eDiscovery und Cyberangriffe: Worauf müssen sich Kommunen vorbereiten?

Markus Grüneberg

Public Sector Security Spezialist

Wichtige IT-Sicherheitstrends

Hochentwickelte Angriffe

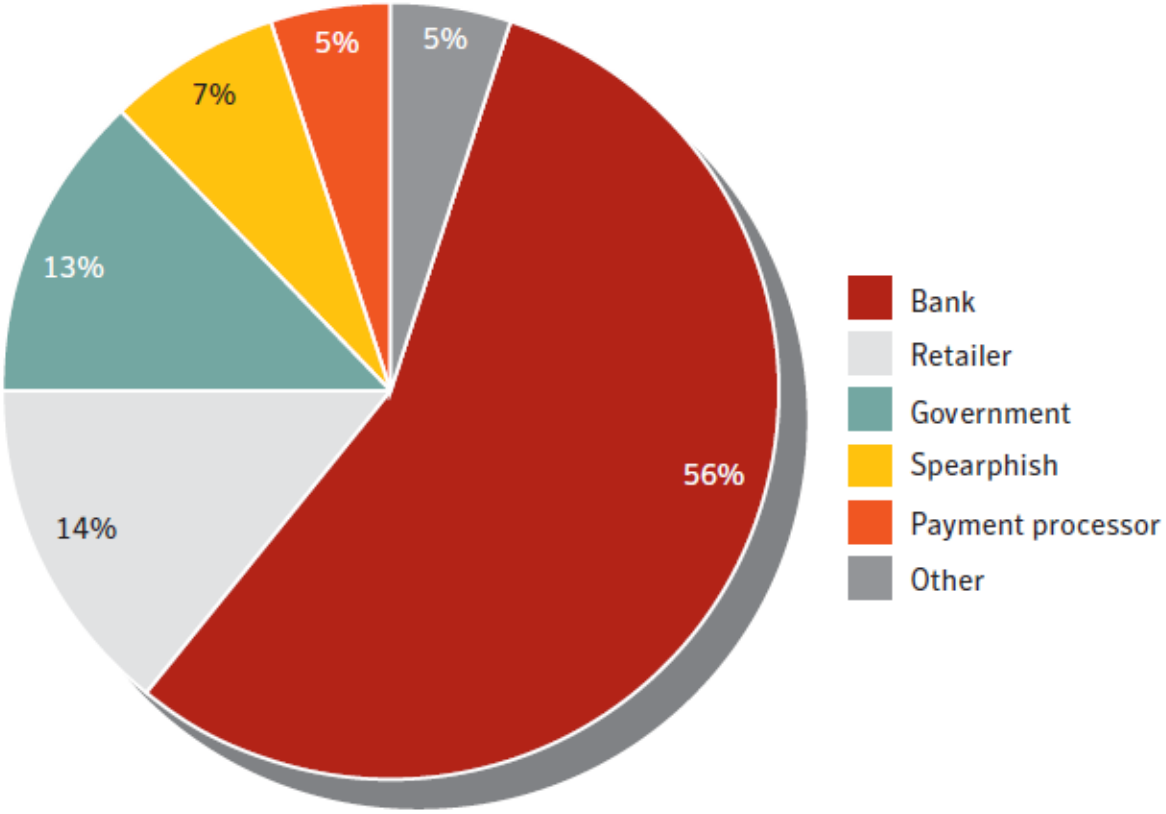
Komplexe heterogene Infrastrukturen

Explosionsartige Zunahme von Informationen

Zunehmende Aufmerksamkeit bei Sicherheits-vorfällen

Phishing Kategorien

- 56% der Angriffe zielten auf den Bankensektor
- Immer mehr auf den behördlichen Sektor (z.B. BKA-Trojaner)

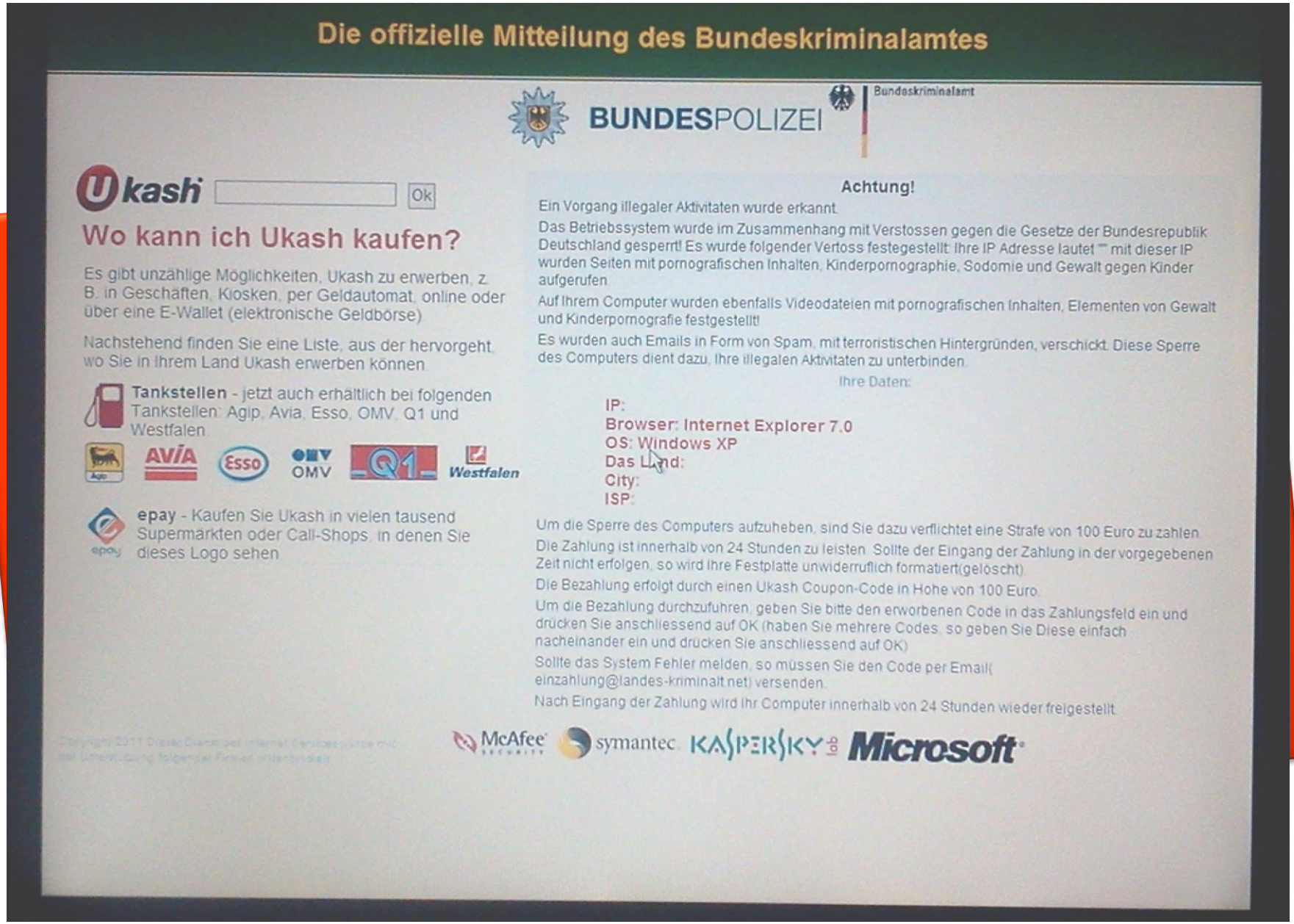


Bösartige Aktivitäten gehen verstärkt von Schwellenländern aus

Trojan GPCoder G

Zahlen Sie 120 $ oder Sie bekommen Ihre Daten nicht mehr zurück.

Die offizielle Mitteilung des Bundeskriminalamtes



BUNDESPOLIZEI

Bundeskriminalamt

Ukash Ok

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.

Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

Agip AVIA Esso OMV Q1 Westfalen

epay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt.

Das Betriebssystem wurde im Zusammenhang mit Verstossen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Vertoss festegestellt: Ihre IP Adresse lautet "" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen.

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornografie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten:

IP:
Browser: Internet Explorer 7.0
OS: Windows XP
Das Land:
City:
ISP:

Um die Sperre des Computers aufzuheben, sind Sie dazu verflichtet eine Strafe von 100 Euro zu zahlen.

Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert(gelöscht).

Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Hohe von 100 Euro.

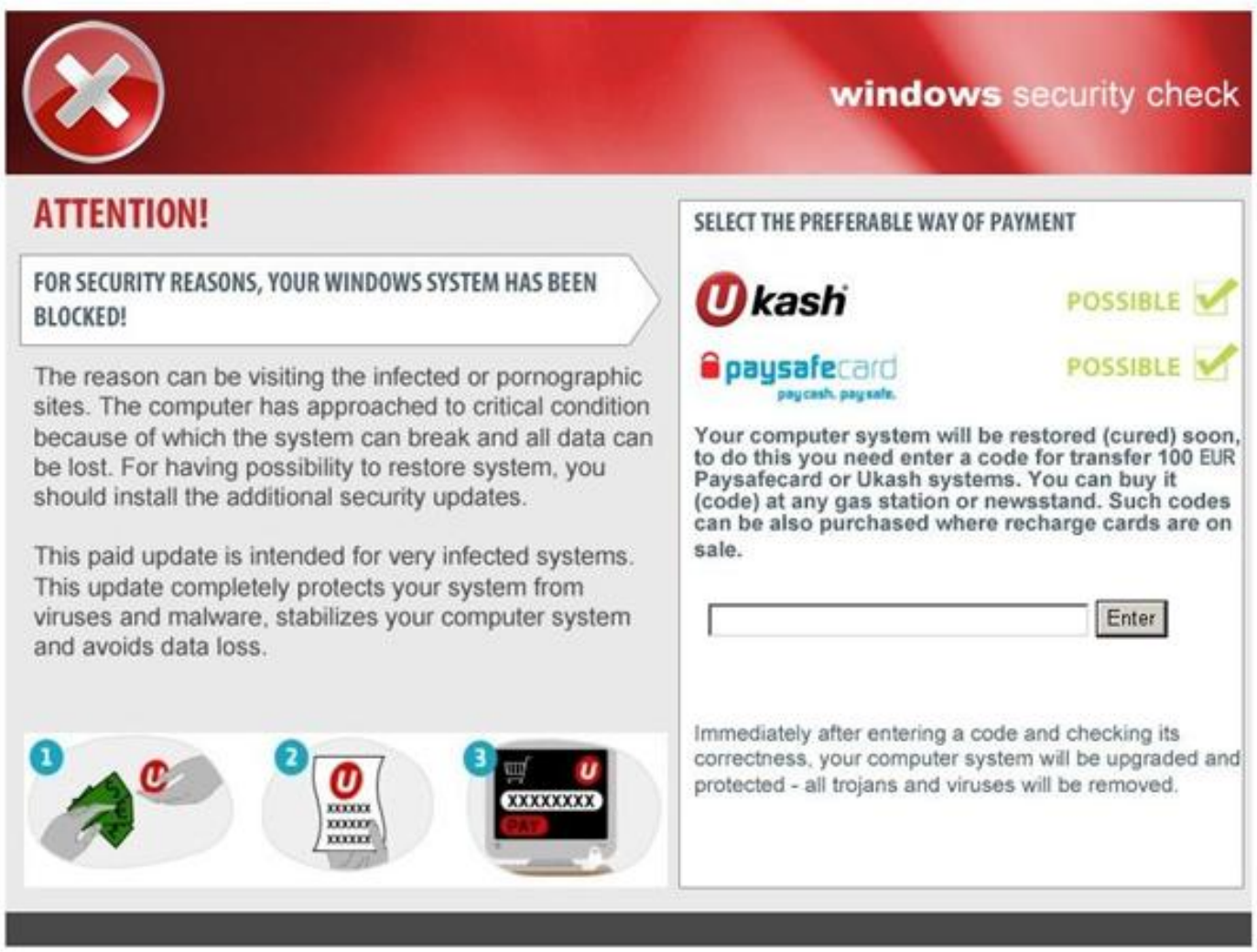
Um die Bezahlung durchzufuhren, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK).

Sollte das System Fehler melden, so müssen Sie den Code per Email(einzahlung@landes-kriminalt.net) versenden.

Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

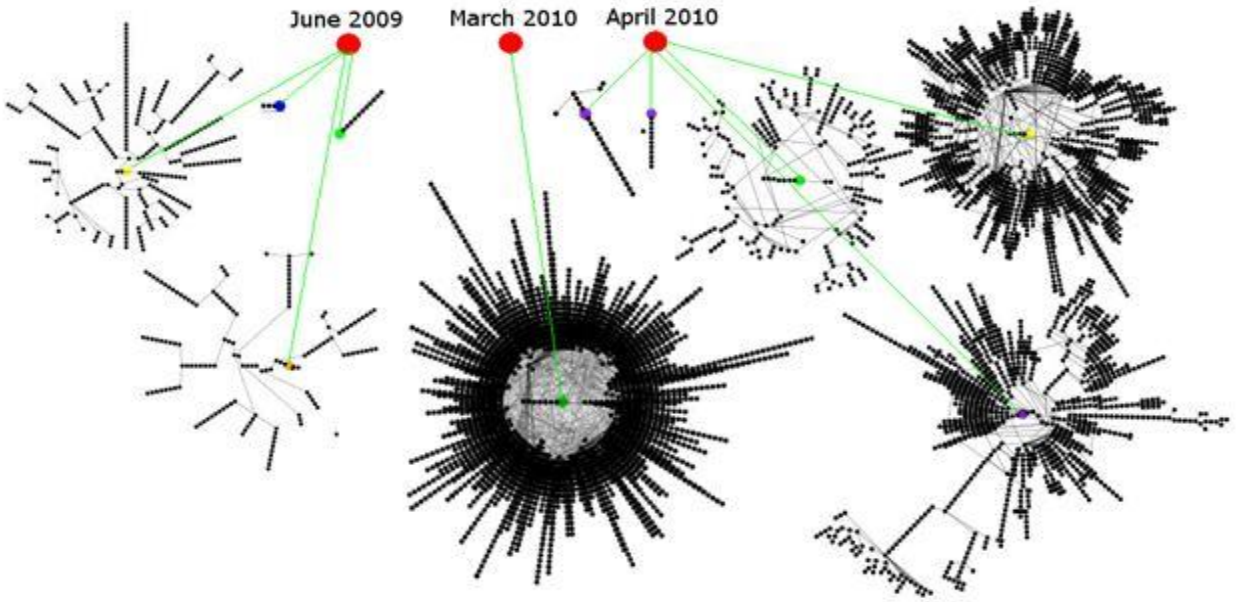
McAfee symantec KASPERSKY Microsoft

Rampant Ransomware



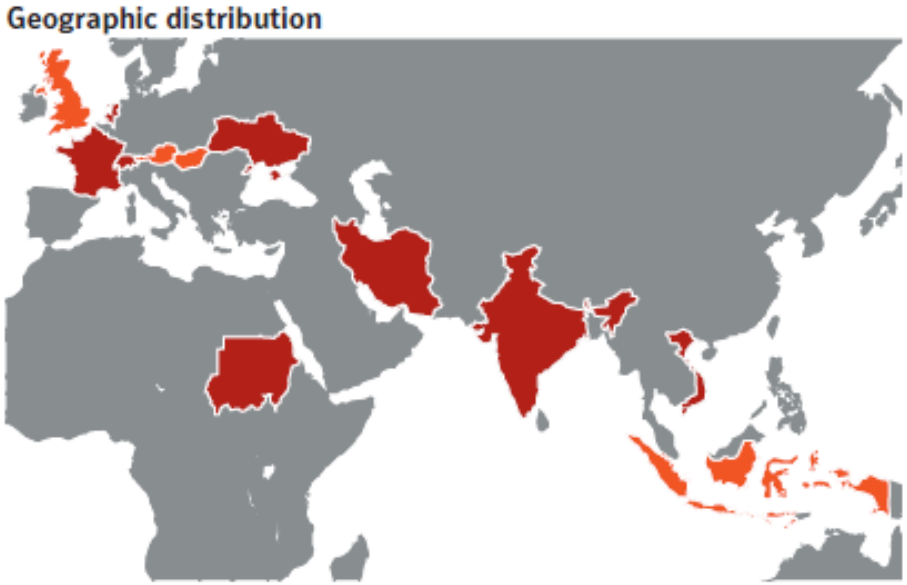
Stuxnet - Refresher

- Stuxnet war ein gezielter Angriff auf fünf Organisationen; 12,000 Infektionen konnten zu fünf Organisationen zurückverfolgt werden
- Drei Organisationen waren einmal angegriffen worden, eine zwei Mal und die andere drei Mal Ziel der Angriffe
- Organisationen wurden angegriffen in Juni 2009, Juli 2009, März 2010, April 2010 und Mai 2010
- Alle Organisationen waren im Iran präsent.

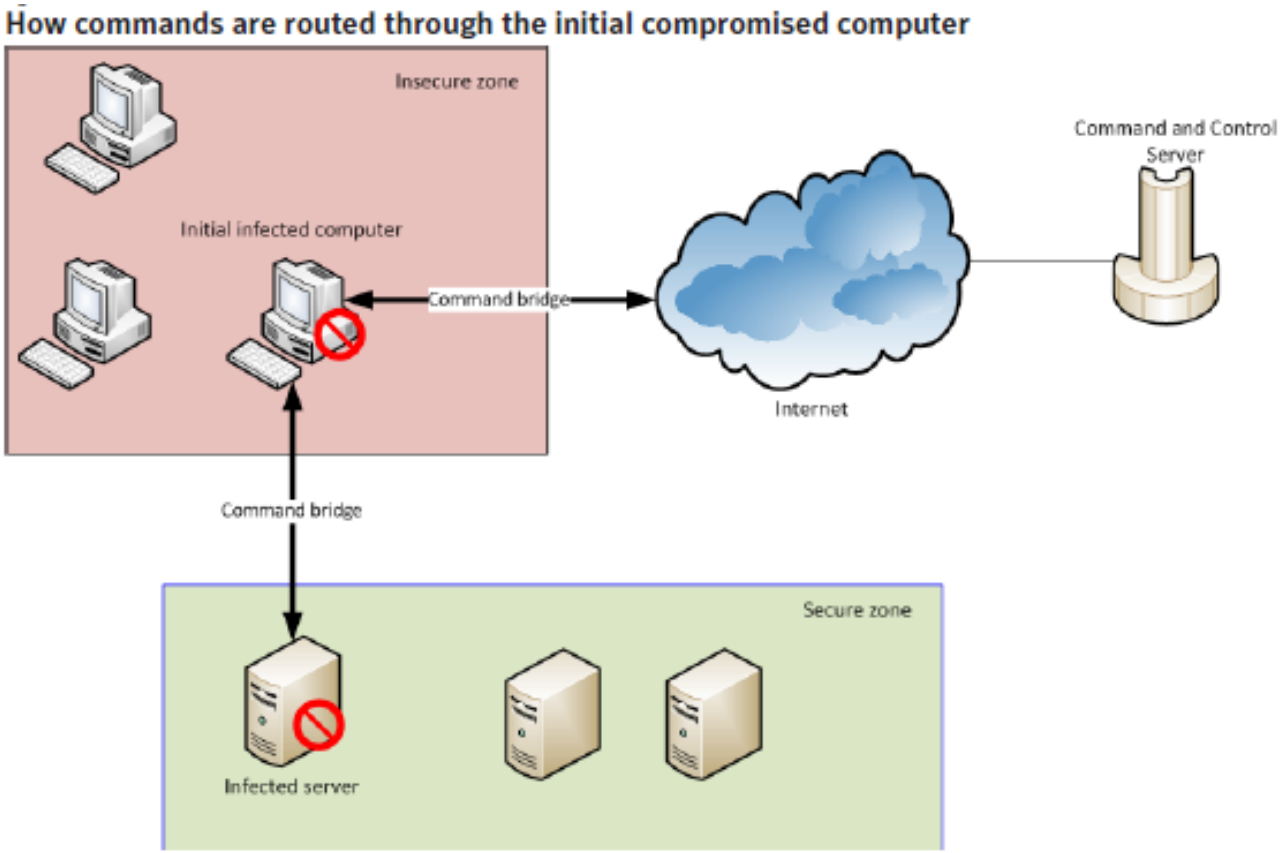


DuQu – Next Gen?

- Duqu Infektionen sind bestätigt in sechs Organisationen in acht Ländern. Diese sechs Organisationen fallen auf:
  - Organisation A—Frankreich, Niederlande, Schweiz, Ukraine•
  - Organisation B—Indien •
  - Organisation C—Iran•
  - Organisation D—Iran•
  - Organisation E—Sudan•
  - Organisation F—Vietnam•



Eine neue Art der „C&C Kommunikation“



Ständig andere Angriffsvektoren

Twitter Hack – PLEASE TAKE ACTION

EMEA Internal Communications

Sent: Montag, 12. März 2012 17:47

To: EMEA Internal Communications

Symantec. | SPECIAL BULLETIN

Twitter Hack – PLEASE TAKE ACTION

Over the weekend certain Twitter accounts have been compromised. This special bulletin has been put together to highlight the current situation and provide advice on how to prevent or counteract the potential threat.

Any messages containing subjects such as "somebody is posting real bad rumors about you here" and "omg...I am laughing so hard at this pic of u someone found", both have a links – **do not click on them!**

Additional steps to take to prevent the potential threat are:

1. Change your password (the second time twitter does this automatically)
2. Scan your machine with SEP
3. Revoke access from all third party accounts

If all fails you will need to deactivate your account immediately.

It is recommended that you change your password and review which applications have been granted access to your account. If you see any unusual behavior act fast, do not click any links and worst case deactivate your account (30 days before permanent deactivation).

Analysis from both the Threat Response and STAR is that this is a phishing campaign. The link directs people to a page that resembles the real Twitter page and asks people for their credentials. Once the credentials are entered your account has been compromised. Messages from social media sites should be evaluated with the same level of caution as email. This campaign appears to be widespread and is targeting more than Symantec employees.

For additional guidelines please click on the following link for information directly from Twitter: https://support.twitter.com/articles/31796

Immer komplexere Szenarien

- Nutzen von Sozialen Netzwerken (Schwarmverhalten)
  - Bundesminister zu Guttenberg innerhalb von 12 Tagen von allen Ämtern zurückgetreten
    - Einführung eines GuttenPlagWIKI
    - Umfangreiche Investition an Zeit in diese Plattform durch Freiwillige
    - Nutzen „virtueller social media“ Accounts zur Meinungsverstärkung
  - Im September 2008 bewarb sich die hundertprozentige Post-Tochter *DHL* als Logistikdienstleister der *Bundeswehr*.
    - Aktivisten nutzen das Internet um, aktiv eine Kampagne zu starten
    - Kosten der Kampagne relativ gering
    - dhl.blogsport.de

Relativ professionelle Hetzkampagnen

Real eingetretener Schaden

Nicht alle Angriffe dienen wirtschaftlichen Zwecken

- Operation „Payback“
  - „Low Orbit Ion Cannon“
  - Symbolische Aktion von Bürgern
  - Netzdemonstration

- Niederlande verhaftet Jugendlichen
  - Geständnis wg. Verhaftung Assange
  - Kein Hacker, keine Versuche sich unkenntlich zu machen
  - Nach Bekanntwerden Solidaritätsbekundungen im Netz
  - Angriff richtete sich jetzt auch auf niederländische Behörden

Immer komplexere Szenarien, und was wäre wenn …

- Demonstrationen zukünftig durch Internetaktivisten unterstützt werden?
  - Nutzen virtueller Identitäten um Massen zu „steuern“
  - Unterstützende Hetzkampagnen
    - Evtl. resultierende zunehmende Unterstützung in der Bevölkerung
  - Ausnutzen von Schwächen moderner Infrastrukturen
    - Stören des „GRID“ - Verbundes
    - Sabotage von Steuerungstechnik
    - Einspeisen von Fehlinformationen in Führungs- und Leitsysteme

… es dem gezielten Stören moderner Infrastrukturen dient.

Bedrohungslage

- Gezielte Angriffe auf Unternehmen und Behörden
- Angriffe werden meist auf Kompetenzen verteilt
- Sogenannte “Attack Kits” erlauben es auch unbedarften Angreifern Aktionen auszuführen
- Angriffswerkzeuge der neuesten Generation haben “Steuerungssysteme” und Smartphones integriert
  - Incl. 24x7 Support
- Alle “Systeme” sind im Visier der Angreifer
- Koordination von realer und virtueller Kriminalität

Advanced Persistent Threats

1. EINDRINGEN

Angreifer dringt mithilfe zielgerichteter Recherche mit Firmen- und Mitarbeiterdaten ein.

2. ERKENNEN

Hacker verschafft sich intern eine Übersicht über die Sicherheits-maßnahmen des Unternehmens. Hacker plant die Struktur des Angriffs.

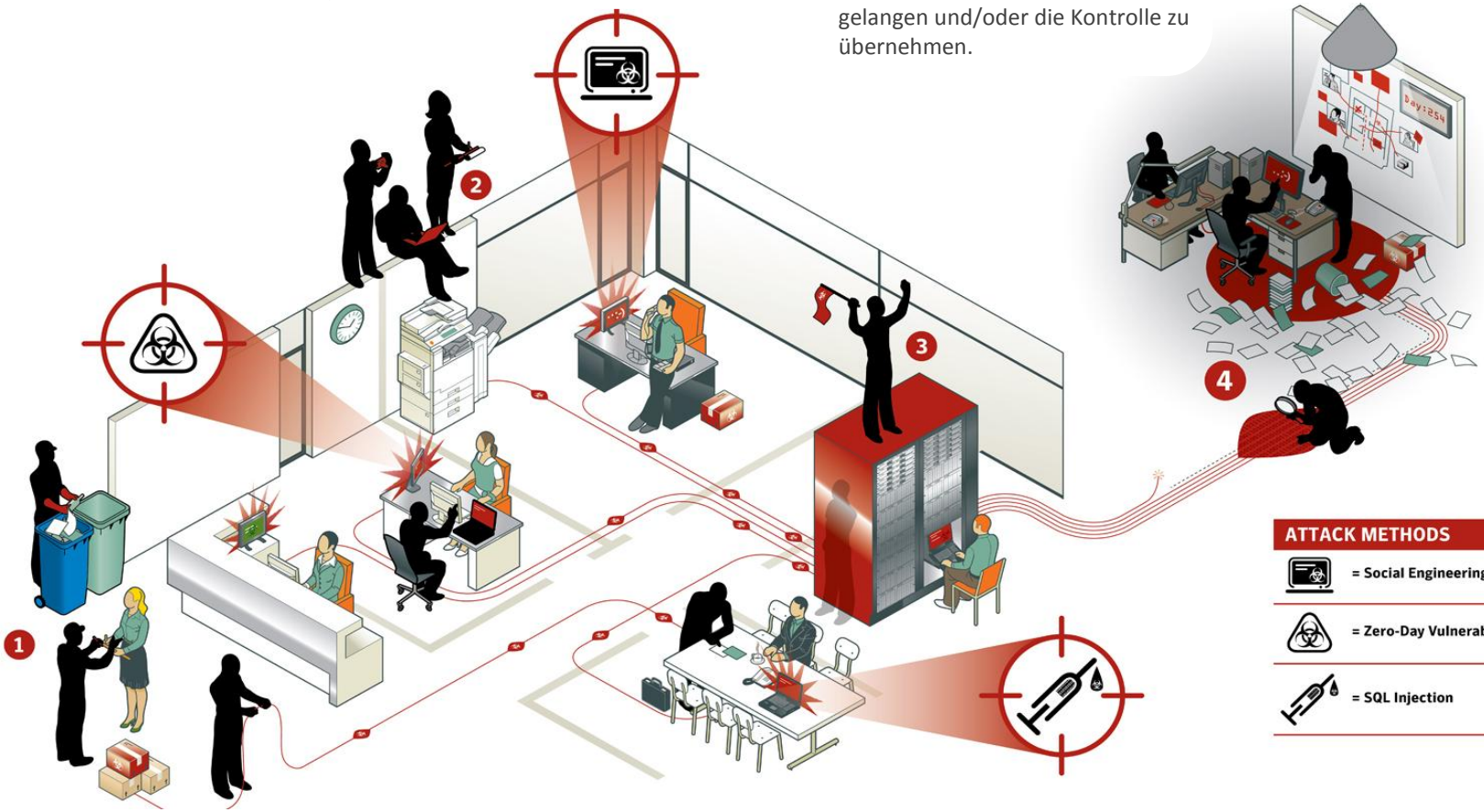
3. ERFASSEN

Zugriff auf Daten auf ungeschützten Systemen

Installation von Malware, um heimlich an wichtige Daten zu gelangen und/oder die Kontrolle zu übernehmen.

4. AUSSCHLEUSEN

Vertrauliche Daten werden zum "Basislager" des Angreifers geschleust, um diese in betrügerischer Absicht zu missbrauchen.



Symantec.

Menschen, Prozesse & Technologien

Menschen	PROZESSE	TECHNOLOGIEN
		

Man benötigt Training, “Incident Response” und entsprechende, moderne Ansätze in allen Bereichen

Überall jederzeit. Geräte- und Sicherung.

Was ist die richtige Strategie für Informationsschutz?

Menschen

Eine integrierte Lösung für ganzheitliche Ansätze

Überall. Jederzeit. Geräteunabhängig.

Access Control

Information Protection

Cloud Visibility

Convenience

Control

Security

Compliance

Private Cloud

salesforce

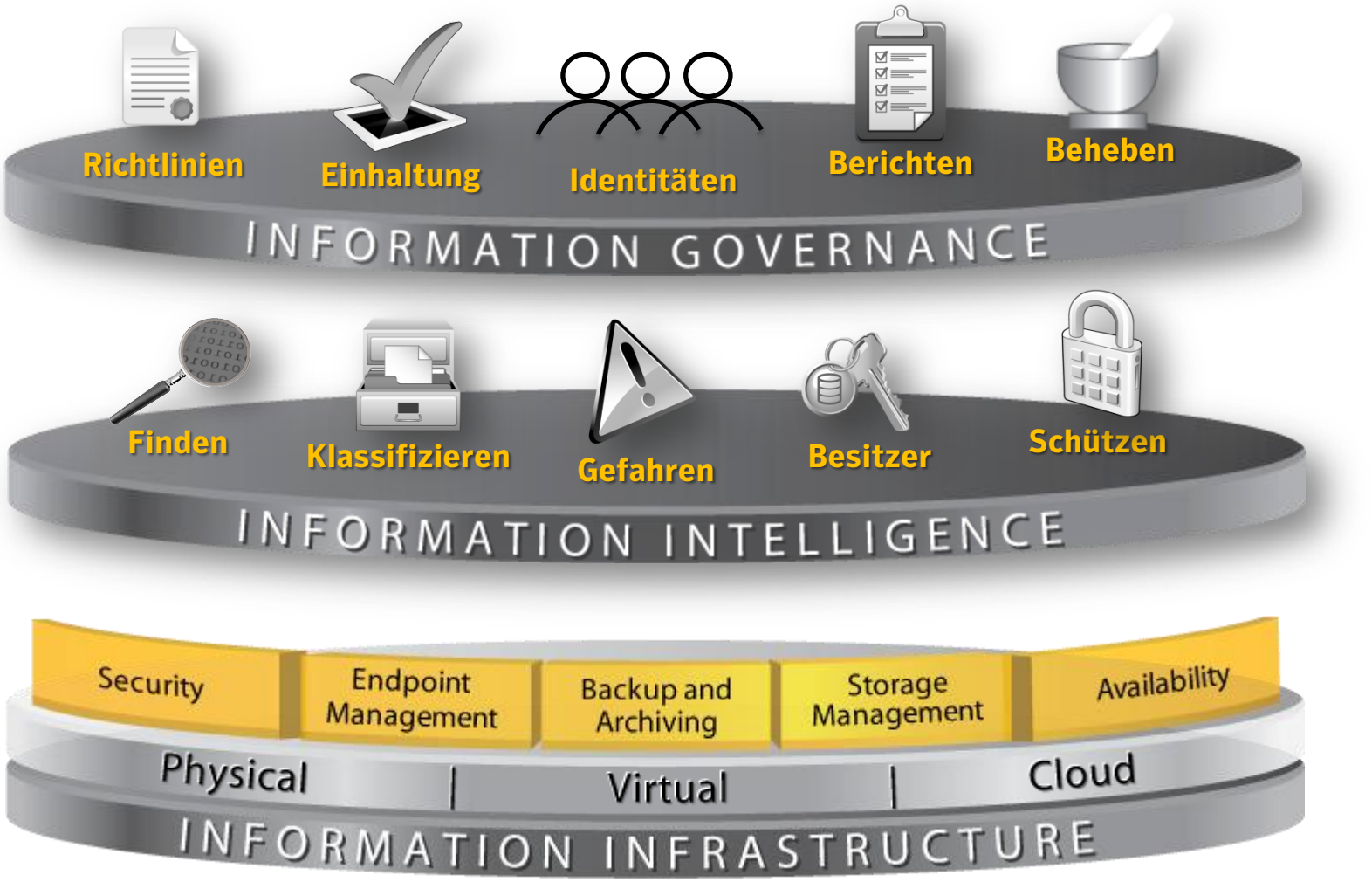
Google Apps

amazon web services

chatter Collaboration Cloud

Microsoft Office 365

Information-Centric Model



Cyber-Sicherheit (Lösungs-Sicht)

	Sicherheits Kategorie				
Sicherheits Gruppe	1 (basis)	2 (medium)	3 (erweitert)	4 (hoch)	5 (kritisch)
Information-Intelligence	Threat Intelligence	Grundschutz / Compliance	Datenkorrelation		
Perimeter & Gateway Schutz	Spamschutz	HTTP / Botnetz Prävention	Verschlüsselung am Perimeter	Datenflusssteuerung	
Sicherheit von Zentralen Diensten	Schutz vor Schadcode	Netzwerkzugangskontrolle	Härtung von Kritischen Systemen	Schutz von Mailservern	Verwaltung von Servern
	Datenflusskontrolle	Verschlüsselung von Email/ Storags	Schutz von Datenbeständen vor Schadcode	Sharepoint Schutz	
Endpunktsicherheit	Schutz vor Schadcode	Netzwerkzugangskontrolle	Systemwiederherstellung	Verwaltung von Endpunkten	
	Verschlüsselung	Härtung von kritischen Systemen	Datenflusskontrolle	Signierung von Daten	
Basisleistungen & Services	24x7 Essential Support & Business Critical Support (BCS)	Beratung, Training & Ausbildung/ know-how Transfer			

Die Ansätze müssen Menschen, Prozesse & Technologien berücksichtigen

Integrieren der Prozesse in das operative Geschäft

Meinungen …

Punkt.

Markus Grüneberg

Markus_Grueneberg@Symantec.com

+49 172 219 7043