



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](mailto:information(at)pallas.de)
<http://www.pallas.de>





- 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



- 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



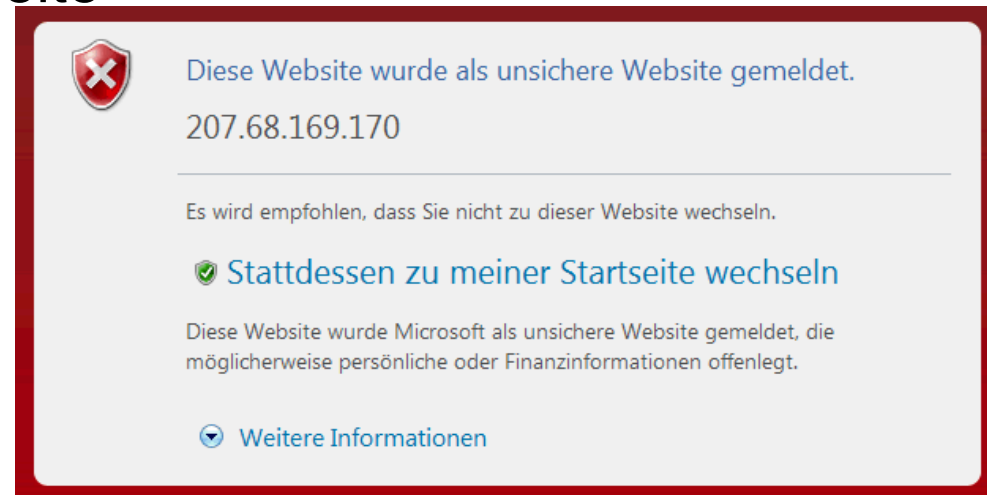
- Eingeführt in Internet Explorer 8
- Ergänzt den bereits in IE7 enthaltenen Phishingfilter

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

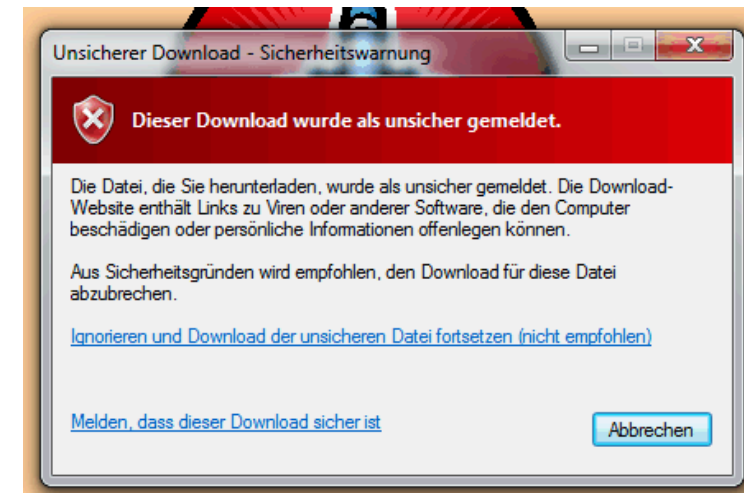
 - Microsoft sichert zu, die gelieferten Daten nicht zur Identifikationsfeststellung oder Werbung zu verwenden



■ Beispiel: Unsichere Web-Seite



■ Beispiel: Unsicherer Download





- 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!**



- 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



■ Beispiel einer Fehlerseite

Als Betrugsversuch gemeldete Webseite!

Die Webseite auf www.yewknee.com wurde als Betrugsversuch gemeldet und gemäß Ihrer Sicherheitseinstellungen blockiert

Mit Betrugsseiten versuchen Kriminelle Sie dazu zu bringen, persönliche oder finanzielle Daten preiszugeben. Dabei ahnen sie in betrügerischer Absicht Webseiten oder E-Mails nach, denen Sie eventuell vertrauen.

Falls Sie hier persönliche Daten eingeben, müssen Sie mit Identitätsdiebstahl oder sonstigem Betrug rechnen.

[Diese Seite verlassen](#) [Warum wurde diese Seite blockiert?](#)

[Diese Warnung ignorieren](#)

■ Test und Diagnose Seite von Google SafeBrowsing

Safe Browsing
Diagnoseseite für promoddl.com Ratgeber - bereitgestellt von **Google**

Wie ist die gegenwärtige Einstufung von promoddl.com?
Diese Website ist gegenwärtig nicht als verdächtig eingestuft.

Welche Befunde hat Google beim Besuch dieser Website festgestellt?
Bei 2 Seite(n) von insgesamt 114 Seiten dieser Website, die wir in den letzten 90 Tagen getestet haben, wurde festgestellt, dass Malware (Schadsoftware) ohne Einwilligung des Nutzers heruntergeladen und installiert wurde. Der letzte Besuch von Google auf dieser Website war am 2010-02-13 und verdächtiger Content wurde auf dieser Website zuletzt am 2010-01-21 gefunden.

Die Malware wird in 2 Domain(s) gehostet, darunter warez-box.net/, ddl-city.com/.

Bei der Verteilung von Malware an Besucher dieser Website fungieren anscheinend 2 Domain(s) als Überträger, darunter moscowteiment.mybb.ru/, spamfreeforums.net/.

This site was hosted on 1 network(s) including [AS43350 \(NFORCE\)](#).

Hat diese Website als Überträger zur Weiterverteilung von Malware fungiert?
In den letzten 90 Tagen hat promoddl.com anscheinend nicht als Überträger für die Infektion von Websites fungiert.

Hat diese Website Malware gehostet?
Nein, diese Website hat in den letzten 90 Tagen keine Malware gehostet.

Nächste Schritte:

- [Zur vorherigen Seite zurückkehren](#).
- Falls Sie Eigner dieser Website sind, können Sie eine Überprüfung Ihrer Website mit den Google [Webmaster-Tools](#) anfordern. Weitere Informationen über den Prüfprozess erhalten Sie in der [Hilfe für Webmaster](#).

Updated 6 hours ago



- 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

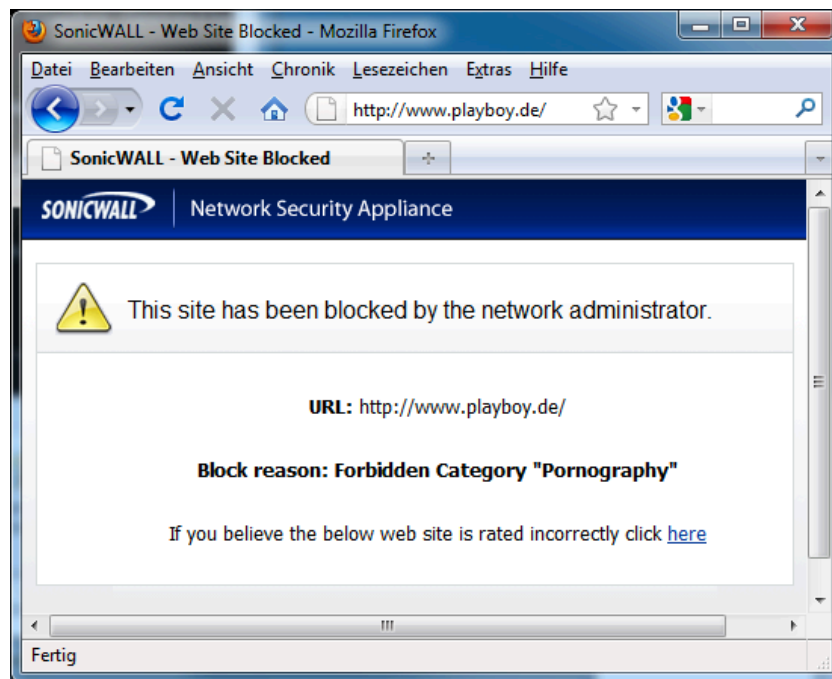
- - **Eine Umgehung des SafeBrowsing ist für jeden User mit lokalen Admin-Rechten möglich!**



- 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



- 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**

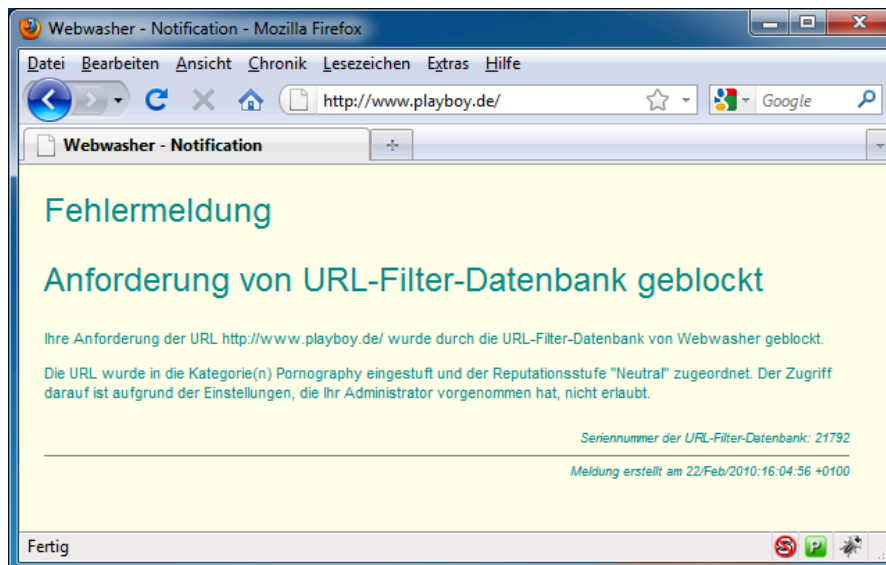


- 98 Kategorien, davon 10 Security Relevant
 - Criminal Activities
 - Malicious Sites
 - Hacking/Computer Crime
 - Spyware/Adware
 - Phishing
 - Spam URLs
 - Illegal Software
 - Anonymizers
 - Anonymizing Utilities
 - Residential IP Addresses
- Block gemäß Web-Reputation möglich
- Einsicht in Kategorien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

McAfee WebWasher (TrustedSource)



■ Exemplarische Fehlermeldung




■ TrustedSource Bewertung

Information for 'www.playboy.de'

This page shows general information on the domain playboy.de, its message volume and the number of unique IPs sending email during the last 30 days, and IP addresses in this domain sending substantial amounts of email.

Is this your domain? Request more in depth information with our [Domain Health Check](#) !

Web Reputation
Reputation: 2010-02-22 

SmartFilter Category: Pornography
[Make Category Suggestions](#)

IP: [193.201.12.60](#)

Nameservers: [ns1-chi.playboy.com](#)
[ns15.customer.level3.net](#)
[ns2-chi.playboy.com](#)
[ns21.customer.level3.net](#)
[ns29.customer.level3.net](#)

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**



- 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 üblicherweise bei >99 %



- 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>



Kontinuierliche Datenquellen für die URL Datenbank



Benutzer
Anfragen



Traffic
Sammler an
Knotenpunkten




Web trends



Security
Alliance
Partner




Gefährdungsanalyse,
Zombie-Netze



Dynamische
URL
Analyse



Spam
trends
2,000,000,000 Mails pro Tag



0-hour
malware
patterns



■ Exemplarische Fehlermeldung

FEHLER

Der angeforderte URL konnte nicht geholt werden

Während des Versuches, den URL **http://www.playboy.de/** zu laden, trat der folgende Fehler auf

- Zugriff verweigert auf Basis der Pallas RealTime URL Filter Datenbank powered by Commtouch

- Anfragende IP: 10.234.1.222
- Benutzername: ssachweh
- Kategorien der URL:
33 Pornography/Sexually Explicit

Aufgrund von Zugriffsbeschränkungen ist Ihre Anfrage zur Zeit nicht erlaubt.
Bitte kontaktieren Sie Ihren Service Provider, wenn Sie der Meinung sind, daß dies nicht korrekt ist.

- Rot markiert Daten des aufrufenden Benutzers

■ Commtouch Kategorie (n)

pallas Pallas Kundenportal

Commtouch Realtime Web Security

Web-Adresse (URL):

URL	CatID	Kategorienname
www.playboy.de	33	Pornography/Sexually Explicit

Bitte wählen

Kommentar für diese Meldung (optional)



- 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



"Anwalt" <anwalteq@gmx.de> - Montag 21.09.2009 10:37

Rechnung
Anwalt an: Administrator
Bitte antworten an "Anwalt" <anwalteq@gmx.de>

Sehr geehrte Damen und Herren,

vielen Dank für ihre Anmeldung bei unserem Online Casino.
Bitte holen Sie ihr Geld Gewinn über 136,52 Euro ab.

Hier sind ihre Zugangsdaten:

Ihr User Name: cyberstar-881753
Ihr Passwort: Rtwt

Ihre IP Adresse wurde bei der Anmeldung gespeichert.

Ihre IP: 217.136.112.153
Uhrzeit: 21:47 Uhr

Auf ihren Spielerkonto sind aktuell:

Betrag: 136,52 Euro

Letzte Kontobewegung: Gestern um 21:47 Uhr.

Sie können ihr Geld einfach und direkt auszahlen.
Downloaden und Starten Sie einfach kostenlos
dann können Sie sofort über ihr Geld verfügen.
<http://luckygames365.net>

Unser Online Casino hat ein Gütesiegel vom Computer Bild und ist Testsieger von 2009.

Real Security. In Real Time.

URL: <http://luckygames365.net>
Malware

View Current URL Classification

McAfee Web Gateway (Webwasher) versions >= 6.5

<http://luckygames365.net>

Check URL

URL	Status	Categorization	Reputation
<u>http://luckygames365.net</u>	Categorized URL	- Games	Unverified

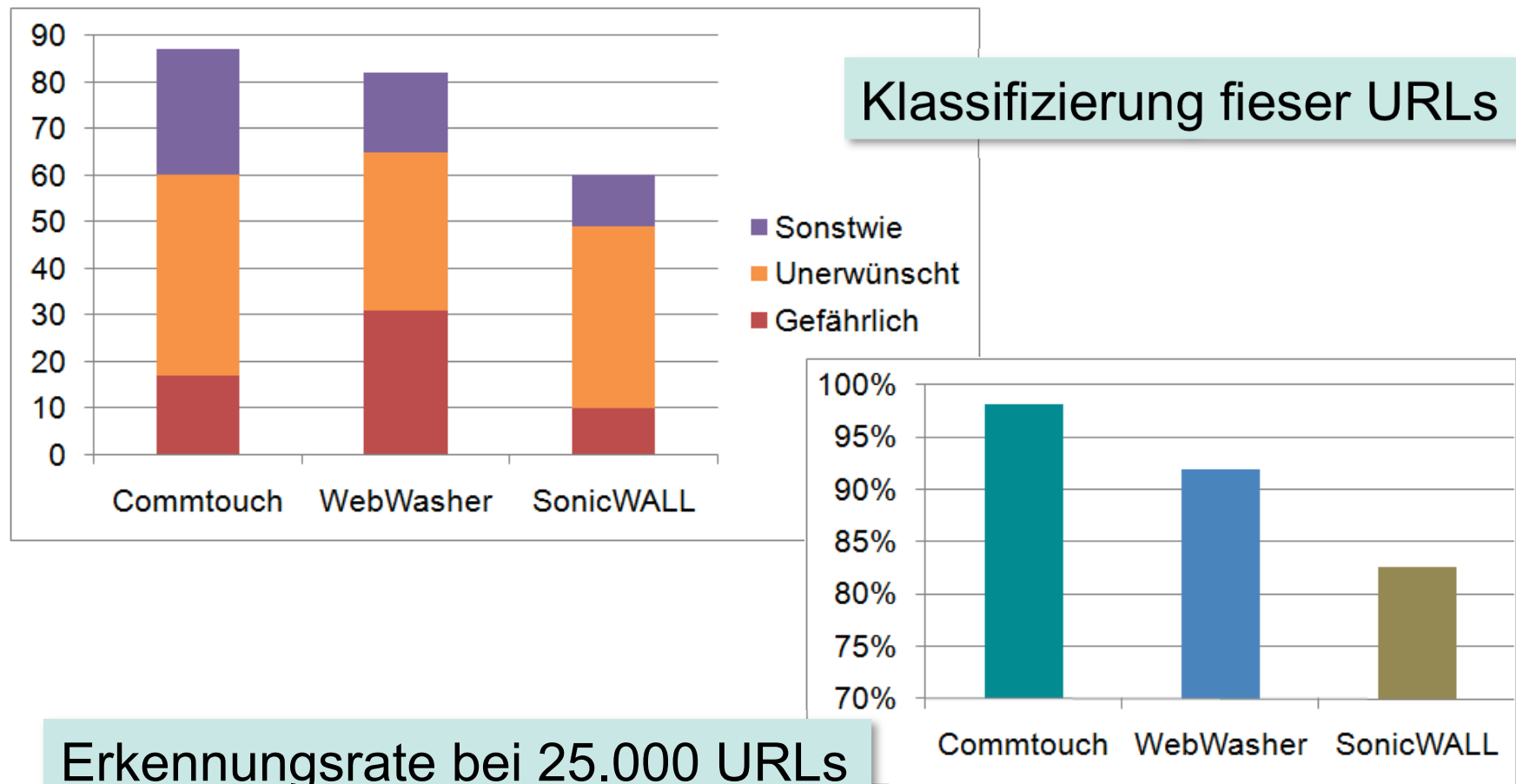
Zwei Tests: 87 fiese / 25 T URLs aus der Praxis



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

Gefährliche: criminal, illegal, compromised, malicious...

Unerwünschte: gambling, porno, dating...



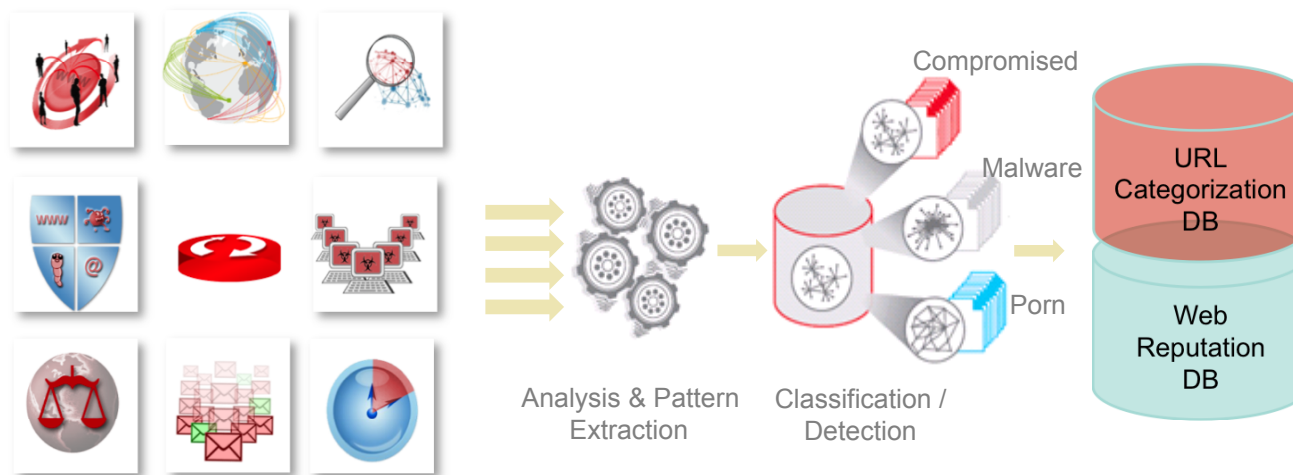
Gerne beantworte
ich Ihre Fragen



Stephan Sachweh
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

[stephan.sachweh\(at\)pallas.de](mailto:stephan.sachweh(at)pallas.de)
<http://www.pallas.de>

Detection Center Architecture



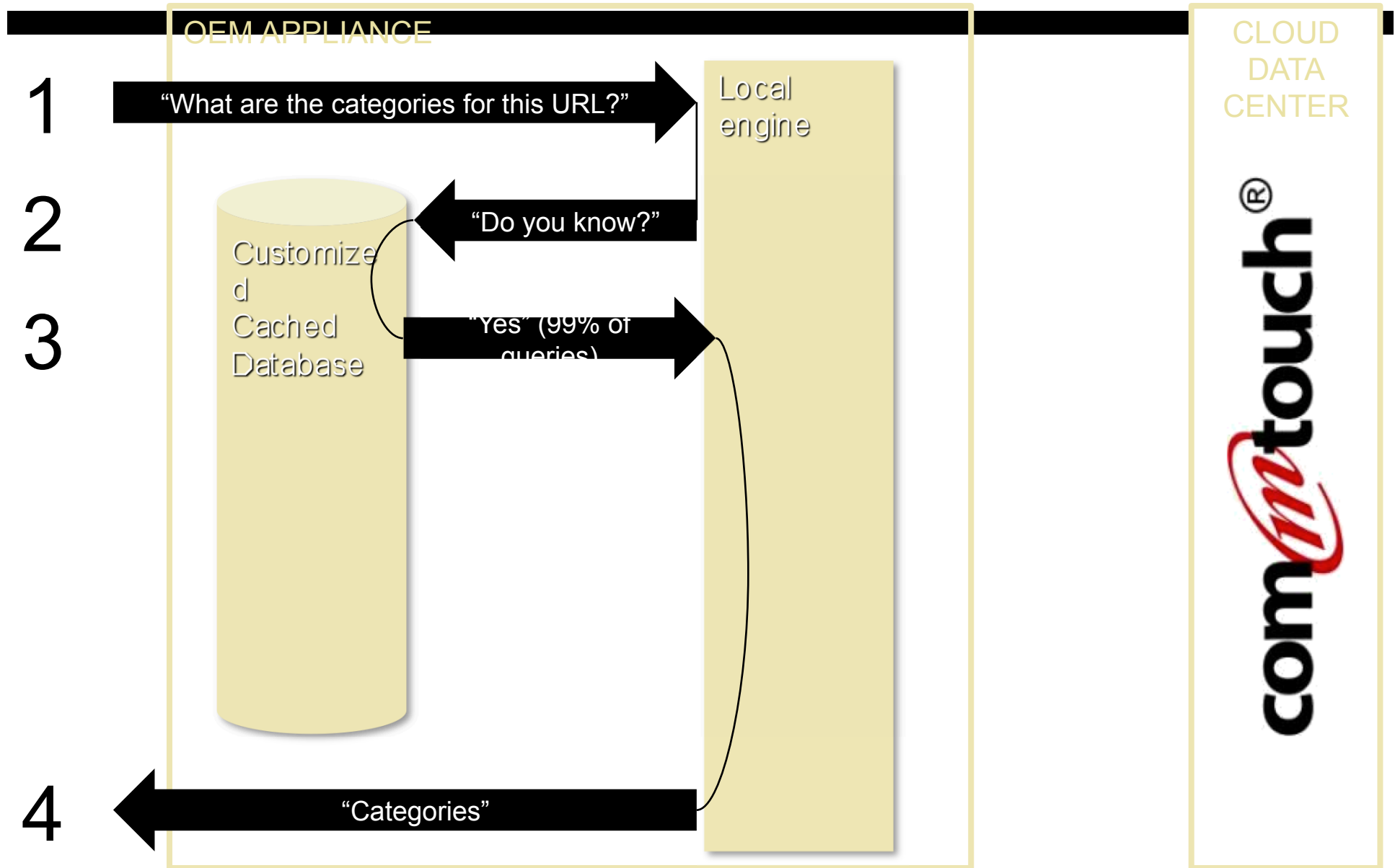
•Categorization

- Link analysis
- Text classification
- Image classification
- Profile analysis

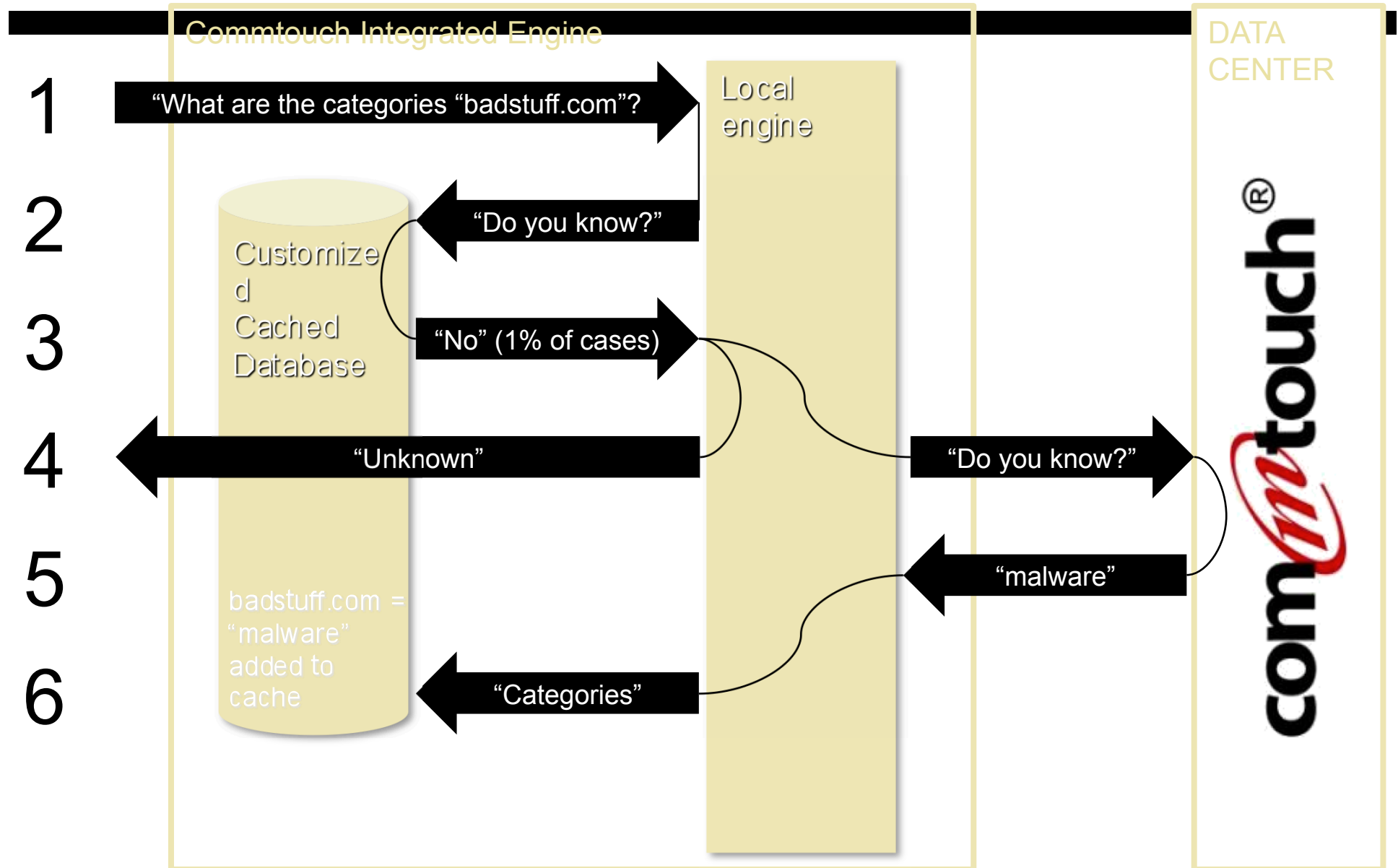
•Detection

- 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

