
IBM Tivoli Security Day: X-Force Trend and Risk Report 2011

Kassel, 14. September 2011



Agenda

- Aktuelle Sicherheitslage
- Kassel Lab

Aktuelle Sicherheitslage

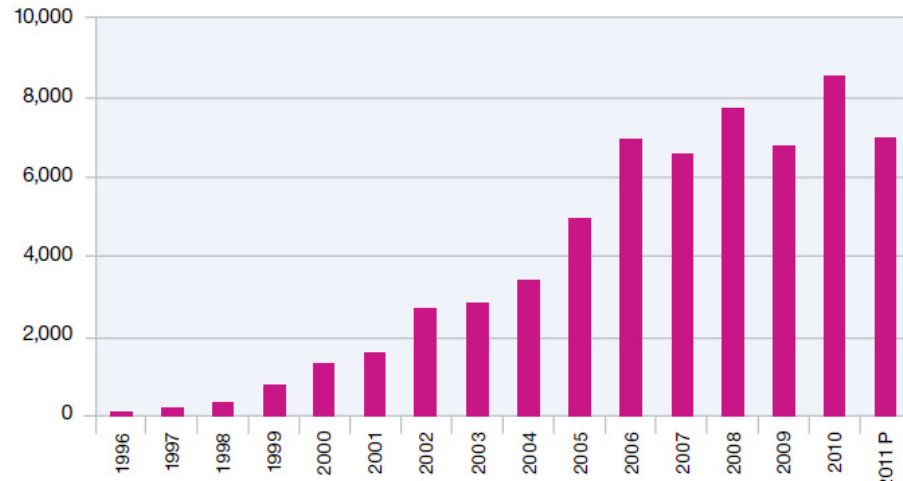


Highlights aus dem X-Force Bericht 2011:

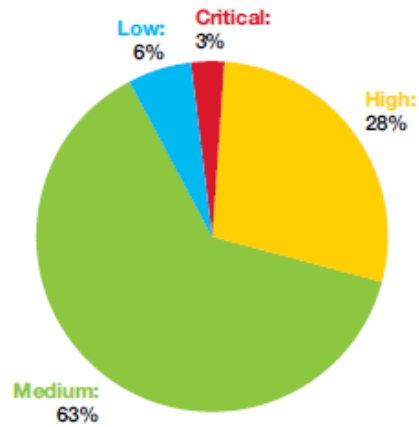
- Die Anzahl der aufgedeckten Schwachstellen in 2011 bewegt sich auf dem Niveau von 2006.
- Der Anteil der Schwachstellen in Web Applikationen ist in 2011 von 49% auf 37% stark zurückgegangen.
- Das traditionelle E-Mail Phishing ist weiter auf dem Rückzug. Nur noch 0.01% aller Spams sind E-Mail Phishings.
- Mobile Endgeräte (Smartphones) werden zunehmend Ziel von Malware. Der in 2010 erkennbare Trend setzt sich ungebremst fort.

Anzahl neu entdeckter Schwachstellen

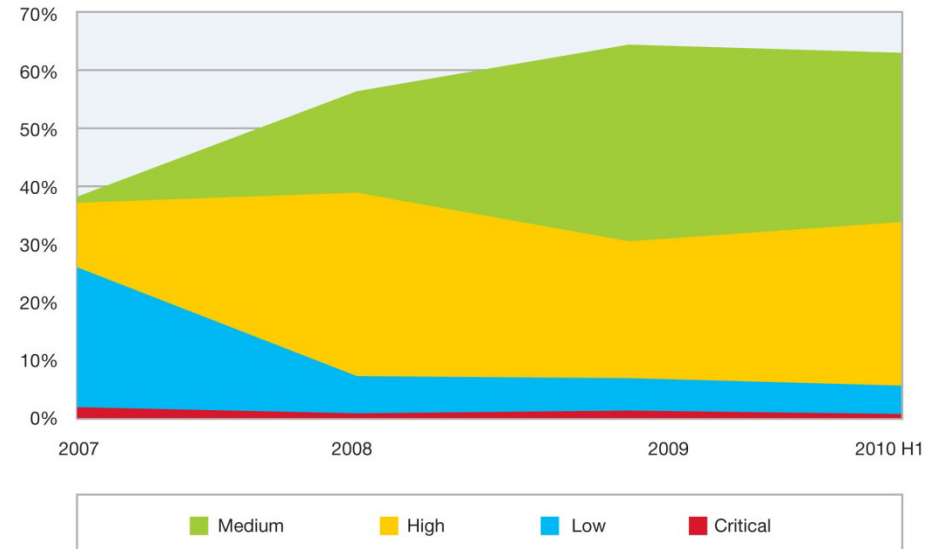
Vulnerability Disclosures Growth by Year
1996-2011 (2011 Half-year Projection)



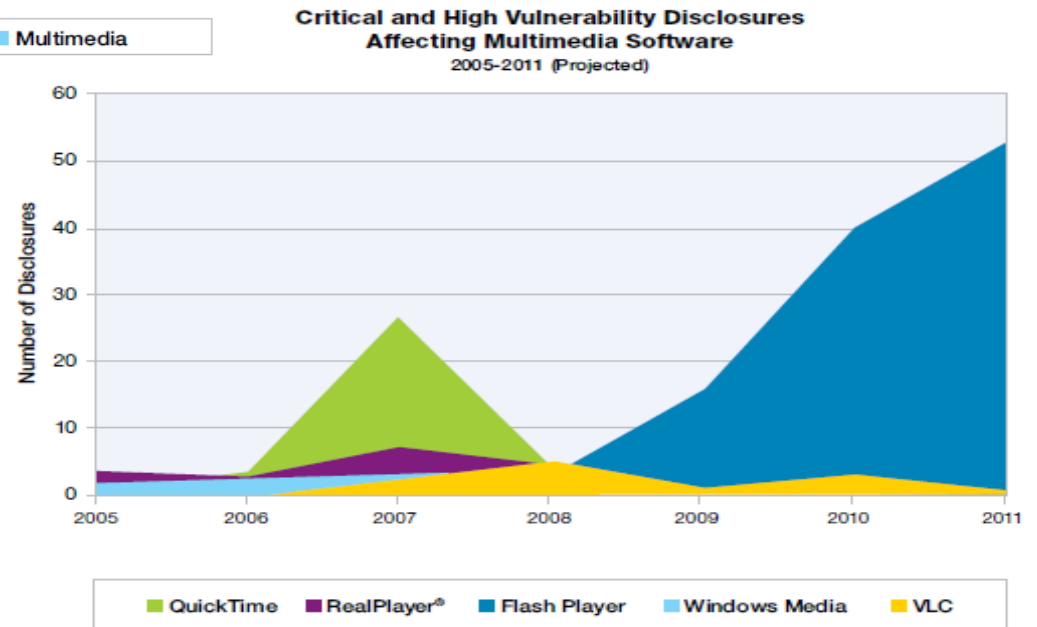
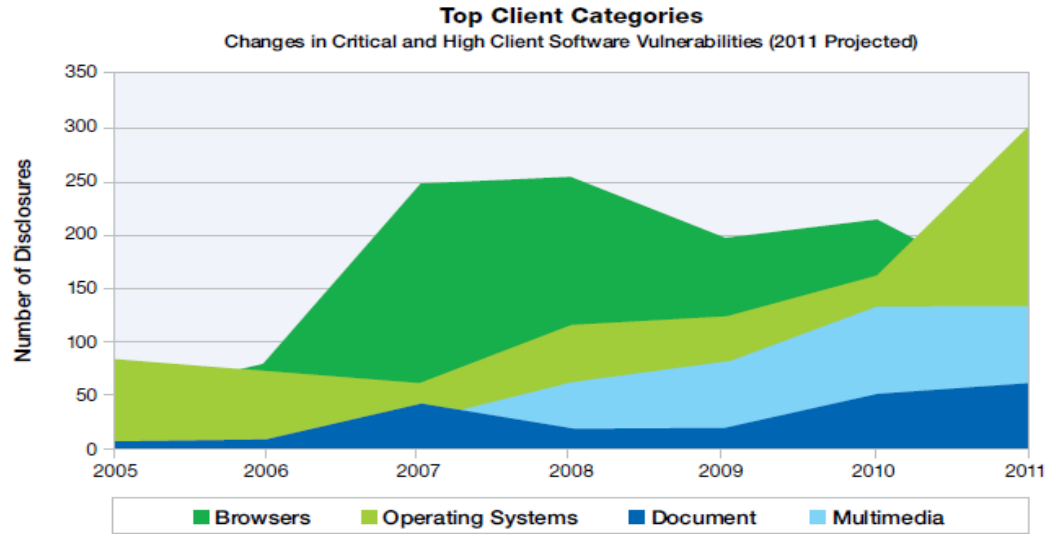
2011 H1



CVSS Base Scores, Vulnerability Disclosures by Severity
2007-2010 H1

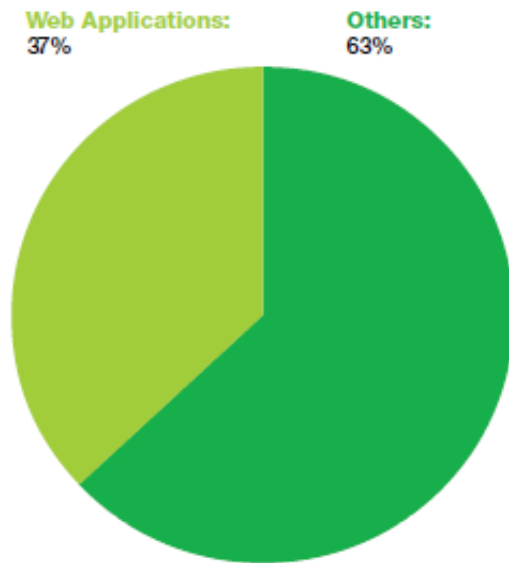


Wo befinden sich die Schwachstellen?

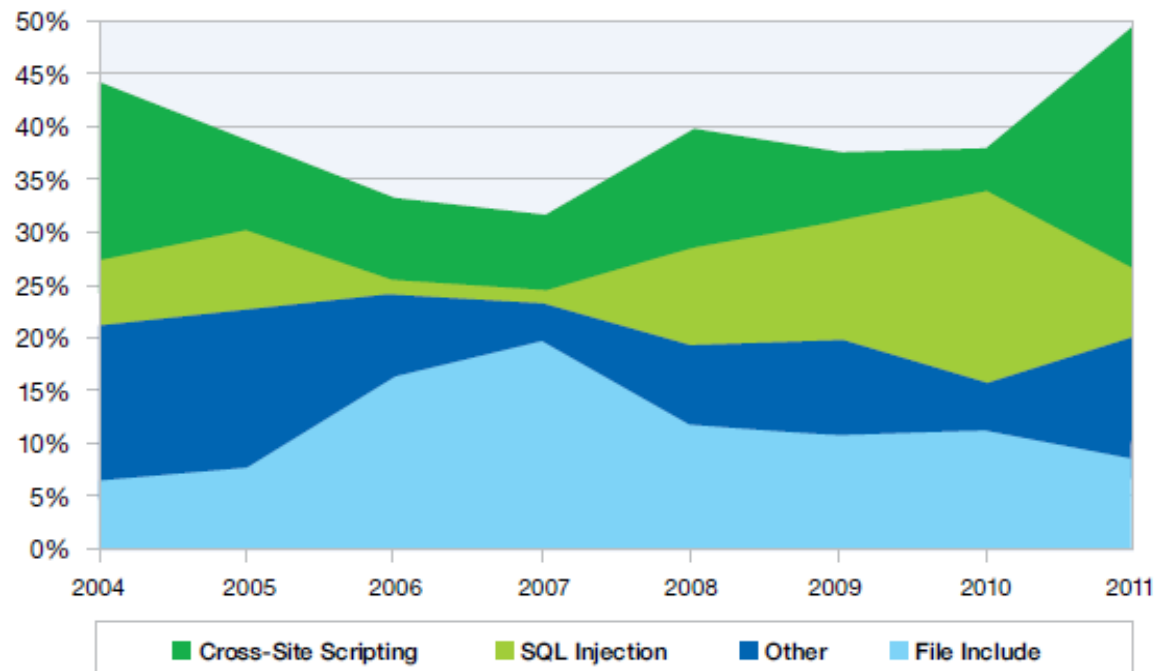


Schwachstellen in Web-Applikationen

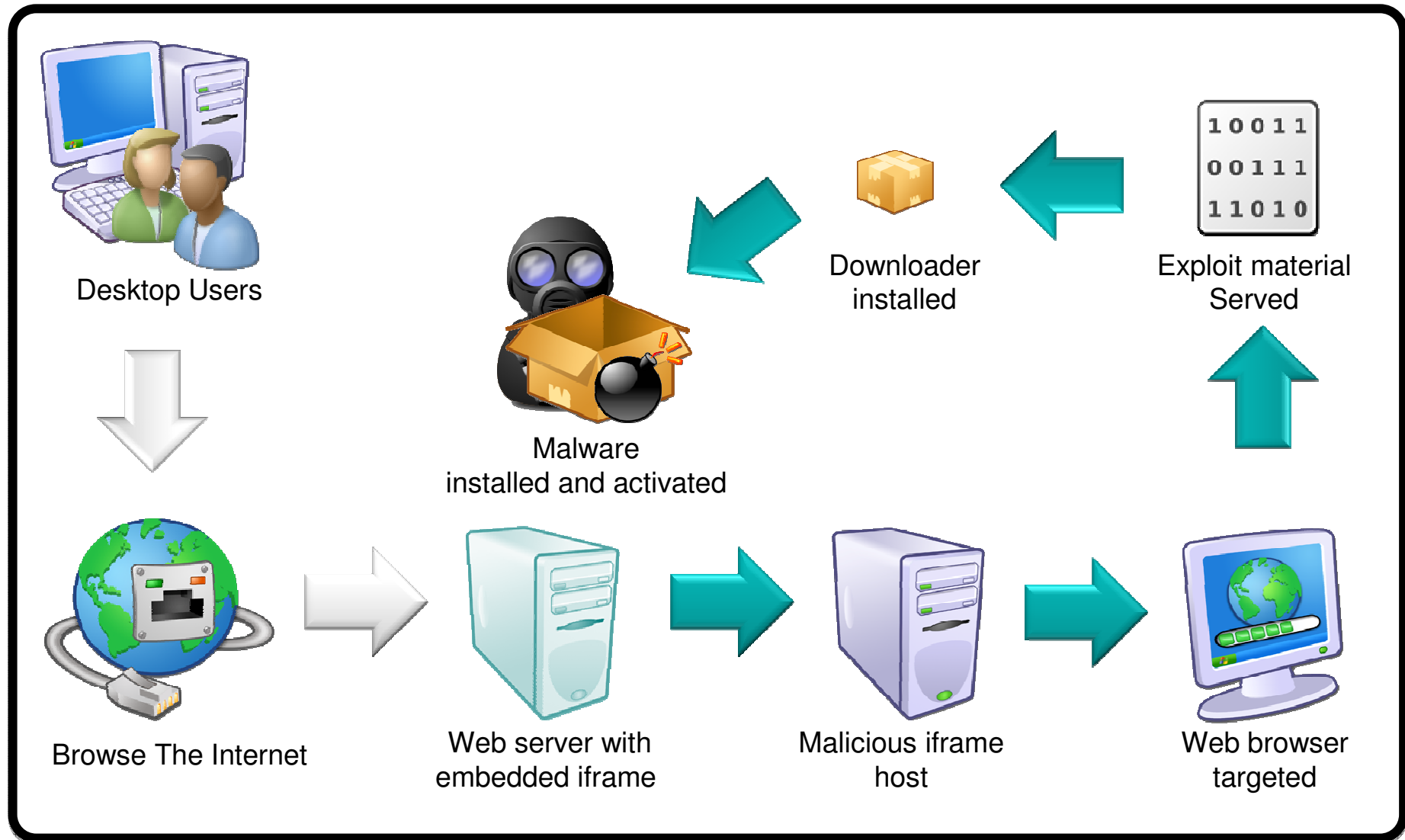
Web Application Vulnerabilities
as a Percentage of All Disclosures in 2011 H1



Web Application Vulnerabilities by Attack Technique
2004-2011 H1



The drive-by-download process



Bot Net Infrastrukturen

- Um Zeus hat sich eine komplette Schattenwirtschaft gebildet:
 - Angepasste Versionen des Toolkits mit spezial plugins
 - Konfigurations Dienstleistungen
 - Hosting und kompletter managed Service
 - Hart umkämpfter Markt (Zeus <-> SpyEye)

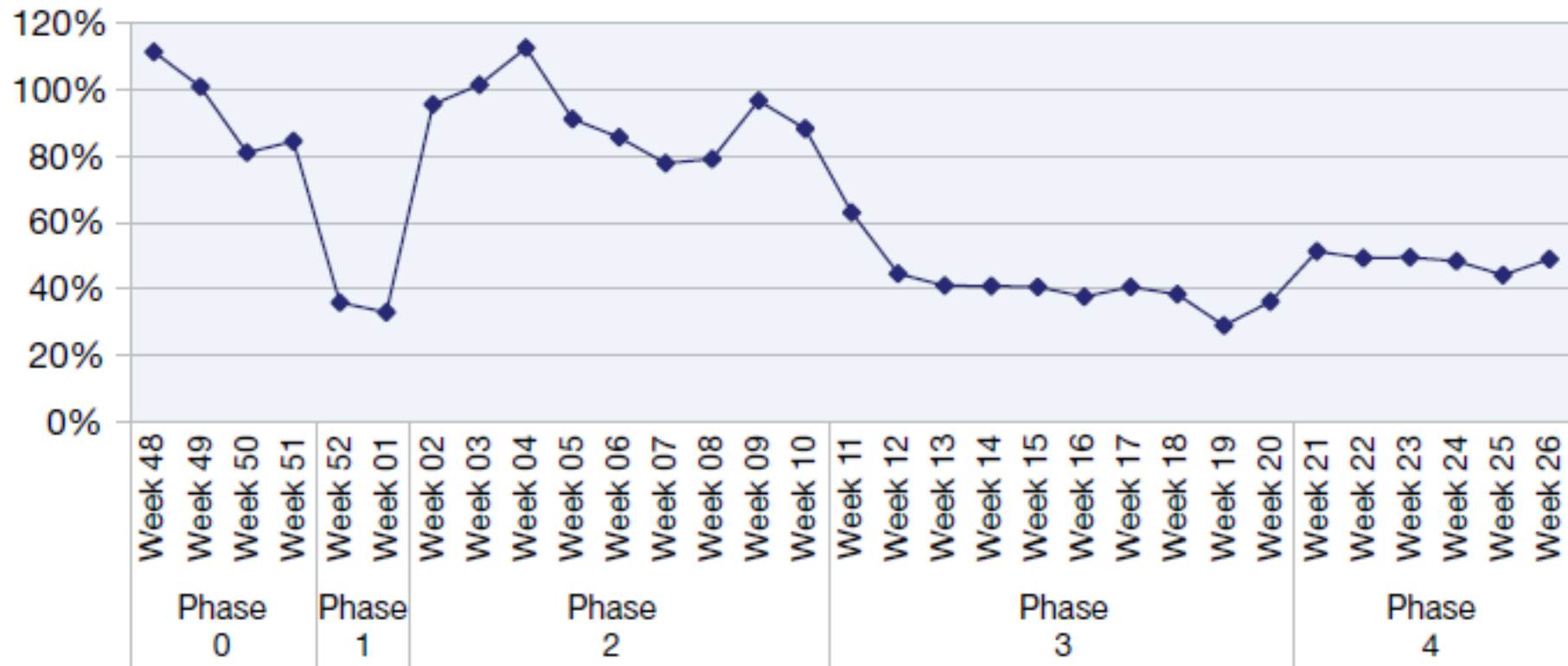
<p><u>[\$20] Zeus 1.2.7.19 BINS [Buildded Bot] (1 2 3)</u> b1sh0p</p>
<p><u>\$100 - Zeus 1.2.9.3 with FF & Opera Module [Only 3 sales!!] (1 2)</u> Bankjob</p>
<p><u>Schwarze Sonne RAT 0.2 Beta (1 2 3)</u> slayer616</p>
<p><u>Selling Zeus 1.2.7.19 with FireFox module enabled + Free BP hosting</u> DarkNet</p>
<p><u>Zeus 1.2.7.19 - FF module Enabled = 30\$:d (1 2 3)</u> Zeusf0sh0</p>

5-~~00000000~~31
 setupservice@~~xxxx~~.ru
 BL:146 TL:0
 -
 Setup Public Zeus - free
 Setup Private Zeus - Details in icq\msn
 (Opera 10.10 & FF 3.5.5)
 Private Exploit System - Details in icq\msn
 I will help to rent hosting for Zeus - cheap and quickly
 -

Spam

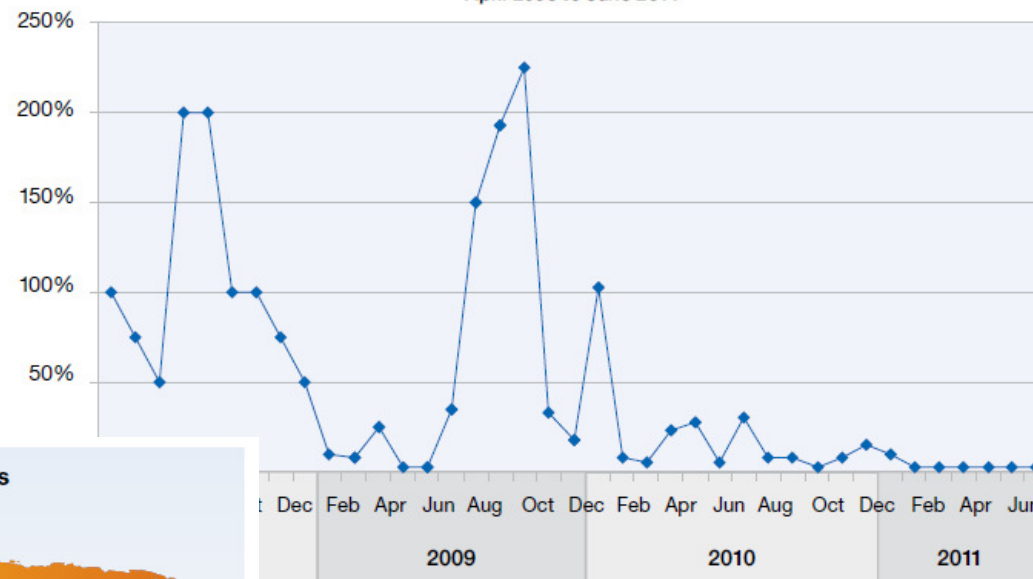
Weekly Spam Volume During Botnet Take-down

December 2010 to June 2011



Phishing

Phishing Volume Over Time
April 2008 to June 2011



Geographical Distribution of Phishing Senders
2011 H1

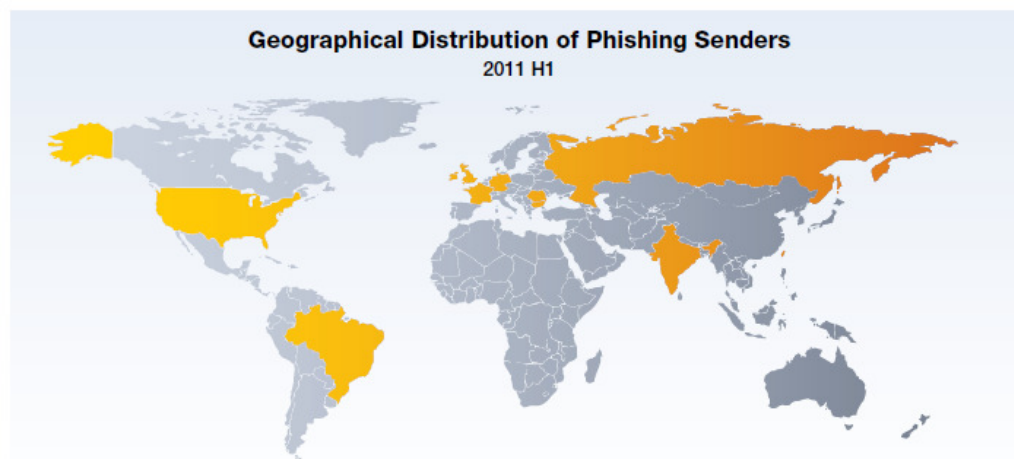
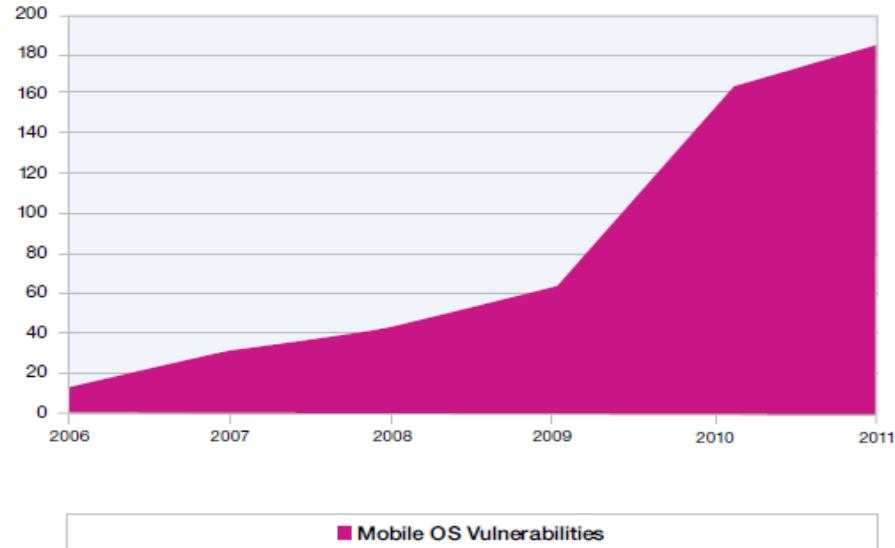


Figure 24: Geographical Distribution of Phishing Senders – 2011 H1

Country	Quota	Country	Quota
USA	41.5%	India	3.0%
United Kingdom	6.8%	France	2.9%
Brazil	3.5%	Taiwan	2.7%
Bulgaria	3.2%	Germany	2.7%
Romania	3.2%	Russia	2.6%

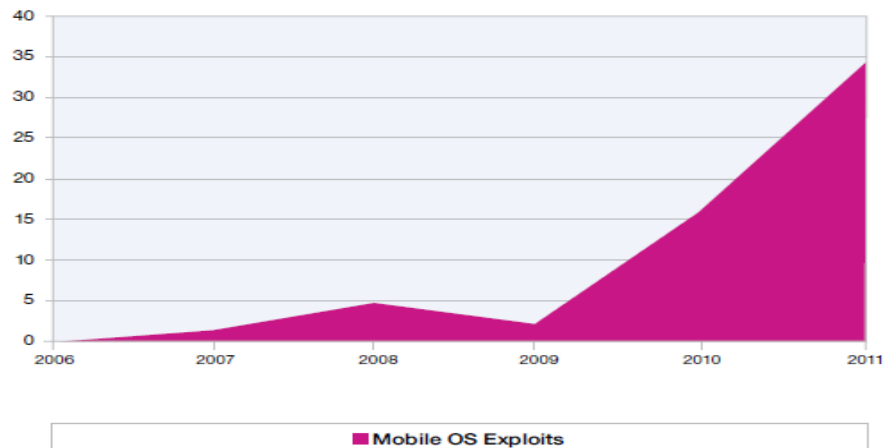
Ausbreitung von Mobilgeräten erzeugt neue Risiken

Total Mobile Operating System Vulnerabilities
2006-2011 (Projected)



- Signifikanter Anstieg sowohl der Anzahl entdeckter Sicherheitslücken als auch die Anzahl der Exploits
- Hauptsächlich gemeinsame Komponenten (für Desktop und Mobile) betroffen

Mobile Operating System Exploits
2006-2011 (Projected)



For More IBM X-Force Security Leadership



X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security,. Find out more at <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>



X-Force Security Alerts and Advisories

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at <http://xforce.iss.net/>



X-Force Blogs and Feeds

For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at <http://iss.net/rss.php> or the Frequency X Blog at <http://blogs.iss.net/rss.php>

Kassel Lab



Products, Services, internal Applications, Technologies, ...

- Key Products

- Lotus Protector for Mail Security
 - ICSA Certified
 - available as virtual and software appliance (HW independent)
 - Worldwide IBM rollout planned for 2011
 - Integrated in Lotus Live

- SDKs (Software Development Kits)
 - Spam Filter
 - URL Filter
 - Web Application Control (WAC)
 - IP Reputation (IPR)



- X-Force Research for Spam detection, Web classification, WAC and IPR
- X-Force data center operations to provide content streams for our Products
- X-Force Trend and Risk Report



Key Customers / IBM Product Integrations

- IBM Product Integrations:

- Lotus Live
- MIOP - Web filter enabled cache for Mobile Broadband Provider (at UMTS access points)
- NG Firewall (ISS)
- ISS Proventia Multifunctional Appliance
- Tivoli Appscan
- Tivoli WebSeal
- IBM Developerworks
- Lotus Foundation

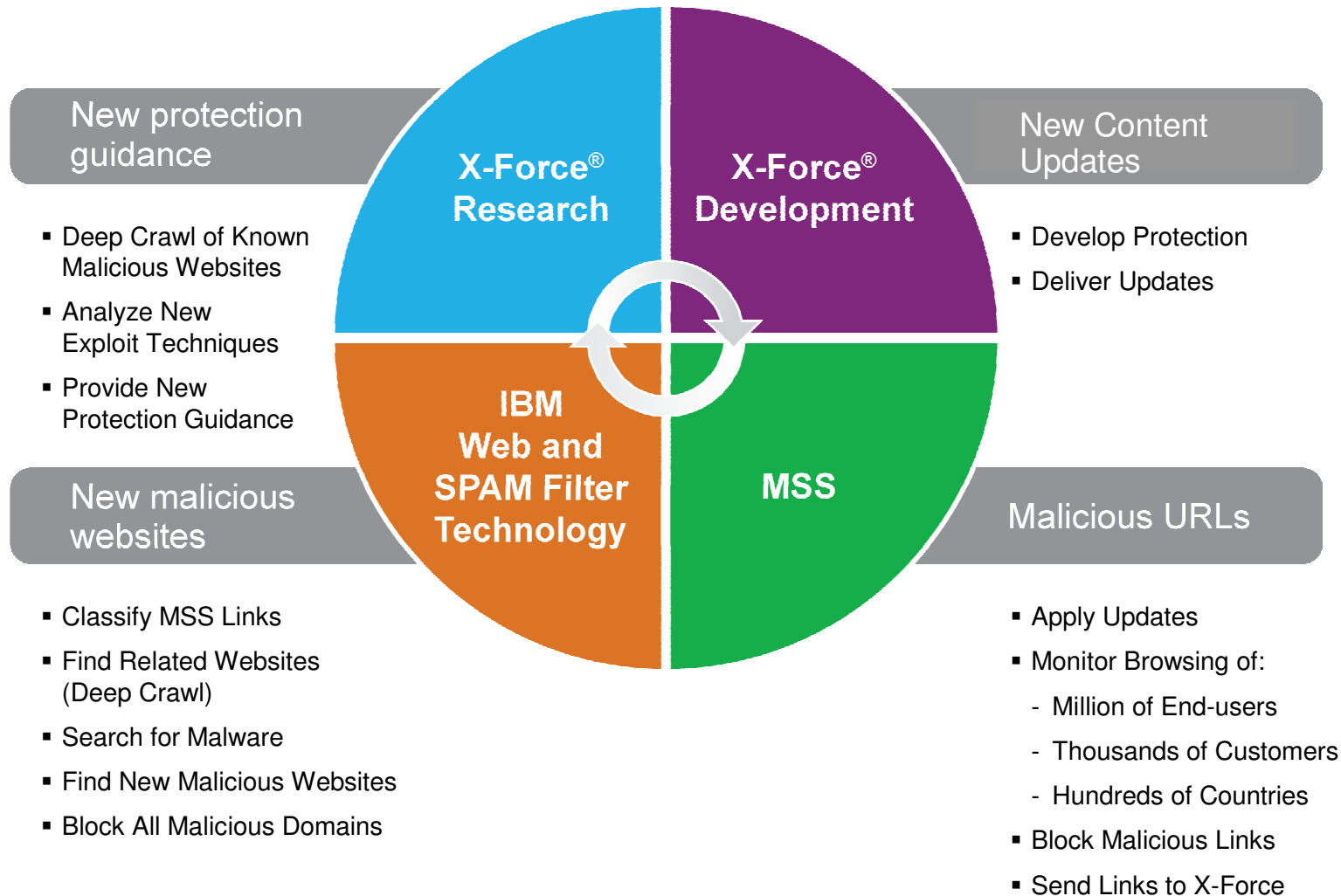


- Key OEM Customers:

- Aladdin
- ArtsAndTV
- Avira
- Cyan Networks
- Barracuda
- Finjan
- Symantec
- T-Online
- TimeForKids



IBM X-Force web intelligence lifecycle



World's largest URL filter list

■ Aktualität

- Crawler sammeln an 365 Tagen, 24 Stunden pro Tag Inhalte aus dem Internet -> **200 Million Inhalte pro Monat**
- Kunden erhalten täglich mehrmals täglich Updates -> **150,000 einzelne Änderungen**

■ Qualität

- Größte URL-Datenbasis erfüllt fast jedes Filterkriterium durch indexierte URL's -> **68 Kategorien**

■ Quantität

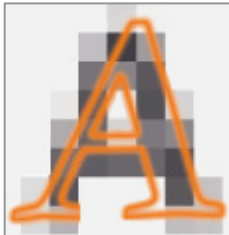
- Weltweit größte URL-Filterliste enthält **170 Millionen URL's**
- Weltweit größte Datenbank mit mehr als **15 Milliarden** ausgewerteter Internet-Inhalte



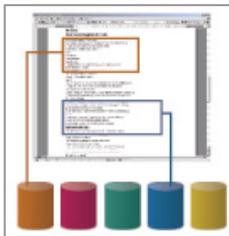
filter database



Core technologies



Text recognition (OCR)



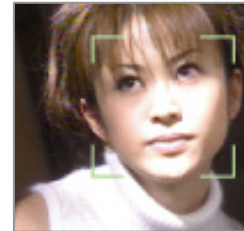
Text classification



Comparison of similarity and identity



Object recognition



Face recognition

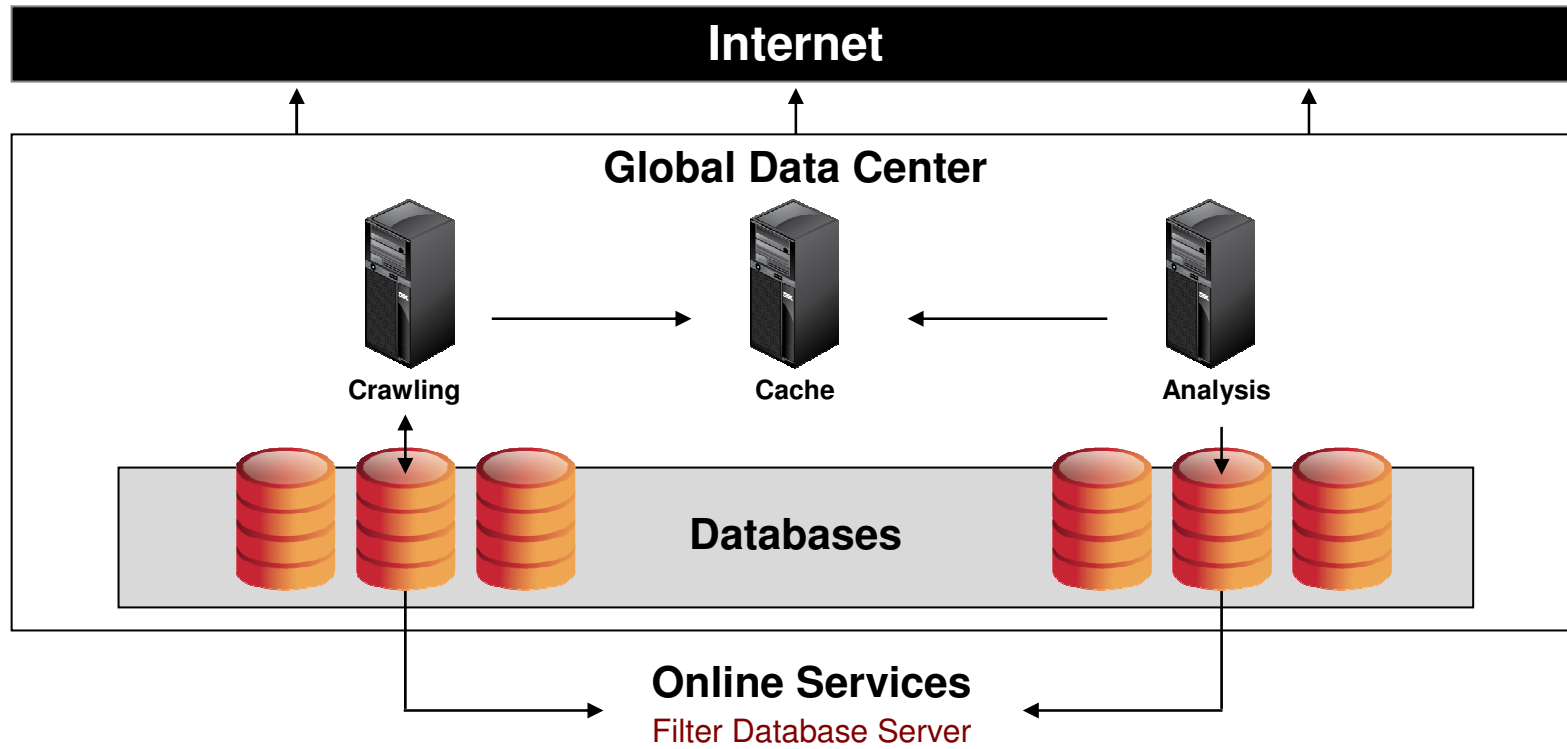


Pornography & nudity detection



Digital fingerprint

Infrastructure



Crawling

- Crawler robots search the web in parallel.
- They download the websites and images, and place them in the cache. The information is stored in the database.

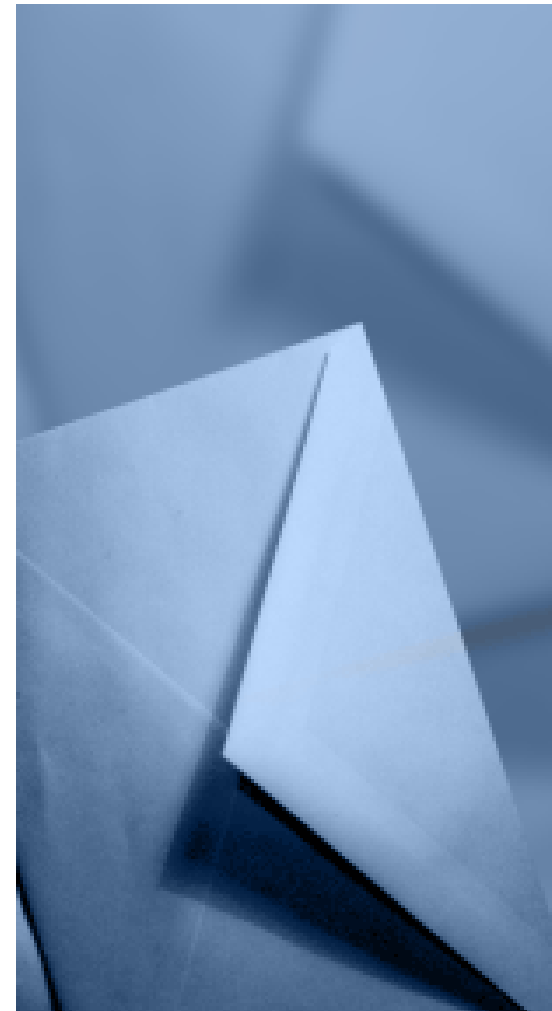


Analysis

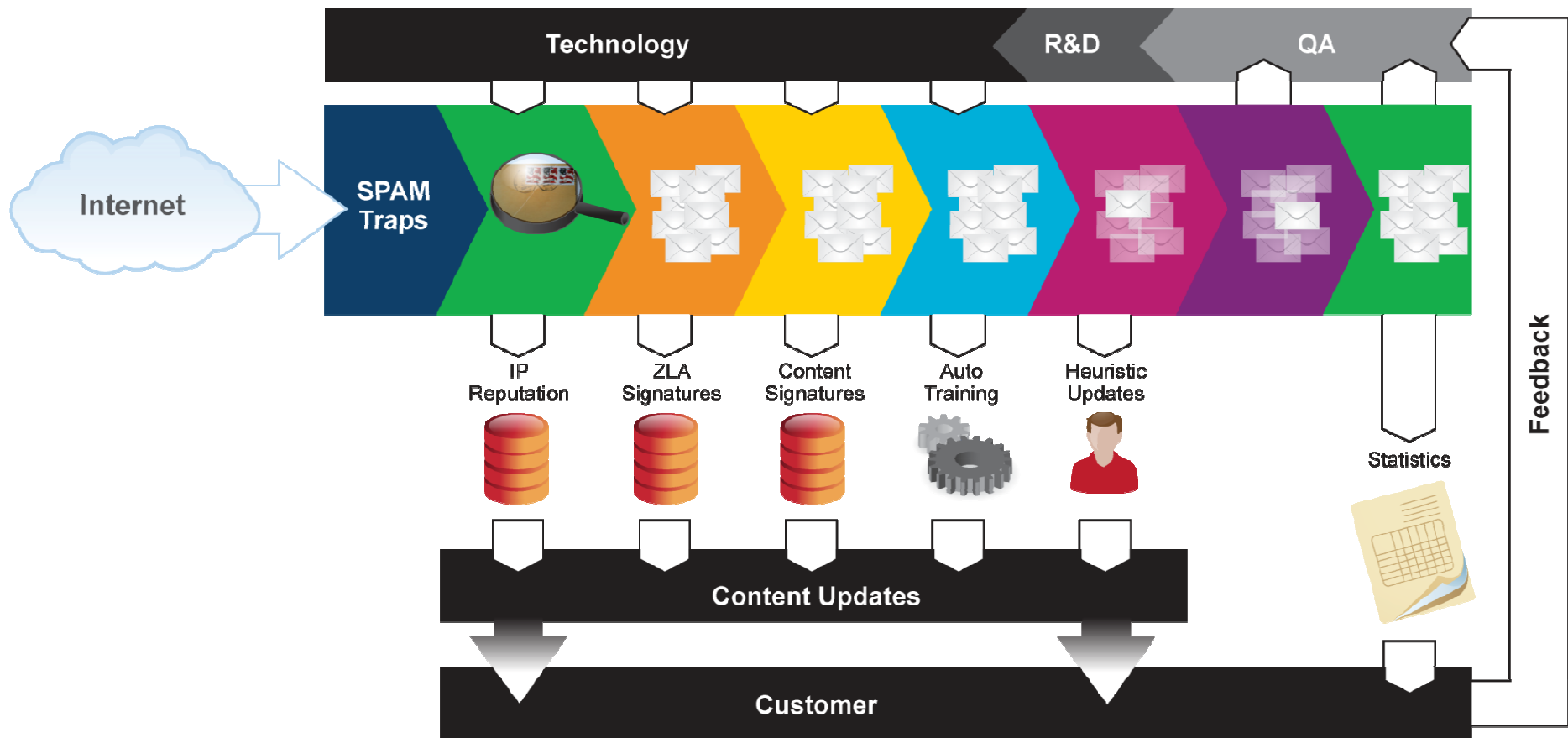
- Server cluster analyze the data acquired by the crawlers.
- The analyzed results are stored in the database.

Spam Database – No spam, no overblocking

- **Aktualität**
 - Weltweit verteilte Spam Kollektoren sammeln an 365 Tagen, 24 Stunden pro Tag Spam -> **bis zu 1,6 Mio. Unterschiedliche Spam's pro Tag**
 - Kunden erhalten alle 5 Minuten Updates
- **Qualität**
 - Ca. **45 Mio.** unterschiedliche **relevante Spams** in der Datenbank
 - > 99.7+ % Spam-Erkennung
 - < 0.01 % Overblocking
- **Quantität**
 - Weitere Verfahren zu effizienten Spam-Erkennung (Bayes Filter, URL Checker, Meta Heuristics, FlowControl, Structure Analysis, Phishing detection, ...)

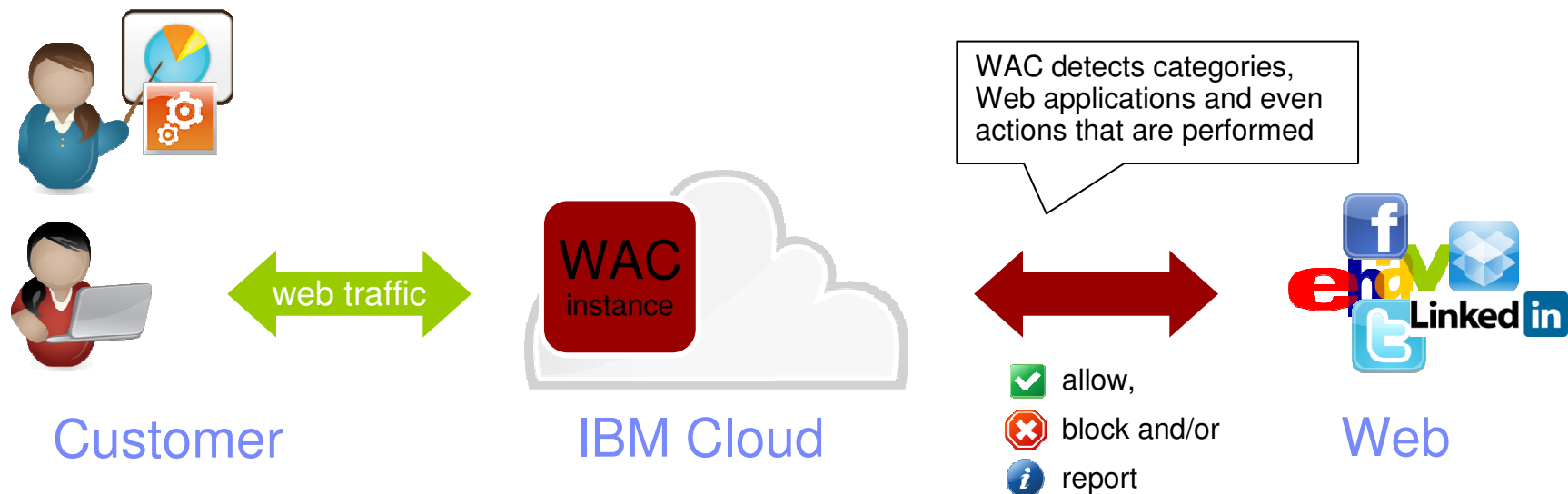


Spam processing



Web Application Control as a Service

- Get your personal WAC instance deployed and ready to use within minutes, hosted and managed in the IBM Cloud.
- Personal: Your data is isolated from other customers.
- Seamlessly integrates into the customer's infrastructure - completely *without* any additional devices or end point agents.
- The Web Application Control Policy can be customized via a Web UI.
- Get more insights about Web usage behaviour through comprehensive reports that are also accessible through the Web UI.



Rundgang



Thank you for your time today.

For more information:

- IBM X-Force Page on IBM.com: www.ibm.com/security/x-force
- IBM X-Force Sales Kit on Software Group Sellers Workplace: <http://w3-103.ibm.com/software/xl/portal/content?synKey=C850820116680T38#overview>
- IBM Security Solutions Main Page on IBM.com: <http://www-01.ibm.com/software/tivoli/solutions/threat-mitigation/?tactic=featuredhome>
- IBM Security Sellers Blog: http://w3.ibm.com/connections/blogs/ISS_Sellers_Blog/?lang=en
- If you need help with an issue that is impacting a security sale, contact the cross-brand IBM security war room at secwarm@us.ibm.com

Name	Title	Telephone	Email
Venkat Raghavan	Director Security, Risk and Compliance Tivoli	Phone: 1-512-300-6518	vraghava@us.ibm.com
Carsten Dietrich	XF Product Line Manager, Content Security	Phone: 49-561-57 0 87 15 Mobile: 49-173 541 48 05	Carsten.Dietrich@de.ibm.com
Clinton McFadden	Sr. Operations Manager, XF R&D	Phone: 1-404-236-3174 Mobile: 1-404-423-9618	cmcfadde@us.ibm.com
Jason Brewer	XF Engineering Manager	Phone: 1-404-236-2779 Mobile: 1-678-521-2312	jcbrewer@us.ibm.com
Tom Cross	Manager, XF Advanced Research	Phone: 1-404-236-2976 Mobile: 1-770-329-8581	tcross@us.ibm.com
Jamie Licitra	XF Product Manager	Phone: 1-404-236-3247 Mobile: 1-678-907-4654	jamie.licitra@us.ibm.com
Leslie Horacek	XF Threat Analysis Manager	Mobile: 32-497 41 53 10	horacek@be.ibm.com
Scott Moore	Team Lead, XF Database	Phone: 1-404-236-2988	stmooore@us.ibm.com
Wangui McKelvey	XF Marketing Manager	Phone: 1-404-236-2763	wmckelvey@us.ibm.com