

Webanwendungen Hacker's Best Friend

Andreas Bröhl

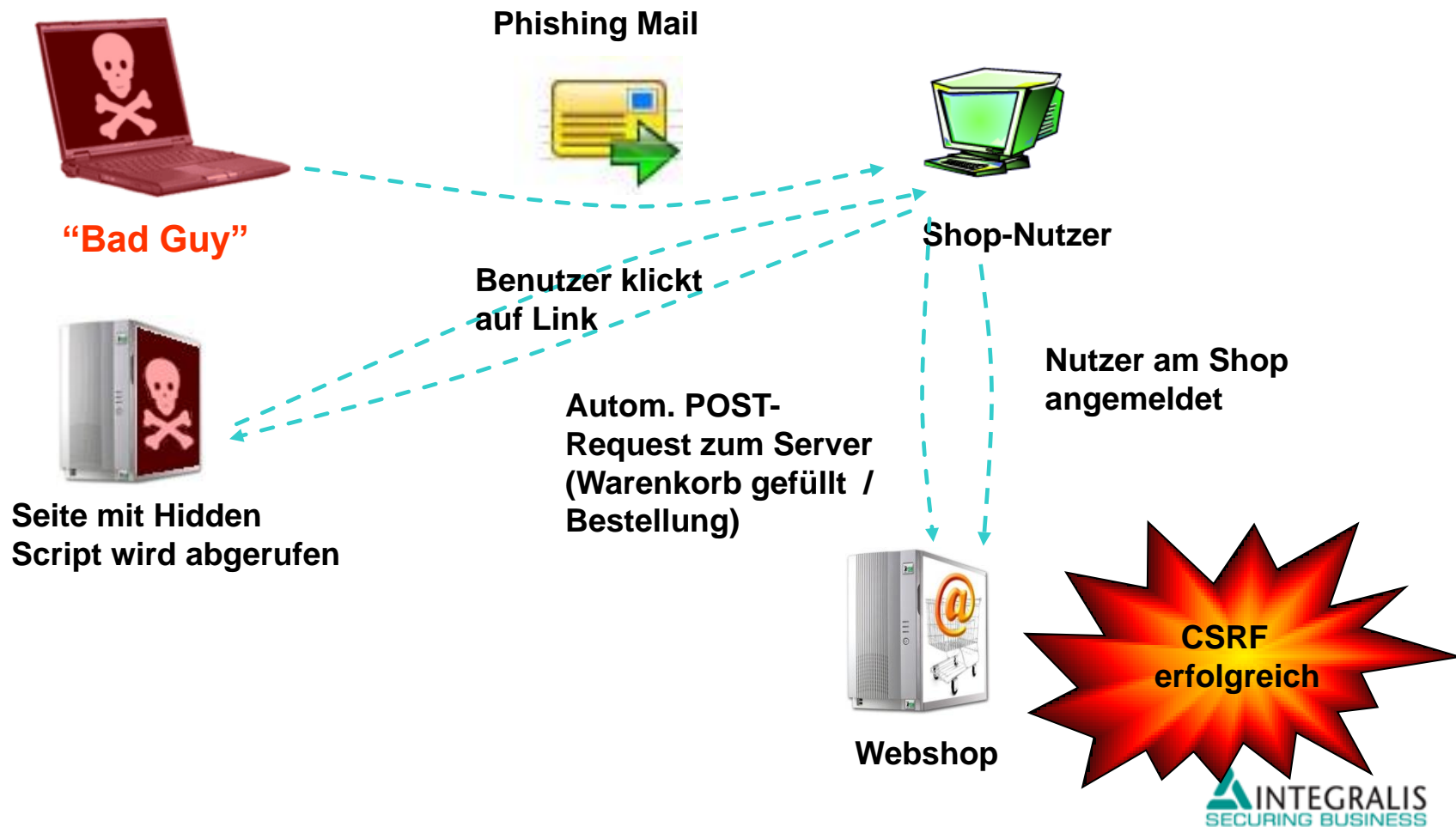
Business Development Manager S3

23.06.2009

Angriffe mittels Cross Site Request Forgery

- Ein angemeldeter Benutzer wird dazu verleitet eine ungewollte Aktion in einer Webanwendung durchzuführen, z.B.:
 - Kontoänderung
 - Passwortänderung
 - Bestellung
- Initiierung erfolgt durch
 - Cross Site Scripting
 - Phishing Mails / Social Engineering

Ablauf des Angriffes



Das Labor



“Bad Guy”



Shop-Nutzer



**Webshop
“www.acme.de”**

- Windows XP SP3
- „Out of the Box“
- Hacking Tools:
 - Webbrowser
 - lokaler Webserver
 - lokaler Proxy
- Windows Vista
- Up-to-Date



Webserver



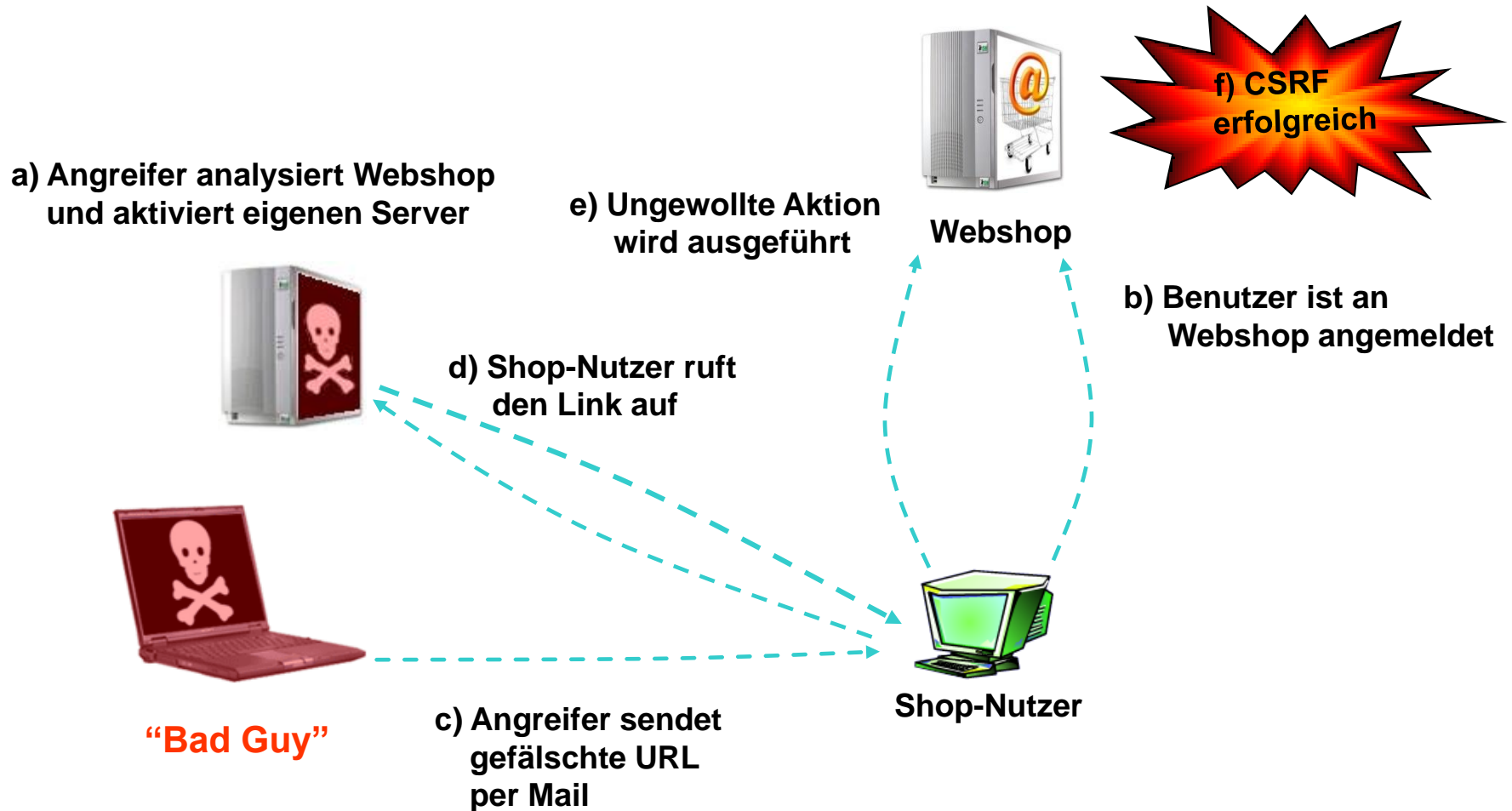
Applikations-
Server



Datenbank

MAGENTO eCommerce Shop
(Ubuntu 8.04 / LAMP)

Cross Site Request Forgery – LIVE



Permanentes Cross Site Scripting

- Script-Code wird in verwundbare Webanwendung vom Angreifer eingebaut, z.B: Forum, Gästebuch
- Benutzer meldet sich an der Anwendung an und besucht die modifizierte Seite
- Schadcode wird im Browser des Benutzers ausgeführt
- Mögliches Resultat ist Session-Hijacking:
 - Senden des Cookies an den Angreifer
 - Übernahme der Session unter Verwendung des Cookies

Permanentes Cross Site Scripting



Schutzmassnahmen für Webanwendungen

- Cross Site Request Forgery
 - Session spezifischer Identifier in die Webseite mit einbauen, der zusätzlich zum Cookie vom Server geprüft wird
- Cross Site Scripting
 - Filterung der Eingaben bei der Programmierung der Webanwendung
- Generelle Empfehlungen
 - Regelmässige Auditierung aller interaktiven Webanwendungen
 - Filterung der Eingaben durch vorgeschaltete Web Application Firewall

Fragen und Antworten



Integralis S3-Services
s3@integralis.de

Integralis® S3
System Security Services