

IBM BusinessConnect 2013

Vernetzter, intelligenter und informierter denn je



Security



© 2013 IBM Corporation

IBM BusinessConnect 2013

Vernetzter, intelligenter und informierter denn je

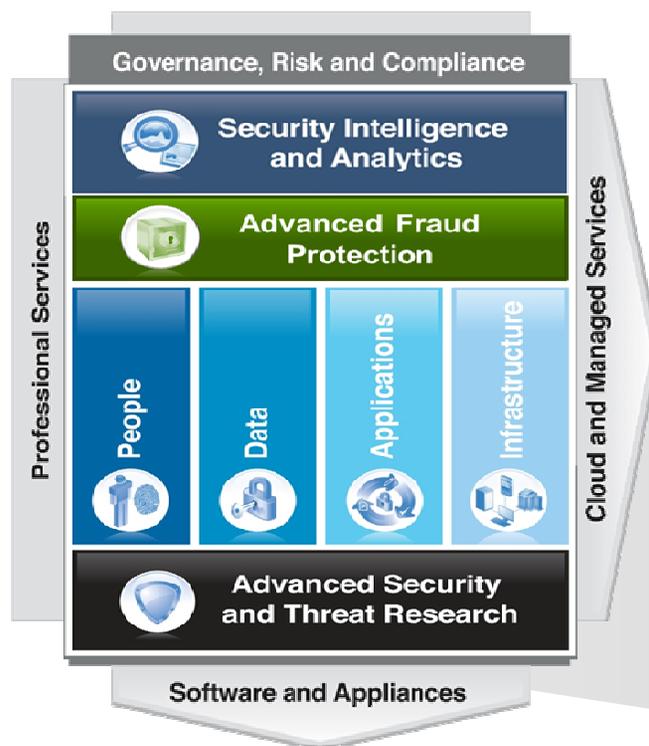


IBM X-Force 2013 Mid-Year Trend and Risk Report

Carsten Dietrich



X-Force bildet die Basis für „Advanced Security and Threat Research“ für das IBM Security Framework



Die Mission der X-Force:

- **Überwachung** und Auswertung der sich schnell ändernden Angriffs-Landschaft
- **Erforschung** neuer Angriffs-Techniken und Entwicklung von Schutzvorkehrungen für die Herausforderungen von Morgen
- **Schulung** unserer Kunden u. der Öffentlichkeit





Verteilte IBM-Teams überwachen und analysieren die neusten Sicherheitsvorfälle weltweit

Abdeckung

20,000+ Geräte
unter Vertrag

3,700+ managed
Kunden weltweit

13Mrd.+ bearbeitete
Ereignisse pro Tag

133 überwachte
Länder (MSS)

1,000+ Security
relevante Patente



IBM Research

Qualität

19 Mrd. Analyzierte
Webseiten u. Bilder

40 Mio. Spam &
Phishing Attacken

64 K dokumentierte
Schwachstellen

Milliarden
Einbruchsversuche
täglich

Millionen
verschiedenen Malware
Exemplare





Die wichtigsten Ergebnisse des Trend Report 2013 H1

Threats and Activity

- 40% mehr Einbrüche (Datendiebstahl) in 2012 – Trend setzt sich in 2013 fort
- Raffinesse ist nicht immer eine Frage der Technologie
- Mit Java so viele Systeme wie möglich infizieren

Operational Security

- Schwachstellen in Web Applikationen steigen an
- Plug-Ins für Content Management Systeme bieten ein leichtes Ziel

Emerging Trends

- Soziale Netzwerke werden zunehmend für Spear-Phishing und das Sammeln von Informationen für Angriffe genutzt

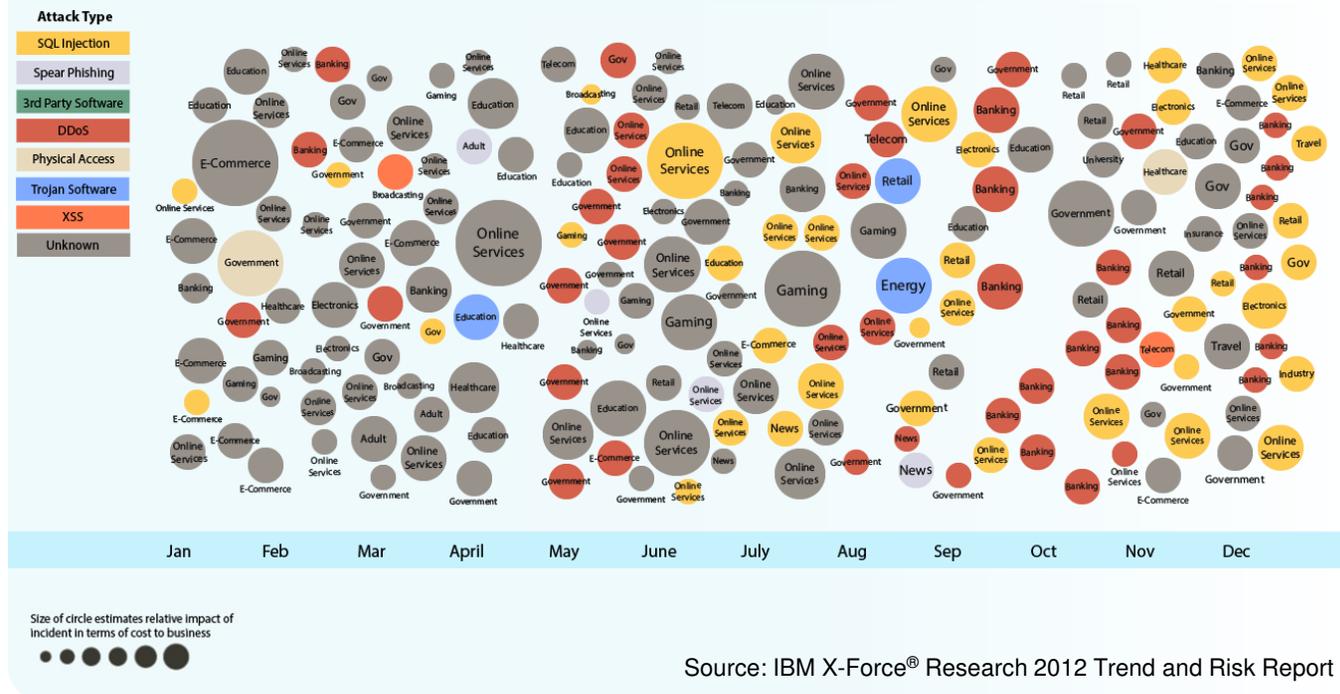


2012: Die Anzahl der Einbrüche explodiert!



2012 Sampling of Security Incidents by Attack Type, Time and Impact

Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



2013: The explosion of breaches continues!



Source: IBM X-Force® Research and Development



Aktuelle Beispiele

heise Security News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 40 > Einbruch bei Adobe: Millionen Kundendaten sowie Sourcecode von ColdFusion und Acrobat geklaut

04.10.2013 09:27

« Vorige | Nächste »

Alert! Einbruch bei Adobe: Millionen Kundendaten sowie Sourcecode von ColdFusion und Acrobat geklaut

heise Security News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 30 > Apple-Entwicklerbereich gehackt

22.07.2013 08:30

« Vorige | Nächste »

Apple-Entwicklerbereich gehackt UPDATE

vorlesen / MP3-Download

Ein erfolgreicher Angriff ist der Grund dafür, dass Apples Entwicklerbereich seit vergangenen Donnerstag **nicht mehr erreichbar ist**. In seiner **aktualisierten Stellungnahme** erklärt das Unternehmen, dass es zu diesem Zeitpunkt einen

heise Security News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 42 > Europol sieht Gefahr in Teams aus Hackern und Schmugglern

18.10.2013 13:43

« Vorige | Nächste »

Europol sieht Gefahr in Teams aus Hackern und Schmugglern

vorlesen / MP3-Download

Mindestens seit Juni 2011 beauftragten holländische Drogenschmuggler professionelle Hacker, um Computersysteme im Antwerpener Hafen auszuspionieren. Mit Hilfe der ausgespähten Daten verschob die Bande mutmaßlich Drogen im Wert von mehreren Hundert Millionen Euro. Rob Wainwright, Chef von Europol, sieht in dieser Kooperation eine neue Art von Kriminalität und hofft auf mehr Technikwissen bei der Polizei. Regierungen und Parlamente sollten aber zusätzlich Gesetze erlassen, mit denen die "Ausnutzung des Internets" bekämpft werden könne, [berichtet](#) die BBC.

heise Security News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2013 > KW 37 > Insider-Angriff: Bankdaten von zwei Millionen Vodafone-Kunden entwendet

12.09.2013 10:33

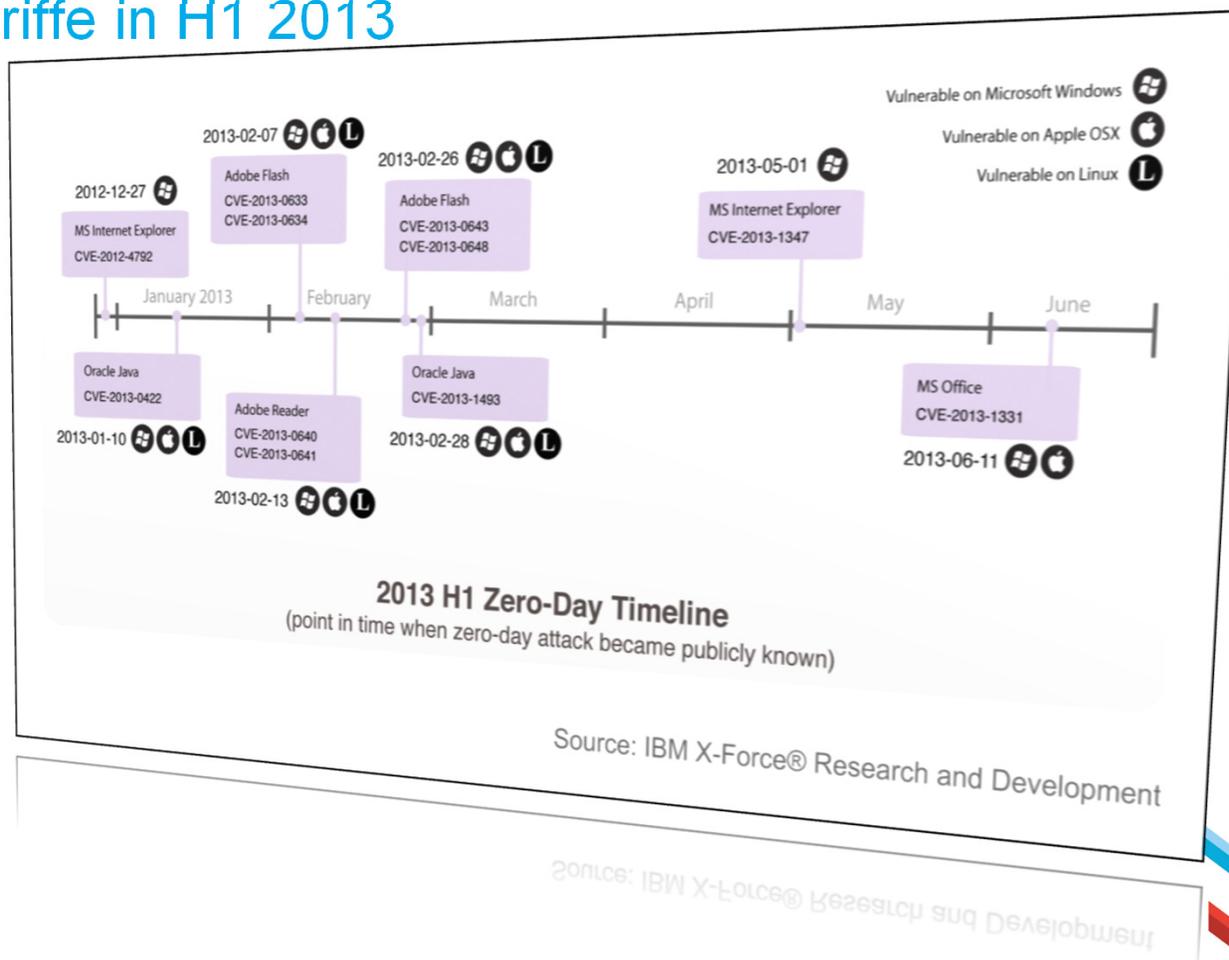
« Vorige | Nächste »

Insider-Angriff: Bankdaten von zwei Millionen Vodafone-Kunden entwendet UPDATE

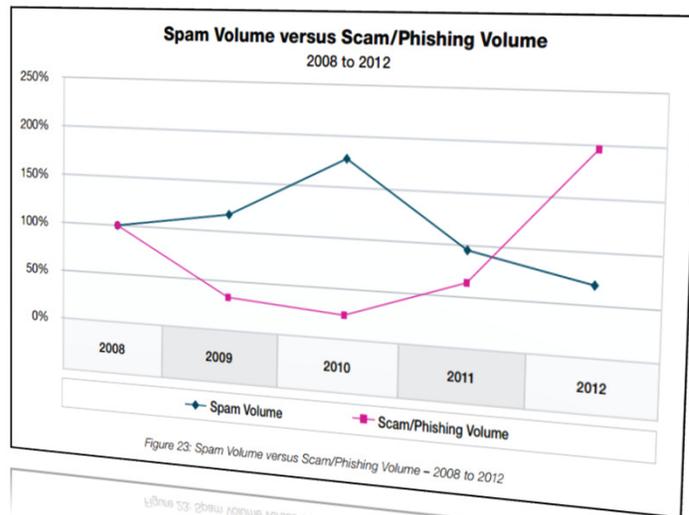
Zero-day Angriffe in H1 2013

Viele Angriffe wurden zunächst als **“Targeted Attacks”** durchgeführt.

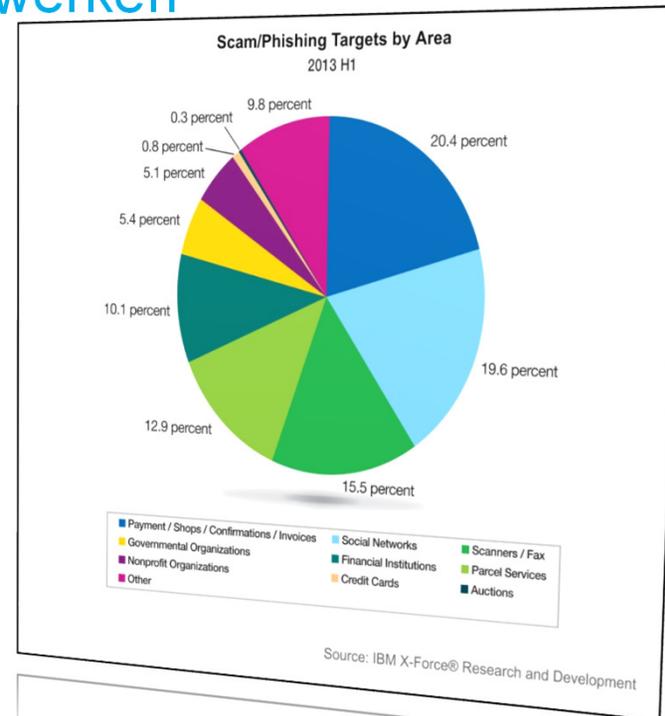
Angriffe sind zunehmend **plattform-unabhängig**



Spear-Phishing „mit“ Sozialen Netzwerken



Spam Volumen ist rückläufig, aber
Spams mit böartigen Attachments steigen an!

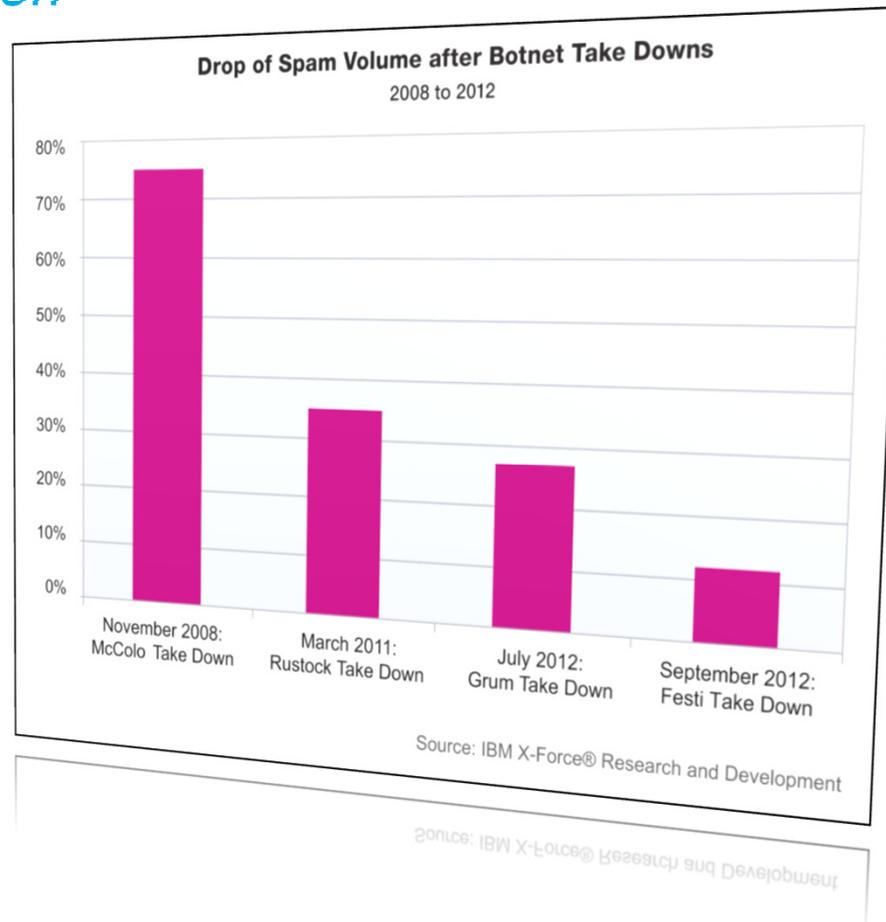


Scammers rotieren ihr
 “Karussell der Ziele”

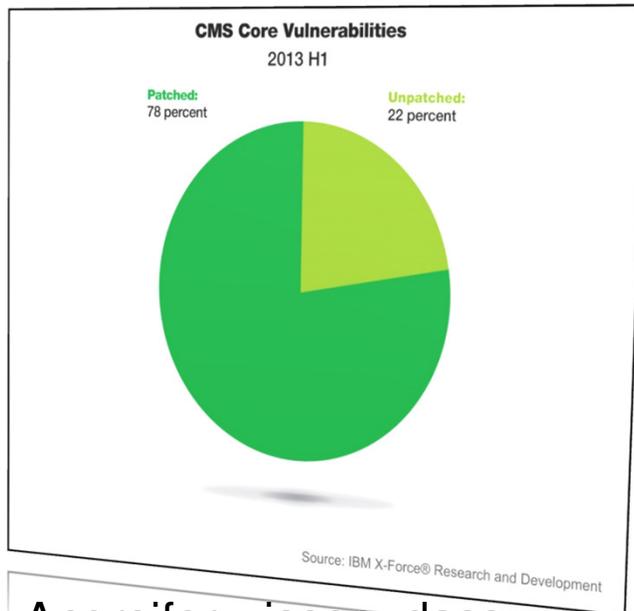


Robustheit von Botnetzen

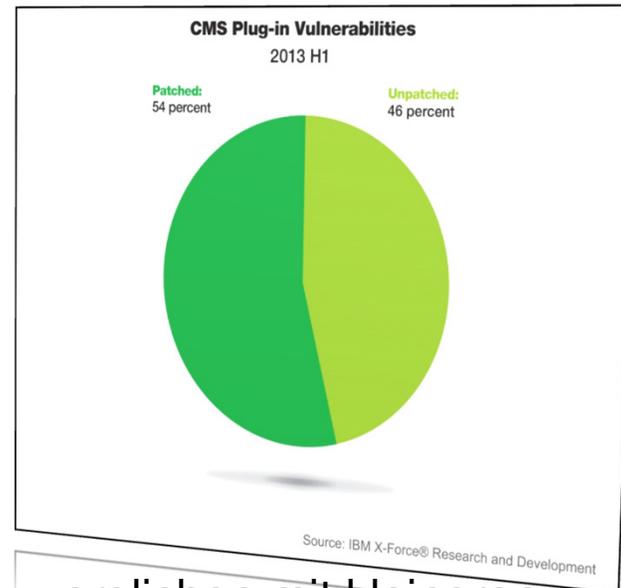
Wenn C&C-Server von Botnetzen ausgeschaltet werden, wird die Funktionalität schneller als jemals zuvor kompensiert.



Content Management Systeme



Angreifer wissen, dass CMS-Hersteller besser patchen



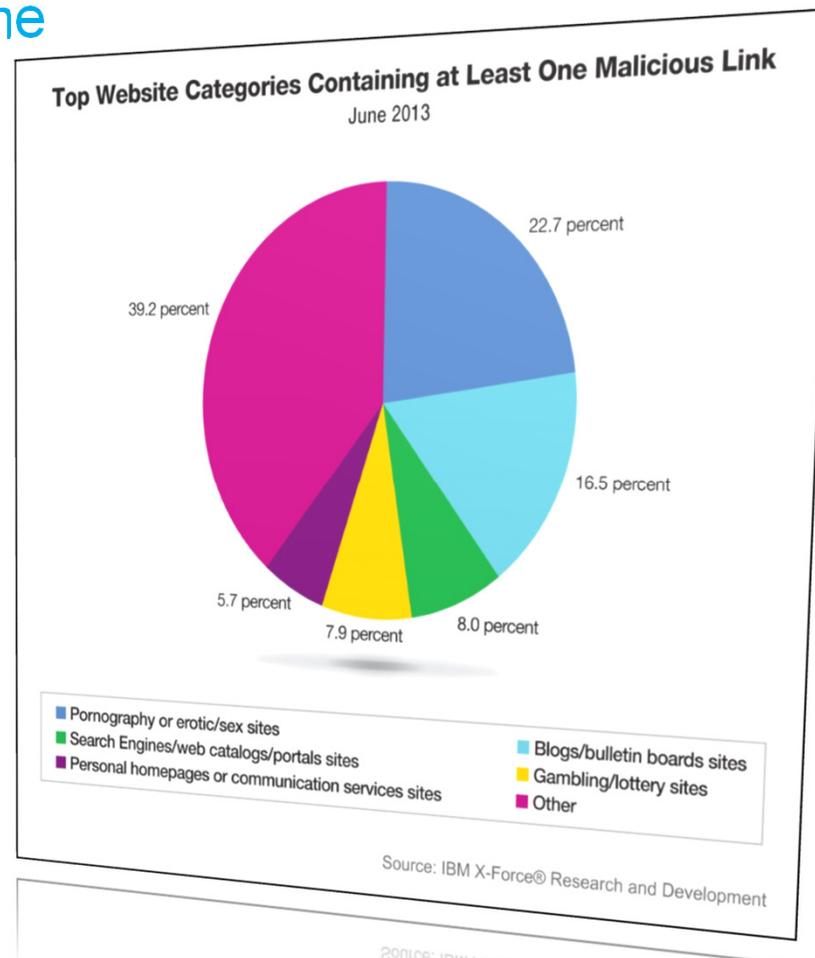
... verglichen mit kleineren Herstellern und Einzel-Entwicklern von Add-Ons und Plug-Ins



Links auf Schad-Programme

Vorsicht!

beim Besuch von
„seriösen“ Webseiten



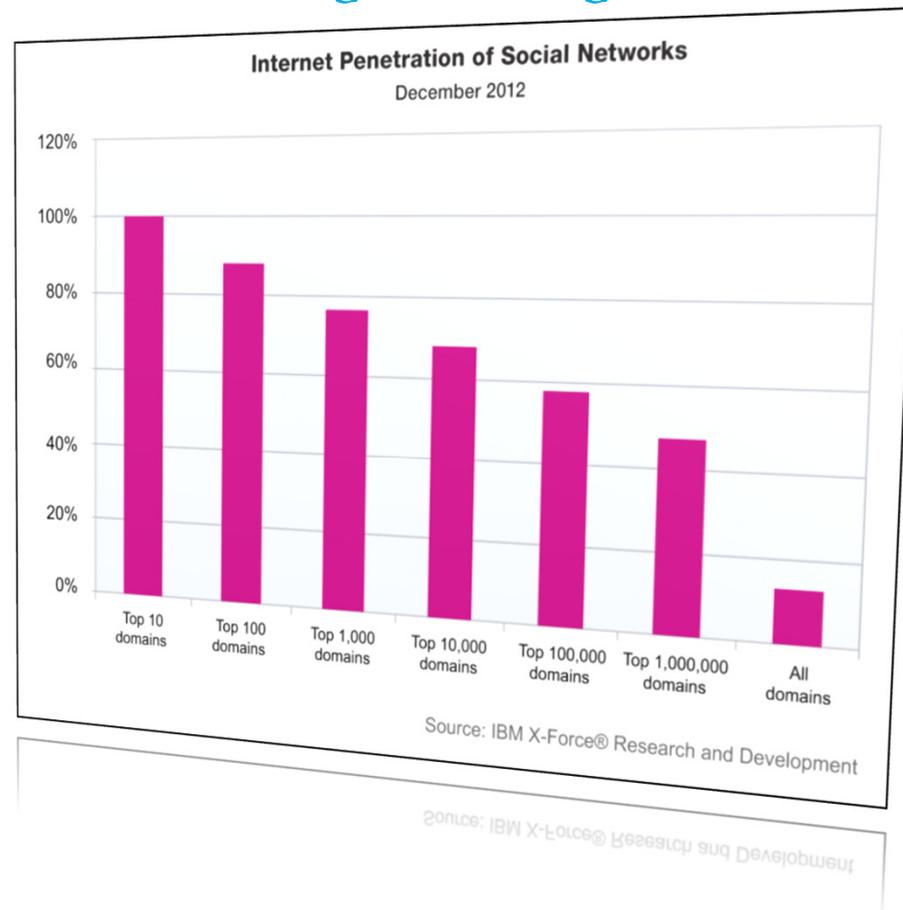
Soziale Netzwerke und Informationsgewinnung



50%

aller Webseiten
haben
Verbindungen
zu Sozialen
Netzwerken

Moderne Spear-
Phishings
scheinen von
Freunden oder
Kollegen zu
kommen



Einfluss sozialer Netze auf die Börse



60 Zeichen kosten den
U.S. Aktienhandel
200.000.000.000 \$
- ja, 200 Mrd.

Durch nur **einen Tweet**

Bleiben Sie mit IBM X-Force Research and Development in Kontakt



Security Intelligence
Blog

<http://securityintelligence.com/>



Download X-Force
security trend & risk
reports

<http://www.ibm.com/security/xforce/>



Subscribe to X-Force alerts
at <http://iss.net/rss.php> or
X-Force Security Insights
blog at

<http://www.ibm.com/blogs/xforce>



Follow us at
#ibmsecurity and
#ibmxforce



IBM BusinessConnect 2013

Vernetzter, intelligenter und informierter denn je



Thank You!

