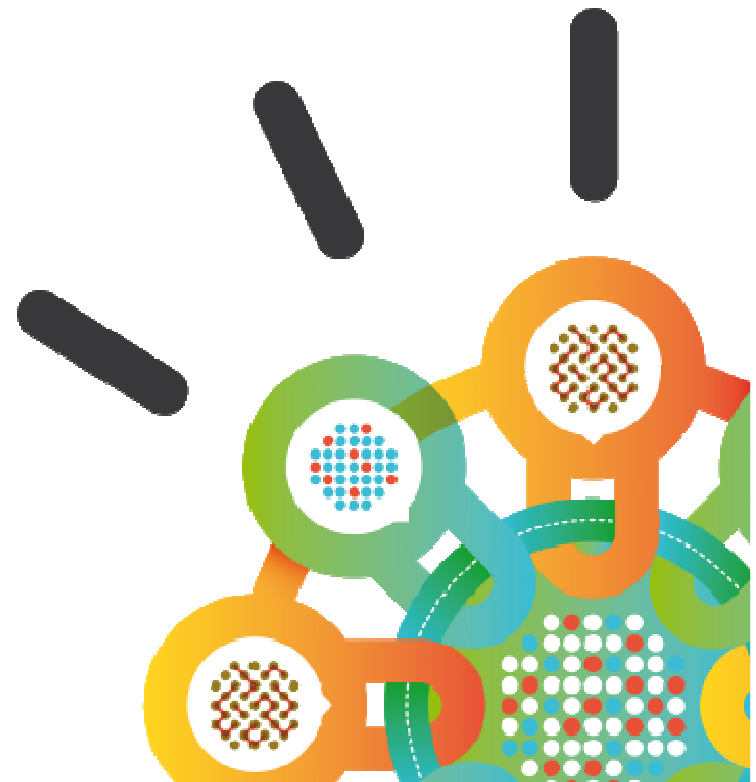


Security Intelligence.
Think Integrated.

IBM Security Systems

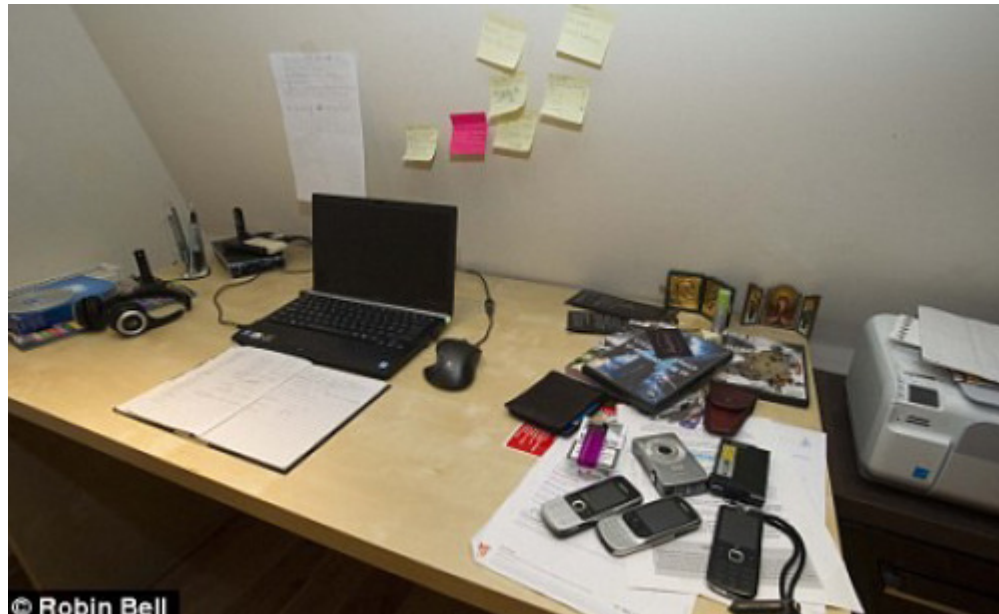
Gerd Rademann
Business Unit Executive





Arbeitsplatz Banking-Trojaner Zeus

Beute:
7 Mio €

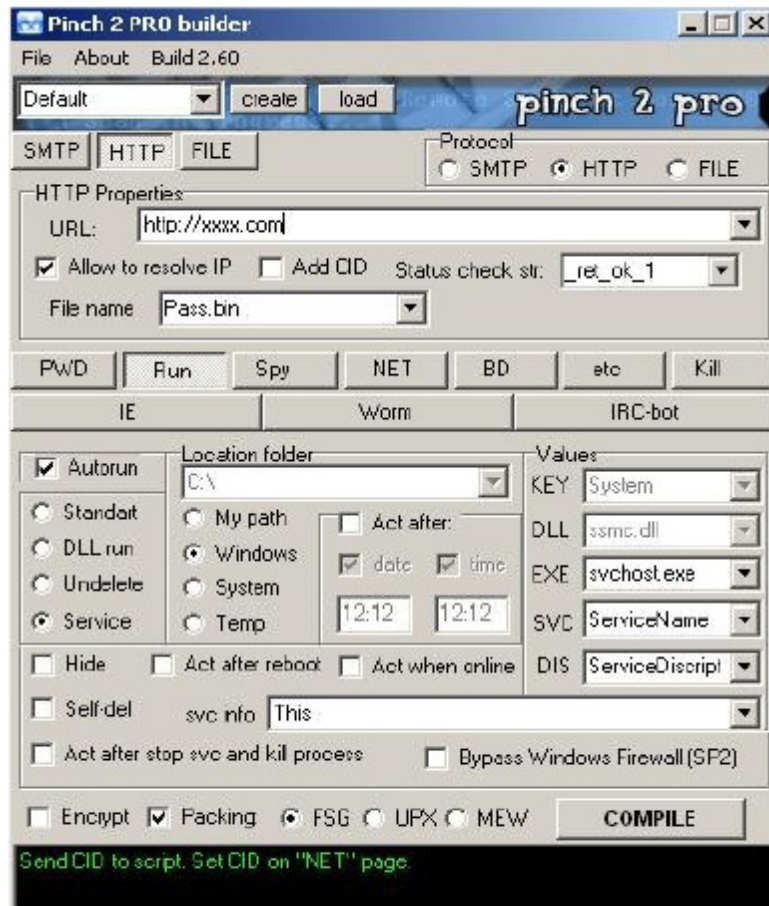


Tatwerkzeug:
Zeus-Trojaner

Zeitraum: 3 Monate



Inoffizieller Markt zur Generierung von Schadprogrammen: mit Komfort und Support



Preisliste

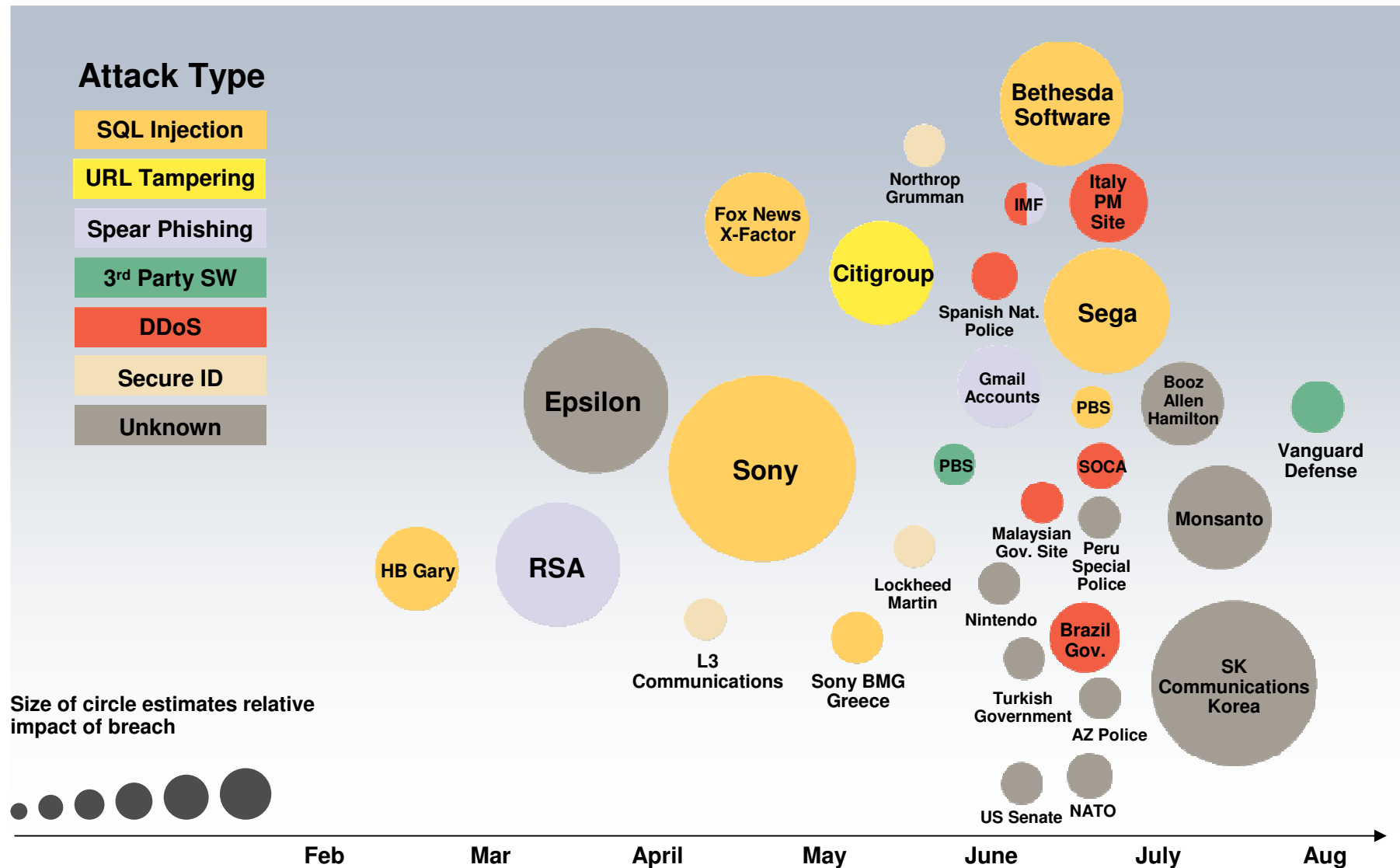
Crimepack:	\$	400
Phoenix Exploits Kit:	\$	400
Adrenaline: (inkl. 24x7-Support)	\$	3.500
Eleonore Exploits Pack	\$	700
Eleonore Exploits Pack	\$	1.200
YES Exploit System	\$	800

JETZT

Vor 10 Jahren



Sicherheitsangriffe auf Unternehmen nehmen kontinuierlich zu



Detecting threads

07.11.2012 13:39

« Vorige | Nächste »

Coca-Cola wurde gehackt - und schweigt UPDATE

 vorlesen / MP3-Download

[Coca-Cola](#) wurde 2009 Opfer einer gut organisierten Cyberattacke, bei der Angreifer mindestens einen Monat lang Daten aus dem Firmennetz klauten. Der weltweit größte Softdrinkhersteller verschweigt den Vorfall. Der [Finanznachrichtendienst Bloomberg](#) hat den Angriff nun bekannt gemacht und [zitiert aus einem internen Bericht](#), der den Fall aufarbeitet. Die Gruppe stahl Daten über einen Milliarden-Deal, der nur wenige Tage später platzte.

Demnach wurde Coca-Cola am 15. März 2009 vom FBI auf die Attacke aufmerksam gemacht. Das FBI teilte dem Unternehmen mit, dass sensible Daten über die geplante Übernahme des chinesischen Getränkeherstellers [Huiyuan Juice Group](#) gestohlen wurden.



Huiyuan verkauft wie Coca-Cola Getränke.



Bild: [Huiyuan Group](#)

Der Datenklau war möglich, da ein Mitarbeiter einen Link in einer präparierten E-Mail anklickte und dadurch Schadsoftware installierte. Die E-Mail arbeitete mit [Social-Engineering](#) und bezog sich thematisch auf die internen Ziele des Unternehmens, Energie einsparen zu wollen. Als Absender wurde ein führender Mitarbeiter angegeben. Ausgehend von diesem infizierten Rechner wurden weitere führende Mitarbeiter angesteuert, bei

einigen Keylogger installiert und so auch Passwörter für administrative Zwecke abgegriffen. Die Angreifer konnten sich relativ frei im Firmennetzwerk bewegen und installierten so auch in den ersten Tagen Werkzeuge, die E-Mails und andere Dokumente abfangen. Mindestens einen Monat waren die Angreifer täglich in dem Firmennetz von Coca-Cola unterwegs.

Die Welt wird immer mehr digitalisiert und vernetzt – dies öffnet die Tür für neue Bedrohungen und Schwachstellen...



DATEN EXPLOSION

Das Zeitalter der großen Datenmengen - die Explosion der digitalen Informationen - hat begonnen und ist begleitet von der Verbreitung von Anwendungen, die von überall genutzt werden



KONSUMERISIERUNG DER IT

Mit dem Aufkommen von "Enterprise 2.0" und "Social Business", verschwindet die Trennung von privaten und geschäftlichen Zeiten, Geräten und Daten



ALLES IST ÜBERALL

Organisationen setzen immer mehr neue Plattformen wie Cloud, Virtualisierung, Mobile, "Social Business" und andere ein



KOMPLEXITÄT DER ANGRIFFE

Die Geschwindigkeit und die Fertigkeit der Angriffe steigt im Zusammenhang mit neuen Antrieben von Internetkriminalität über staatliche Veranlassung bis hin zu Terror

...und macht Sicherheit zu einem vorrangigen Anliegen,
beginnend beim Vorstand

Sicherheitsherausforderungen beeinflussen Innovationen

Externe Gefahren

Starker Anstieg an externen Angriffen durch neue Angreifer

- Cyber-Angriffe
- Organisierte Kriminalität
- Industriespionage
- Angriffe durch Staaten
- Social Engineering

Interne Gefahren

Risiken durch bösartiges und unvorsichtiges Insiderverhalten

- Administrative Fehler
- Unvorsichtiges Insiderverhalten
- Interne Sicherheitsverstöße
- Unzufriedene Mitarbeiter
- Vermischung von privaten Daten und Firmendaten

Compliance

Steigende Notwendigkeit, immer mehr Richtlinien zu entsprechen

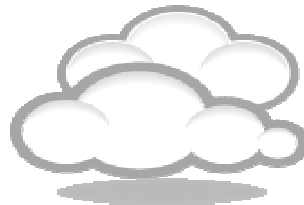
- Gesetzliche Vorschriften
- Industriestandards
- Lokale Richtlinien

Einfluss auf Innovationen

Mobilität



Cloud / Virtualisierung



Social Business



Business Intelligence



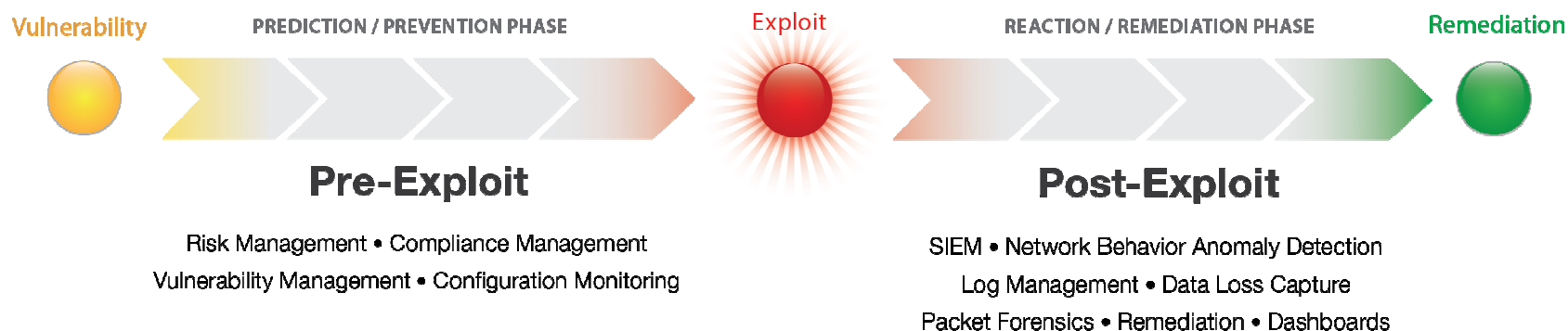
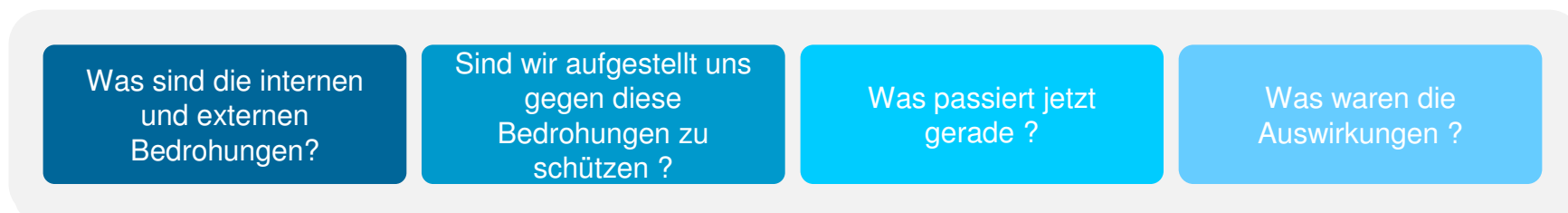
Das Ergebnis: Sicherheit wird ein Thema bei Vorstandssitzungen



Geschäftsergebnisse	Image der Marke	Lieferkette	Juristische Angreifbarkeit	Einfluss von Hacktivismus	Risiko bei Audits
Sony schätzt möglicherweise 1 Mrd. US\$ Schaden als Langzeitfolge – 171 Mio. US\$ / 100 Kunden	Datenleck bei HSBC legt Daten von 24.000 privaten Bankkunden offen	Epsilons Datenleck beeinflusst über 100 amerikanische Marken	TJX schätzt 150 Mio. US\$ Vergleich für Sammelklage bezüglich der Herausgabe von Kreditkartendaten	Lulzsecs 50-tägige Hackserie trifft Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony ...	Zurich Insurance PLC: 2,275 Mio. £ (3,8 Mio. US\$) Geldstrafe für Offenlegung von 46.000 Kundendaten

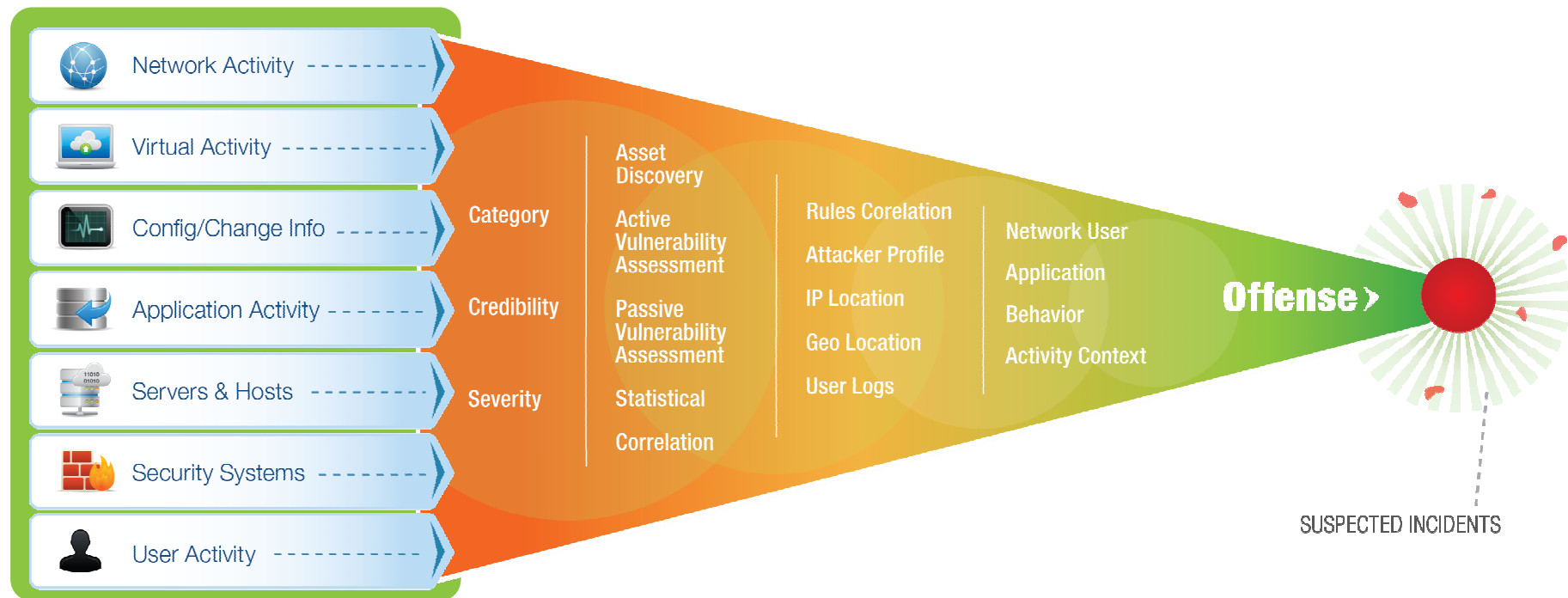
Kann uns das passieren?

Wie kann ich mir Security Intelligence vorstellen ?



Zu einer ganzheitlichen Sicht auf die aktuelle „Lage“ genügt es nicht, nur einzelne Quellen (z.B. Logs) auszuwerten; auch die Netzwerkdaten sind zur Auswertung heranzuziehen

Security Intelligence korreliert die Informationen aller relevanten Systeme und liefert klare Hinweise für Handlungsbedarf



Zu einer ganzheitlichen Sicht auf die aktuelle „Lage“ genügt es nicht, nur Logs auszuwerten !!

IBM hat beispiellose Erfahrung in Security



10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
46K documented vulnerabilities
Millions of unique malware samples



3000+ Security & Risk Management Patente

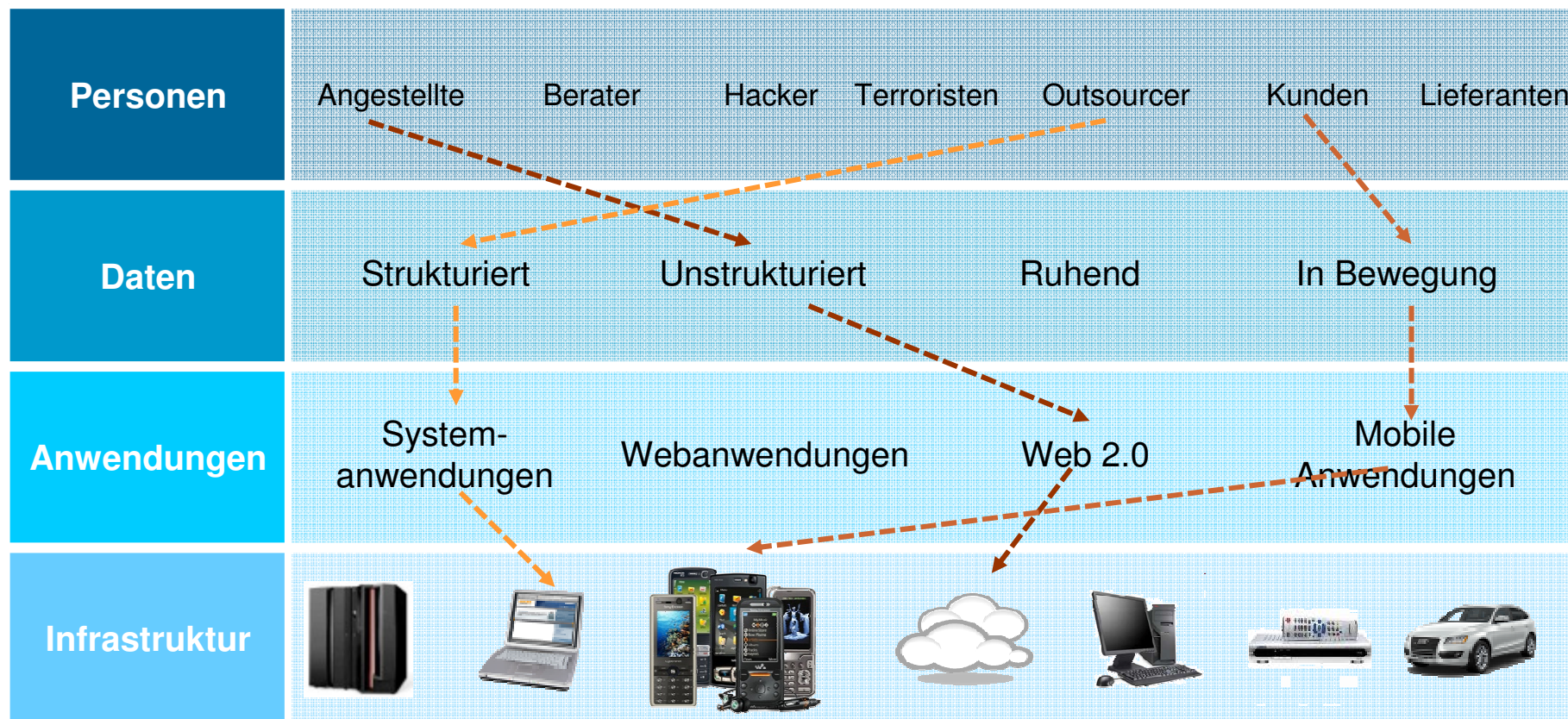
200+ Security Kundenreferenzen

15.000 Forscher, Entwickler und SMEs in Security

40+ Jahre erfolgreiche Sicherheit für den Host

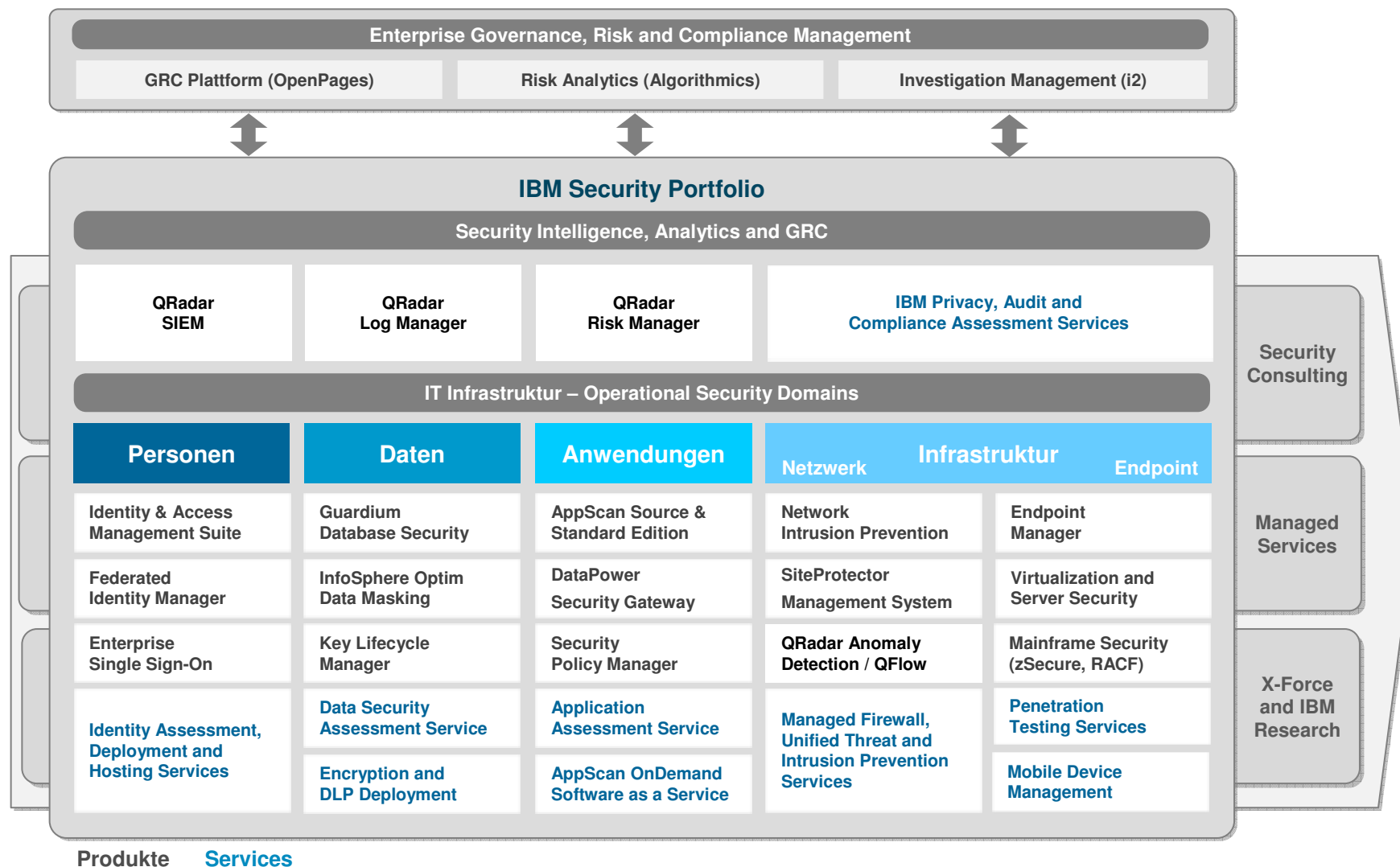
2008 für Security 1.8 Milliarden \$ investiert

Die Lösung eines Sicherheitsproblems ist komplex



Es reicht nicht länger aus die Grenzen zu schützen -
Insellösungen und Einzelkomponenten werden das
Unternehmen nicht schützen

IBM Security Systems als neue Security Brand hat das umfassendste Security-Portfolio





ibm.com/security