.

Aktuelle Verbreitung von HTTP Strict Transport Security (HSTS)

Das Dokument gibt die Ergebnisse einer Untersuchung zur Verbreitung des HSTS Server Response-Headers unter den weltweit 1 Mio. meist-besuchten Websites, den darin enthaltenen rund 40.000 deutschen Websites sowie auf 424 deutschen Onlinebanking-Websites wieder. Die Untersuchung zeigt, dass diese wichtige Sicherheitsmaßnahme bisher noch kaum eingesetzt wird.



Whitepaper: HTTP Strict Transport Security (HSTS)

In diesem Whitepaper erklären wir SSL-Strippung und geben konkrete Gegenmaßnahmen an. Dabei steht der HSTS-Header im Vordergrund. Da diese Schutzmaßnahme aber eine Lücke offen lässt und der Header auch noch nicht von allen Browsern unterstützt wird, werden weiterführende Empfehlungen gegeben.

Einbruchsichere Webanwendungen mit Java-Frameworks

HDIV und Stinger sind zwei neue freie Java-Frameworks, mit denen eine weitreichende Absicherung von Java-Anwendungen gegen Hackerangriffe möglich ist. Der Artikel beschreibt die Einsatzmöglichkeiten dieser mächtigen Bibliotheken im Umfeld von Java EE, Struts und Spring.

Die Datenbank als Erfüllungsgehilfe für Datendiebe

Eine Kurzeinführung in Injection Angriffe

In diesem Whitepaper schlagen wir den Bogen von der “normalen” und der Blind SQL-Injection über die Advanced SQL-Injection bis hin zur ORM-Injection, die es ermöglicht, SQL-Injection durch moderne O/R-Mapper in die Datenbank zu schleusen.

Management

Thomas Schreiber

Gründer und Geschäftsführender Gesellschafter

Berater für Web Application Security und Seminarleiter.

Alois Richthofer

Leiter Entwicklung Sichere Software

Co-Leitung von mgm security partners. Leitung komplexer Projekte.

Mirko Richter

Geschäftsstellenleiter Dresden

Softwareentwickler und –architekt. Spezialist für Sicherheits-beratungen und -analysen sowie Seminarleiter.

München

Dresden

mgm security partners GmbH

Standort München

Frankfurter Ring 105a
80807 München
Tel.: +49 (89) 35 86 80-880
Fax: +49 (89) 35 86 80-338
www.mgm-sp.com

mgm security partners GmbH

Standort Dresden

Königsbrücker Straße 34
01099 Dresden
Tel.: +49 (351) 465 662-910
Fax: +49 (351) 465 662-911
www.mgm-sp.com