pallas

Web Security

Veranstaltung:

eco AK Sicherheit 5. Mai 2010

Referent:

Stephan Sachweh, Technischer Leiter

Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information(at)pallas.de
http://www.pallas.de

Agenda

- Warum Web Security?
- Web Security im Browser
  - Internet Explorer SmartScreen-Filter
  - Firefox SafeBrowsing
- Web Security Gateways
  - SonicWALL Content Filtering Service (CFS)
  - McAfee Web Security Gateway (WebWasher)
  - Commtouch GlobalView URL Filtering Service
- Ein Test

Warum Web Security?

- Typische Einsatzgebiete für Web Security
  - Sicherheit
    - Spam und Malware Schutz
    - Schutz vor kompromittierten Web-Sites
  - Produktivität
    - Nicht Job-relevant (Sport, Spiele, Auktionen…)
    - Bandbreitenregulierung (Musik, Video)
  - Regulierung und Übereinstimmung mit Gesetzen
    - Hass-Seiten
    - Waffen / Gewalt
  - Jugendschutz
- In Deutschland primär über Jugendschutz vermarktet
- Jetzt Fokus Richtung Echtzeit-Schutz vor Gefährdungen

Internet Explorer SmartScreen-Filter

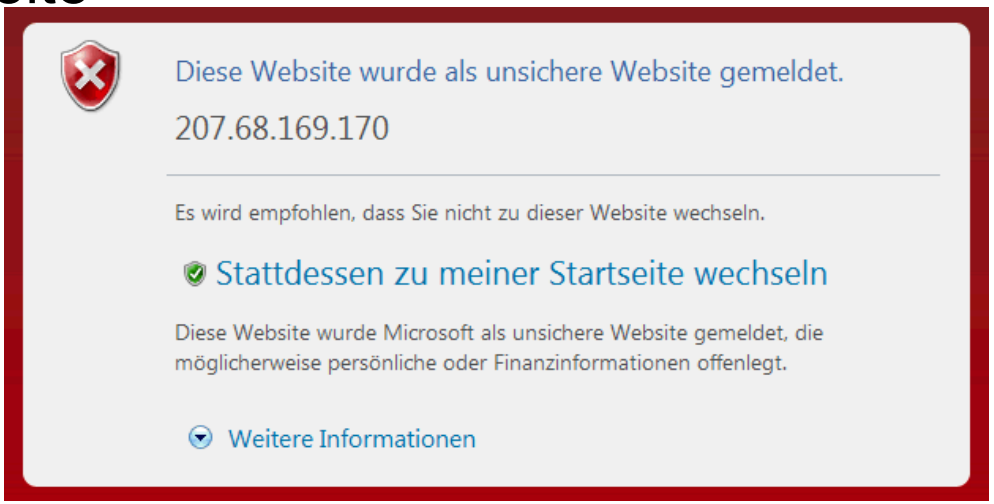
- Eingeführt in Internet Explorer 8
- Ergänzt den bereits in IE7 enthaltenden Phishingfilter

- Funktionsweise
  - URL Daten werden per https an den SmartScreen WebService von Microsoft zur Evaluation geschickt
  - Bei entsprechender Antwort generiert der IE Fehlerseiten

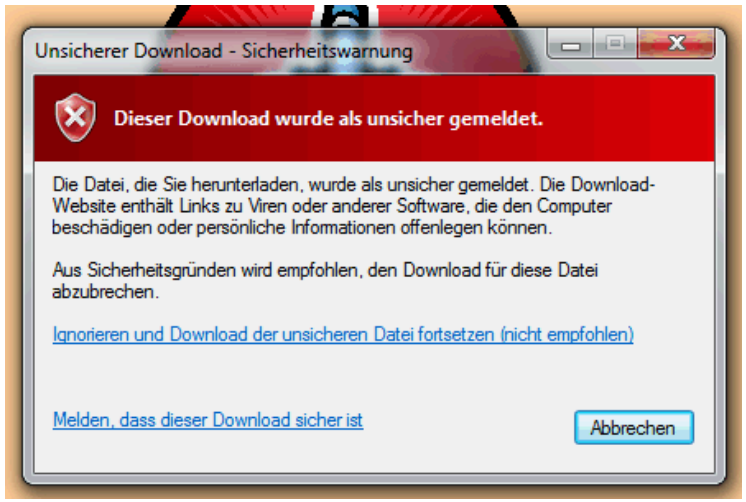
  - Microsoft sichert zu, die gelieferten Daten nicht zur Identifikationsfeststellung oder Werbung zu verwenden

Internet Explorer SmartScreen-Filter

- Beispiel: Unsichere Web-Seite



- Beispiel: Unsicherer Download



Internet Explorer SmartScreen-Filter

- Aktivierung bzw. Administration
  - Als Benutzer
    - Sicherheit -> SmartScreen-Filter
  - Als Administrator
    - Mittels Group Policy
      - *Verwalten von Phishingfilter deaktivieren*
      - *Verwalten von SmartScreen Filter deaktivieren*
      - *Umgehung der SmartScreen-Filterwarnungen verhindern*

- \+ Zentral Verwaltbar in AD-Umgebungen
- **\- Eine Umgehung des SmartScreen-Filter ist für jeden User mit lokalen Admin-Rechten möglich!**

Mozilla Firefox SafeBrowsing

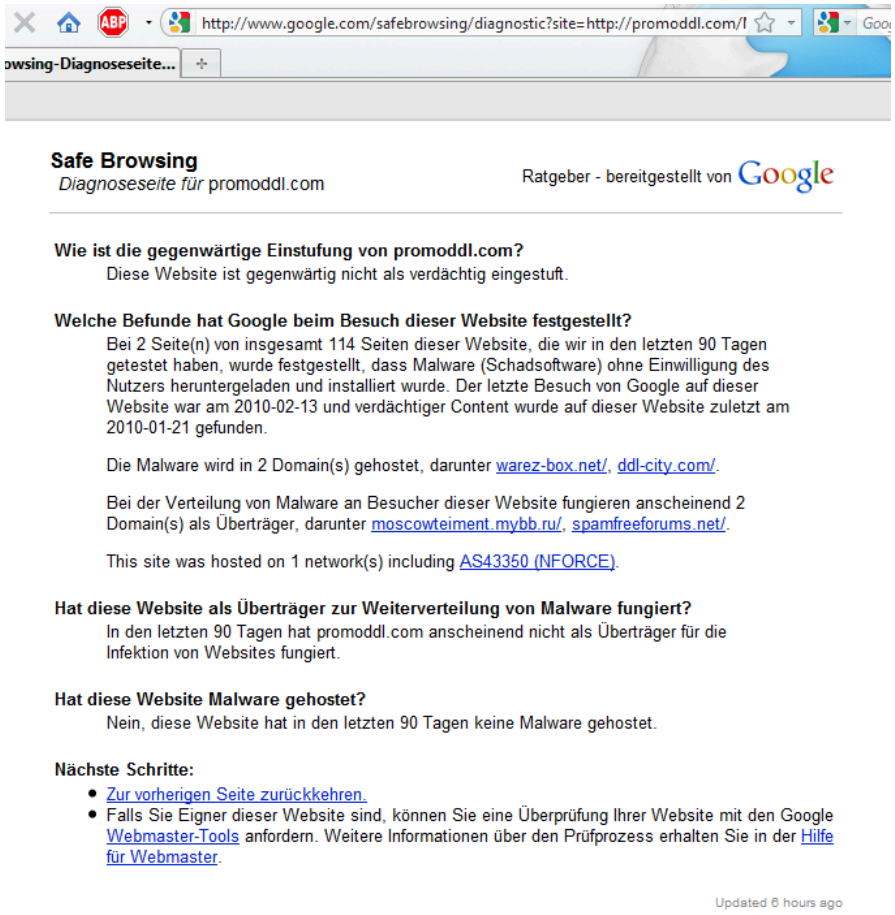
- Eingeführt in Firefox 3
- Basiert auf der Google SafeBrowsing Datenbank

- Funktionsweise
  - Periodische Updates der lokalen SafeBrowsing DB
  - Die DB enthält nur gehashte URLs
  - Vor Abfrage einer URL
    - Prüfung des Hashes der URL gegen die DB
    - Bei möglicher Gefahr Validierung über Google WebService
    - Warnung an den Benutzer über Fehlerseite
  - Google loggt die abfragende IP, ggf. Cookie und den Hash für „einige“ Wochen. Es gilt die Google Privacy Policy

Mozilla Firefox SafeBrowsing

- Beispiel einer Fehlerseite

- Test und Diagnose Seite von Google SafeBrowsing



Mozilla Firefox SafeBrowsing

- Aktivierung bzw. Administration
  - Als Benutzer
    - Extras -> Sicherheit
      - Webseite blockieren, wenn sie als attackierend gemeldet wurde
      - Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde
  - Als Administrator
    - Verteilung von prefs.js
    - FirefoxADM / ADMXPI
    - GPO for Firefox

    => keine wirklich empfehlenswerte zentrale Administration

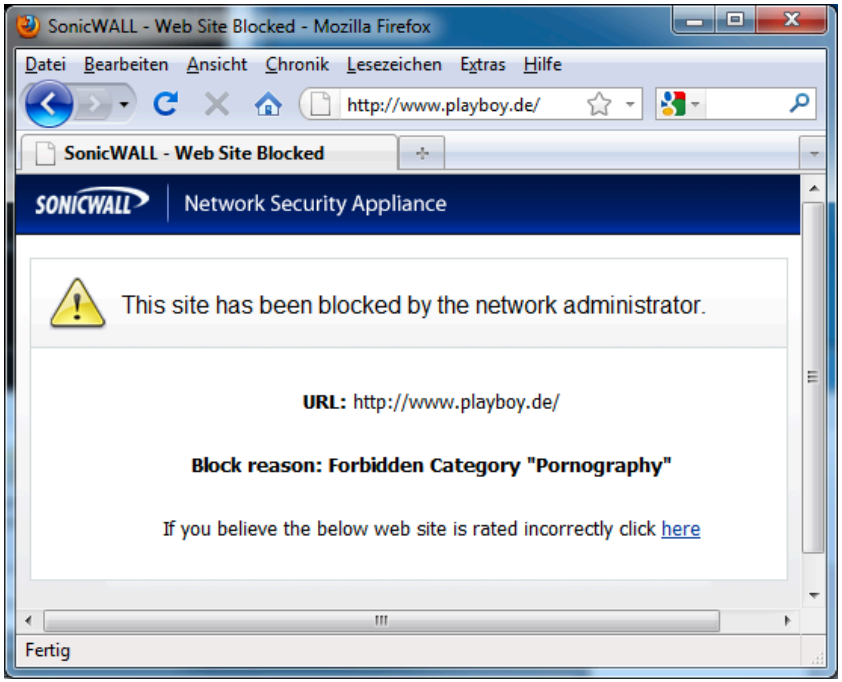
- **- Eine Umgehung des SafeBrowsing ist für jeden User mit lokalen Admin-Rechten möglich!**

SonicWALL Content Filtering Service

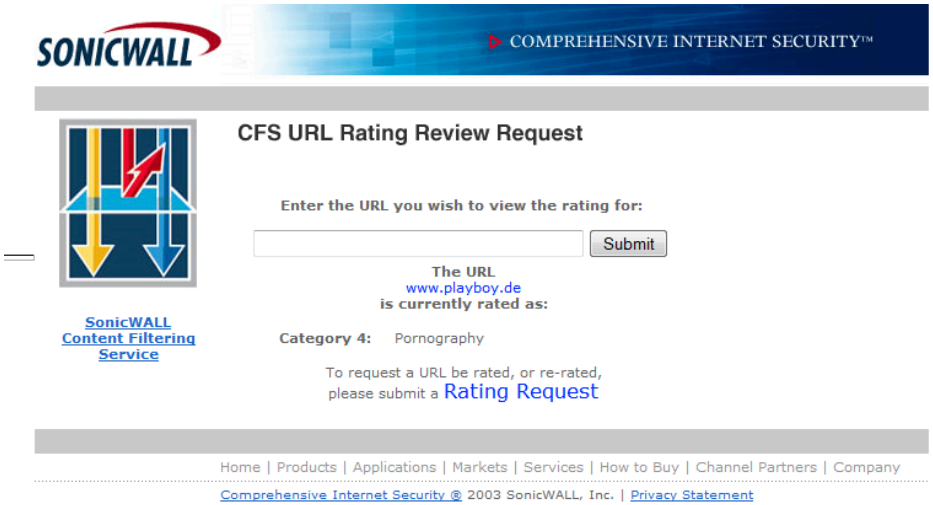
- Hersteller von UTM Security Appliances
- Content Filtering Service als integrierter Service in der Appliance
- 64 Kategorien, davon 1 Security relevant
  - 28. Hacking/Proxy Avoidance System
- Manuelles White- und Blacklisting möglich
- Bindung der Security Policy an IP-Bereiche
- Als Security Gateway verpflichtende Kontrolle für die Benutzer
- Blockade Seite frei gestaltbar
- https Sites nur auf IP-Basis prüfbar
- Kategoriebewertungen über http://cfssupport.sonicwall.com einsehbar

SonicWALL Content Filtering Service

- Exemplarische Blockade-Seite



- Anzeige der Kategorie einer Web-Site



SonicWALL Content Filtering Service

- Zentrale Administration durch Security Gateway möglich
- Umgehung durch den Benutzer unmöglich
- Recht kleiner URL-Cache => Online Verbindung benötigt
- Wenig Security relevante Kategorien
- Nutzbar mit jedem Browser
- Kein Realtime!

- Für kleine Installationen und geringere Anforderungen brauchbar
- Für große Installationen ungeeignet

McAfee WebWasher (TrustedSource)

- Als Software und als Appliance nutzbar
- URL-Filter Teil der Lösung, weitere Teile
  - SSL-Scanner
  - Malware-Scanner
  - Content-Scanner
- Sehr flexible Aktionen (Allow, Block, Authorized Override, Coaching, Delay, Quotas, Timeframes)
- Bindung der Policy an IP-Adressen, Namen
- Lokale Datenbank mit inkrementellen Updates
  - Alle 3 Stunden wird geprüft
  - Ca. 1-2 mal am Tag Änderungen der Datenbank

  => nicht Realtime

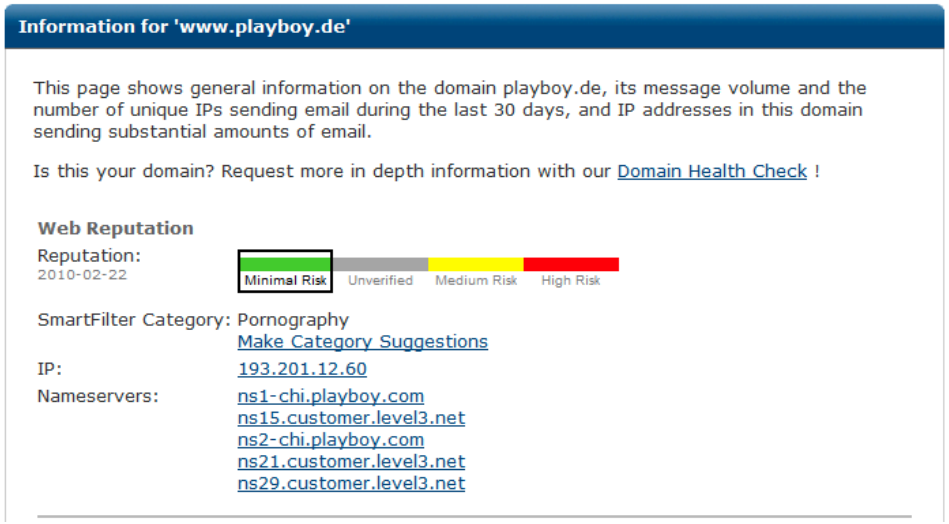
McAfee WebWasher (TrustedSource)

- 98 Kategorien, davon 10 Security Relevant
  - Criminal Activities
  - Malicious Sites
  - Hacking/Computer Crime
  - Spyware/Adware
  - Phishing
  - Spam URLs
  - Illegal Software
  - Anonymizers
  - Anonymizing Utilities
  - Residential IP Addresses
- Block gemäß Web-Reputation möglich
- Einsicht in Kategorien und Bewertungen unter
  - http://www.trustedsource.com/

McAfee WebWasher (TrustedSource)

- Exemplarische Fehlermeldung

- TrustedSource Bewertung



McAfee WebWasher (TrustedSource)

- Zentrale Administration durch Proxy Security Gateway
- Umgehung durch den Benutzer unmöglich sofern Proxy Zwang konfiguriert
- Enterprise Lösung
- Lokale Datenbank
- Umfangreiche Kategorien
- Nutzbar mit jedem Browser
- Kein Realtime!

- Für große Installationen mit feingranularen Einstellmöglichkeiten geeignet
- Sehr flexible Lösung

Commtouch GlobalView URL Filtering Service

- SDK für Integration in OEM Lösung
- Teil der Gesamtlösung von Commtouch für Realtime Dienste
- Commtouch liefert für einen Deep Link bis zu 5 Kategorien
- Aktionen werden durch OEM realisiert
  - Allow
  - Block
- Bindung der Policy wird durch OEM realisiert
  - IP-Adressen
  - Namen möglich
- Lokaler Cache
  - Realtime Abfrage
  - Caching liegt überlicherweise bei >99 %

Commtouch GlobalView URL Filtering Service

- 64 Kategorien, davon 8 Security relevant
  - Anonymizers
  - Compromised
  - Criminal Activity
  - Phishing & Fraud
  - Spam Sites
  - Malware
  - Botnets
  - Hacking
  - Illegal Software
- Einsicht in Kategorien und Bewertungen unter
  - Pallas Kundenportal für Pallas Kunden
  - http://www.commtouch.com/url-miscat

Commtouch GlobalView URL Filtering Service

Kontinuierliche Datenquellen für die URL Datenbank

Commtouch GlobalView URL Filtering Service

- Exemplarische Fehlermeldung

- Commtouch Kategorie (n)

- Rot markiert Daten des aufrufenden Benutzers

Commtouch GlobalView URL Filtering Service

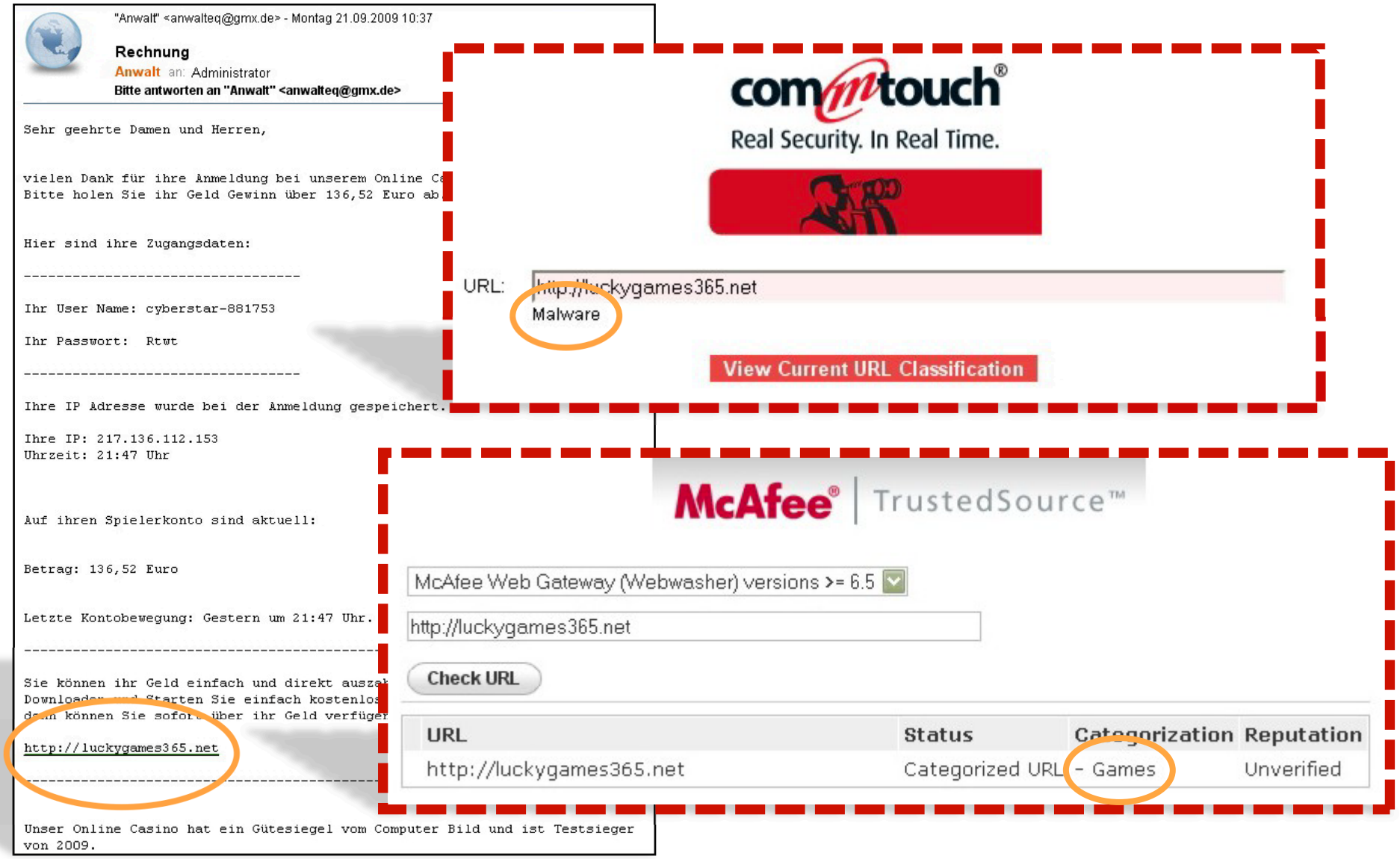
- Kategorisierung von Deep Links schützt vor Malware
  - auf Community Sites wie z.B. Facebook, Xing, Linked-In, Blogspot
  - auf infizierten, regulären Seiten
- Realtime durch
  - in the Cloud Echtzeitabfrage beschleunigt durch Cache
  - Integration mit Real-Time Anti-Spam und Zero-Hour Mail-Security
    - URLs in Malware/Spam Mails werden in Echtzeit kategorisiert
  - Häufung von Kategorie „Unbekannt“ führt zur Kategorisierung, User Feedback Schleife

Commtouch GlobalView URL Filtering Service

- Zentrale Administration durch Proxy Security Gateway
- Umgehung durch den Benutzer unmöglich sofern Proxy Zwang konfiguriert
- Enterprise Lösung
- Lokaler Cache (> 99% Cache Hit Rate)
- Umfangreiche Kategorien
- Nutzbar mit jedem Browser
- **Realtime!**
- **Deep Links werden bewertet!**

- Technologisch High End
- Für große und mittlere Installationen geeignet, „kleine“ Installationen über Pallas Mietmodell

Ein Bewertungsbeispiel

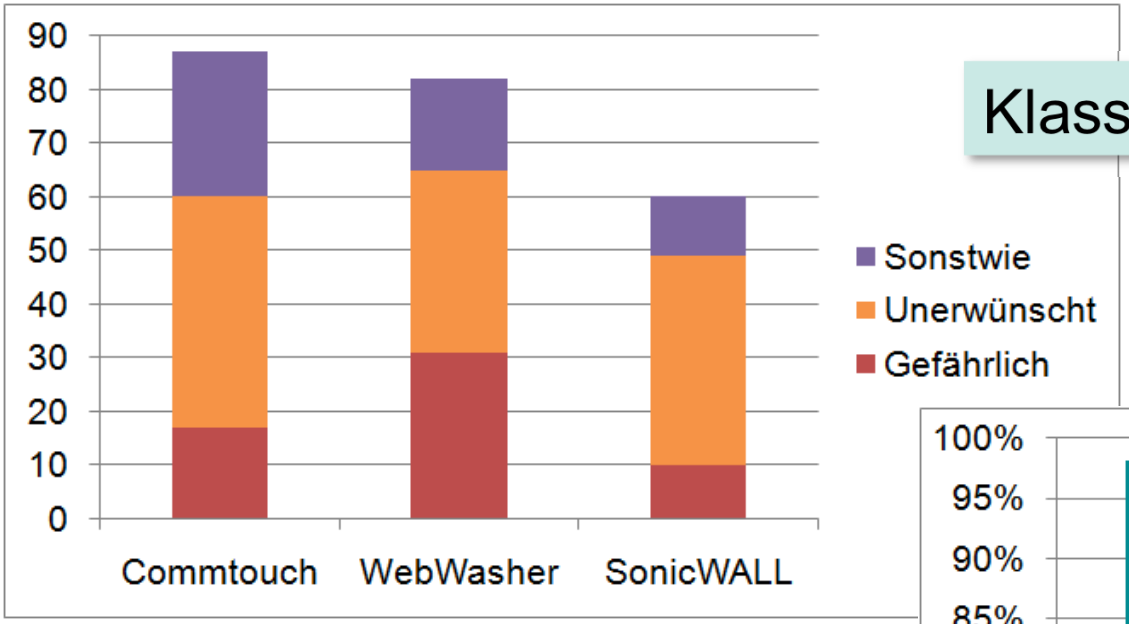


Zwei Tests: 87 fiese / 25 T URLs aus der Praxis

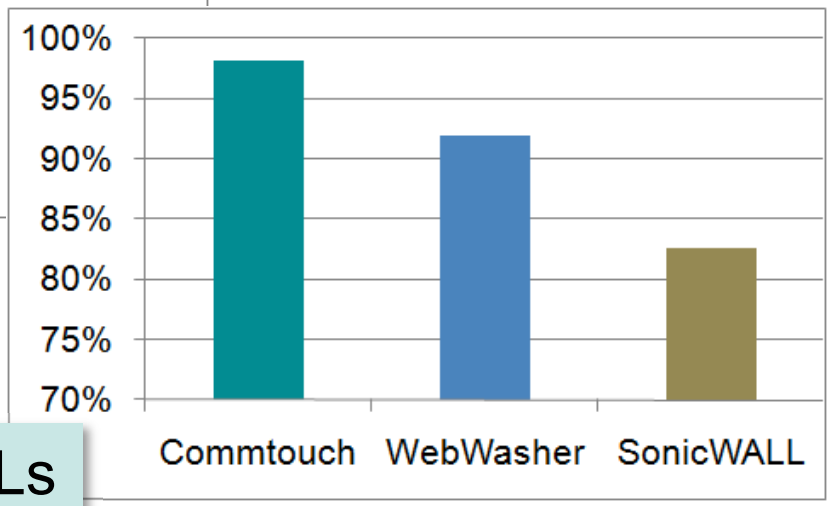
87 fiese URLs: von wenigstens einer Lösung als **Gefährlich** oder **Unerwünscht** klassifiziert

Gefährliche: criminal, illegal, compromised, malicious…

Unerwünschte: gambling, porno, dating…



Klassifizierung fieser URLs



Erkennungsrate bei 25.000 URLs

Gerne beantworte
ich Ihre Fragen

pallas

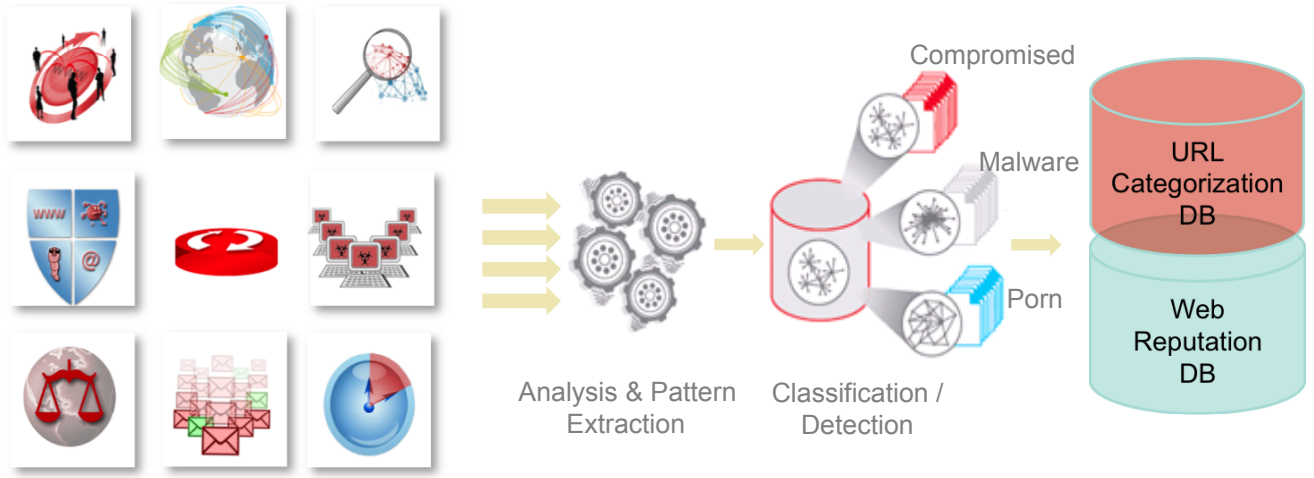
Stephan Sachweh
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

stephan.sachweh(at)pallas.de
http://www.pallas.de

Detection Center Architecture

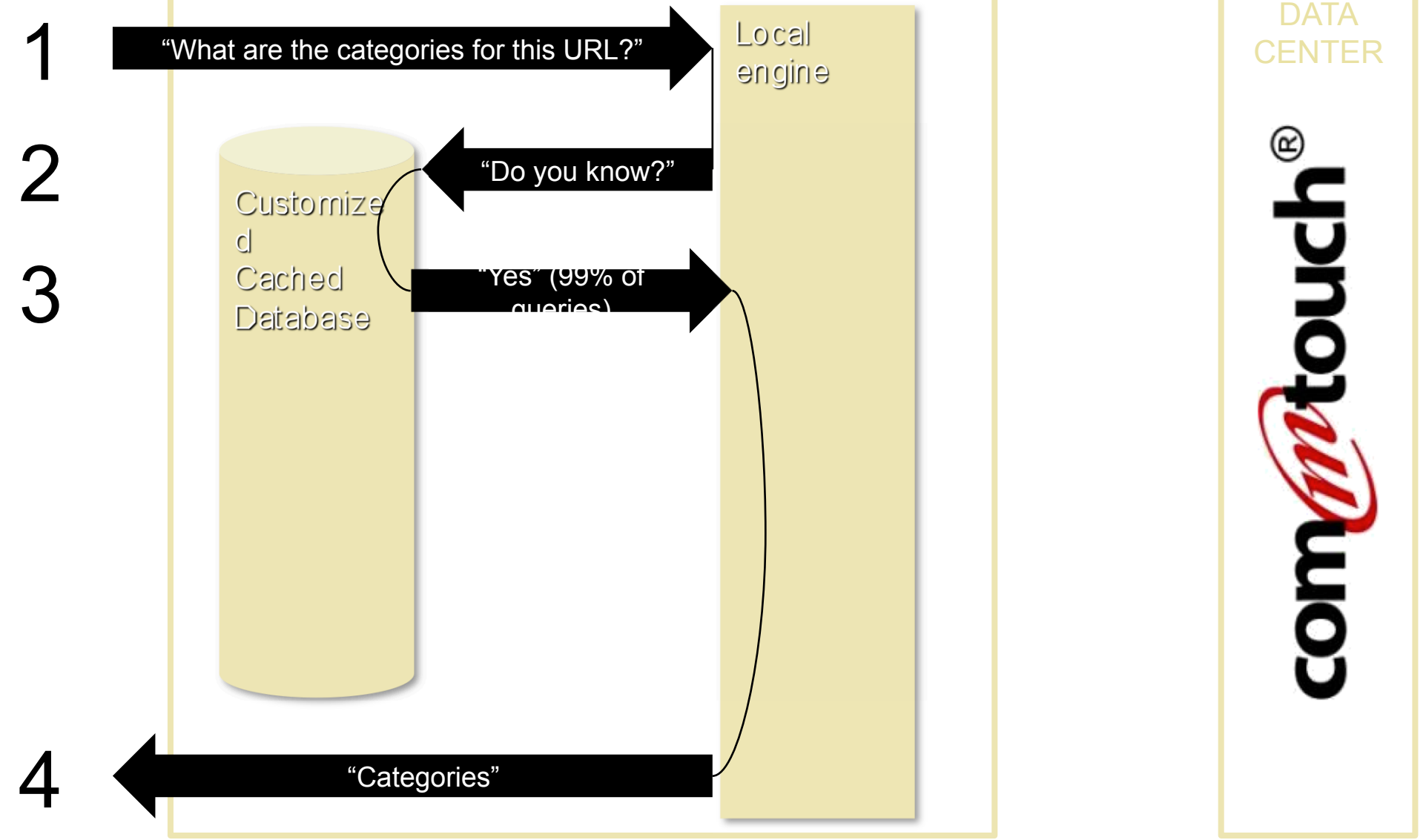
Detection & Classification Center

Comtouch

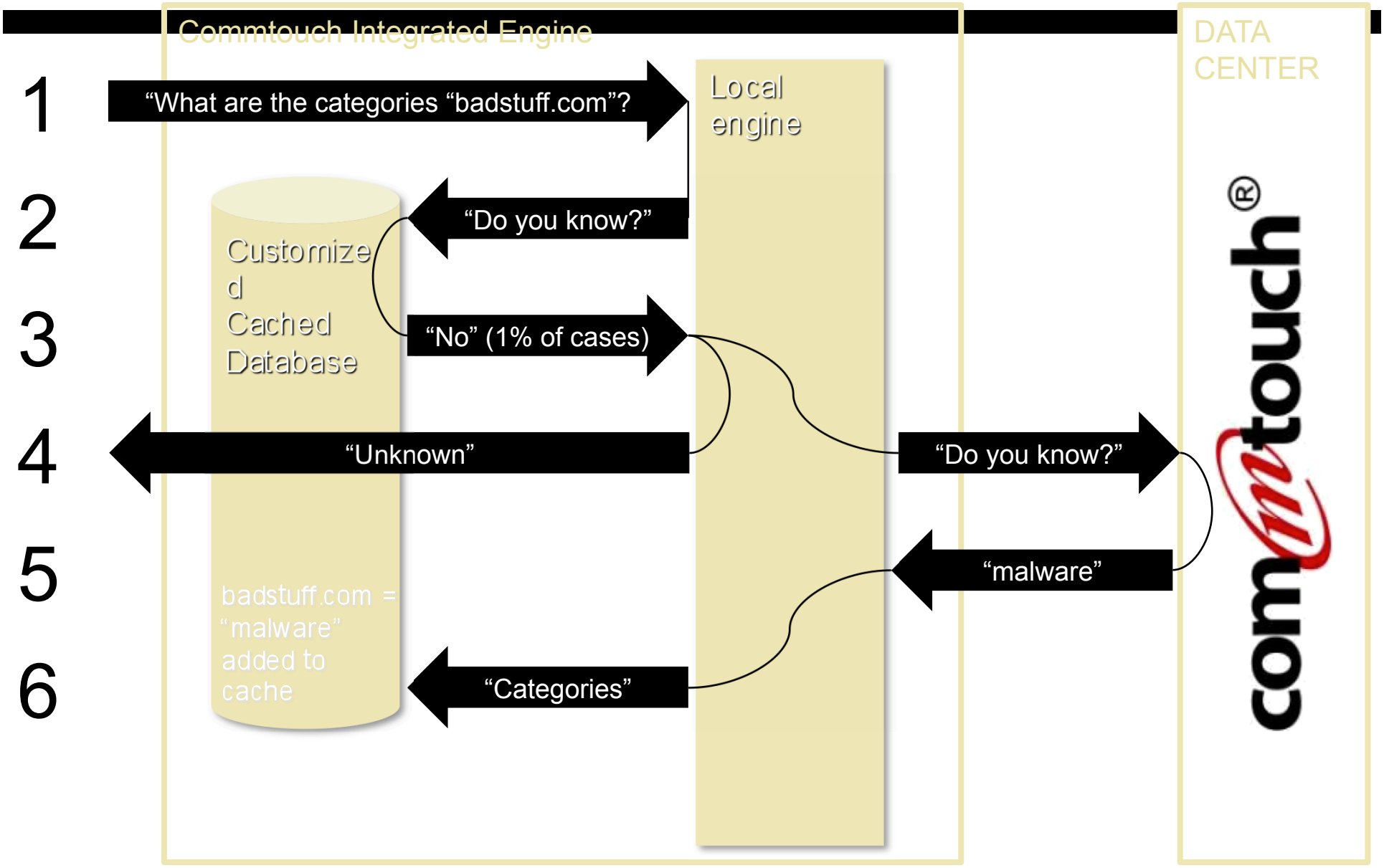


- **Categorization**
  - Link analysis
  - Text classification
  - Image classification
  - Profile analysis
- **Detection**
  - Phishing analysis
  - spam detection
  - Security alliances partners
  - >120 Web Site parameters dynamically set reputation

How it works – "in cache" query flow (99% of queries)



How it works – "in center" query flow (1% of queries)



Commtouch architecture