Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Wirtschaft

9. Tagung der Schweizerischen Expertenvereinigung
«Bekämpfung der Wirtschaftskriminalität»

Phishing – Betrug im Internet

Einführung, Beispiele und Ermittlungsansätze

IWI Institut für Wirtschaftsinformatik

Marco Carraro
Wissenschaftlicher Mitarbeiter
IT-Security & IT-Forensics

FH Zentralschweiz

Agenda

- Begriffe / Ziel
- Aktuelle Beispiele
- Analysemöglichkeiten
  - Analyse der E-Mail-Header
  - Rückverfolgen einer IP-Adresse
- 3 Bereiche eines Phishing Angriffs
    - Phishing-Mail
    - Phishing-Webseite
    - Geldfluss
- Schutzmassnahmen

Begriffe - Klassisches Phishing

- Kunstwort aus „password“ und „fishing“.
- Bedeutung: Nach Passwörtern fischen.
- Begehrte Angriffsziele sind Online-Dienstleister
  - Online-Finanzinstitute (dazu gehören heute alle Finanzinstitute)
  - Online-Bezahl-Dienstleister (PayPal etc.)
  - Online-Auktionshäuser (Ricardo, Ebay etc.)
- Mithilfe *gefälschter* E-Mails werden mögliche Kunden der Online-Dienstleister auf eine *gefälschte* Webseite gelockt, wo sie ihre vertraulichen Anmeldeinformationen eingeben.
- Mit den ausspionierten Informationen versucht der Angreifer, Transaktionen auf Kosten des Opfers auszuführen.

Ziel von Phishing

=> Vertrauliche Login-Informationen (Benutzername/PW etc.)

- Gewinn erzielen
- An vertrauliche Daten gelangen
- (Identitätsdiebstahl)
- (Leistungen erschleichen)

Begriffe - Pharming

- Oberbegriff für verschiedene DNS-Angriffe
- DNS-Abfrage des Internetbrowsers wird manipuliert (z. B. Manipulation der Host-Datei unter Windows)
- Die korrekte Eingabe einer Internet-Adresse führt zu einer gefälschten Phishing-Webseite

- Die Ziele sind die gleichen wie beim Phishing

Aktuelle Beispiele

PostFinance: Phishing-Mails im Umlauf

Informationen, KOBIK, 17.08.2012

Bern. Seit Dienstag 5. Juni 2012 versuchen Betrüger, als PostFinance getarnt, per Mail an Daten von Postfinance-Karten von Bürgern zu gelangen.

KOBIK empfiehlt, bei Erhalt dieses E-Mails zu löschen. PostFinance fordert niemals per E-Mail zu einem Login oder zur Eingabe von Sicherheitselementen auf. Der Einstieg ins E-Finance führt ausschliesslich über die Website www.postfinance.ch.

Inhalt des Phishing-E-Mails

Von: **Post Finance <info@Postfinance.ch>**
Betreff: Sehr Geehrter Kunde,
Datum: 15. August 2012 08:55:51 MESZ
An: undisclosed-recipients:;

Sehr Geehrter Kunde,

Die PostFinance verwendet viel Aufmerksamkeit und Sorgfalt für die Sicherheit und Integrität aller unserer Bankkonten. Wir möchten Sie hiermit bitten, folgendes zu beachten: Im vergangenen Jahr wurde PostFinance, zusammen mit vielen anderen Schweizer Banken, zur Zielscheibe des weit verbreiteten Internet-Betruges. Daher haben wir in den letzten Monaten ein großes Projekt zur Bekämpfung der Internetkriminalität ins Leben gerufen.

Alle Online-Bankkonten sollten mit einem neu entwickelten Sicherheitssystem verbunden werden, welches verdächtige Bewegungen und Verläufe auf Ihrem Online-Bankkonto sofort aufspüren und beheben kann.

Zu Ihrer Sicherheit wurde veranlasst, dass Ihr Online-PostFinance-Konto mit dem neu entwickelten Sicherheitssystem eingerichtet wurde. Bitte nehmen Sie sich 5-10 Minuten Zeit, um dieses Sicherheitsupdate zu vervollständigen.

Erneute Passwort Phishing Attacke, diesmal noch perfider

September 18th, 2012 | Roberto Mazzoni | Keine Kommentare |

→ [for english see below]

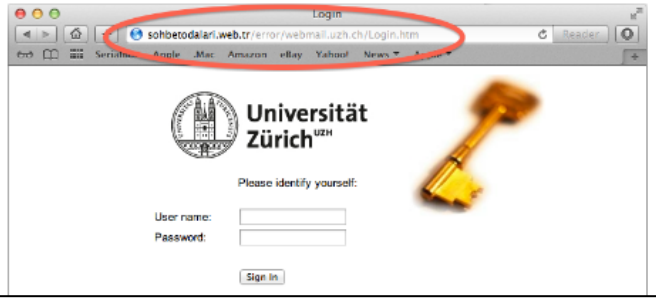
Heute haben wieder sehr viele Benutzerinnen und Benutzer der UZH eine E-Mail erhalten, die nur darauf ausgerichtet ist, das Passwort der Benutzerinnen abzufragen. Der gefälschte Absender war **Webmail – University of Zurich <all@uzh.ch>** und der Betreff "**You Have One New Security Message.**" Der Inhalt sah wie folgt aus:

```
Dear Valued Client,
 Access To Your Web mail Account Is about to
 Expire We advise you update your web mail account
 to avoid Email Suspension

Please follow the link below to update your Web mail access.
 https://webmail.uzh.ch//webmail/ .
 ©2012 webmail.uzh.ch Webmail
```

Auch diese E-Mail stammt wie andere Attacken derselben Art, durchaus mit korrektem Text in deutsch, nicht von der UZH. Ihre E-Mail Accounts laufen NIE separat ab, genau so wie die Informatikdienste Sie auch niemals auffordern, uns eine E-Mail mit Ihrem Passwort zu schicken.

Wenn Sie auf den in der E-Mail erwähnten Link klicken, gelangen Sie auf ein Login, das unserem Webmail Login täuschend ähnlich sind. Sie erkennen aber die Fälschung daran, dass die Adresse im Browser nicht stimmt!



Beispiele II

Steuerverwaltung und Postfinance als Opfer von Phishing-Mails

Montag, 4. Juni 2012, 9:38 Uhr, Aktualisiert 17:31 Uhr

Betrügerische Mails sind in aller Regel leicht zu erkennen: fehlerhaftes Deutsch und absurde Gewinnversprechungen. Doch von dem, was viele Schweizer heute in ihrem virtuellen Briefkasten fanden, haben sich einige doch in die Irre führen lassen. Opfer sind zum einen die Eidgenössische Steuerverwaltung, zum anderen Postfinance.

Eidgenössische Steuerverwaltung ESTV
Administration fédérale des contributions AFC
Amministrazione federale delle contribuzioni AFC
Administraziun federala da taglia AFT

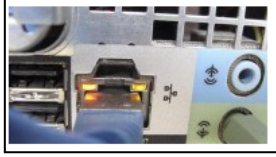
Datum	04 Juni 2012
Unsere Referenz	B/22635/12
Ihr Zeichen	09R/211/12

HINWEIS DER STEUERERKLÄRUNG FÜR DAS JAHR 2011

Phishing

Betrüger nutzen Email und Logo der Steuerverwaltung als Absender

Publiziert: 04.06.2012 — 0 Kommentare · Drucken · E-Mail



BERN - BE - Die Betrüger, die mittels Emails an Geld-, Kreditkarten- oder Kontoinformationen kommen wollen, werden immer unverfrorener. Seit Montag sind Emails im Umlauf, welche scheinbar von der Eidg. Steuerverwaltung stammen und eine Steuerrückerstattung versprechen.

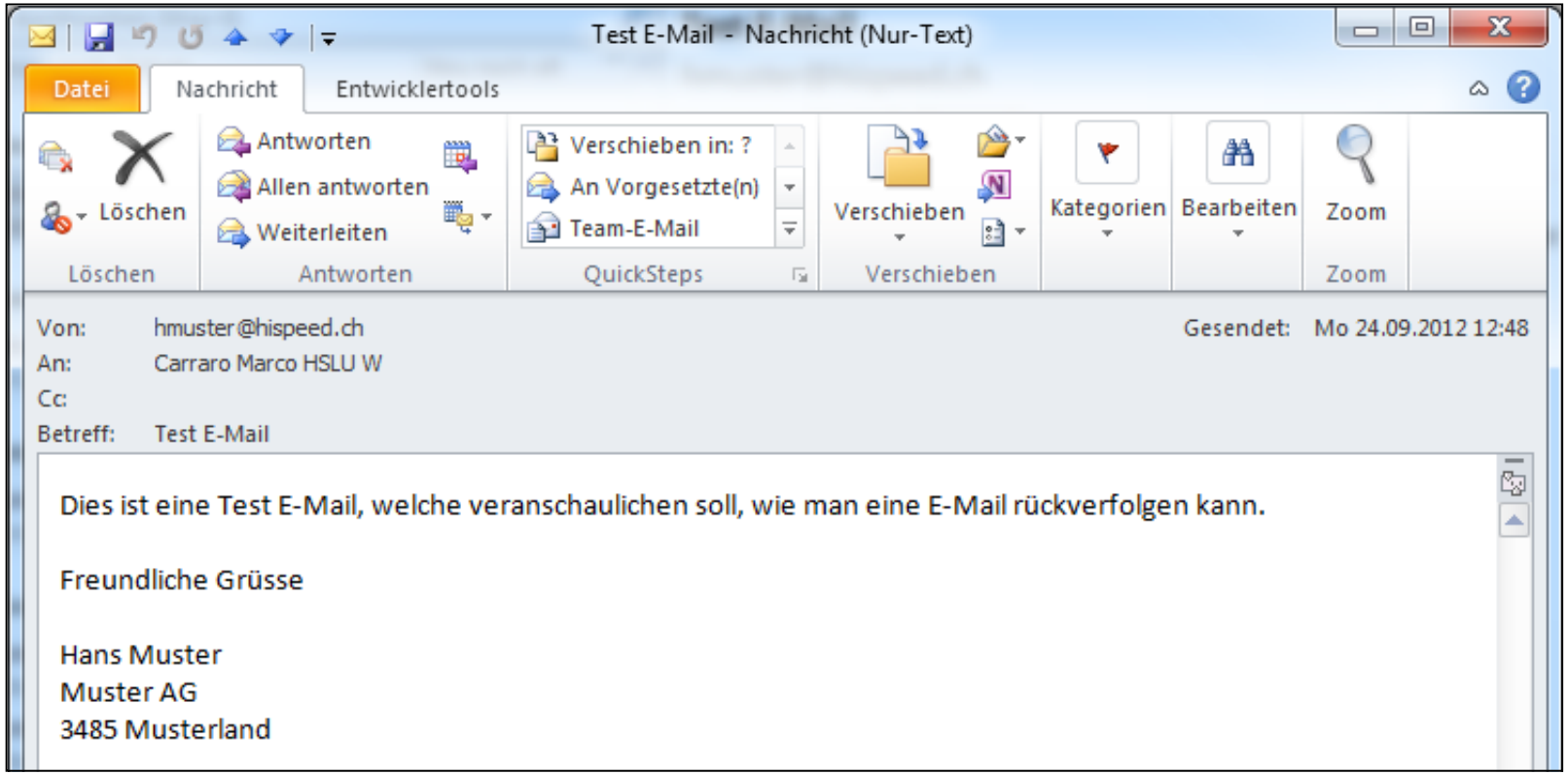
ricardo.ch

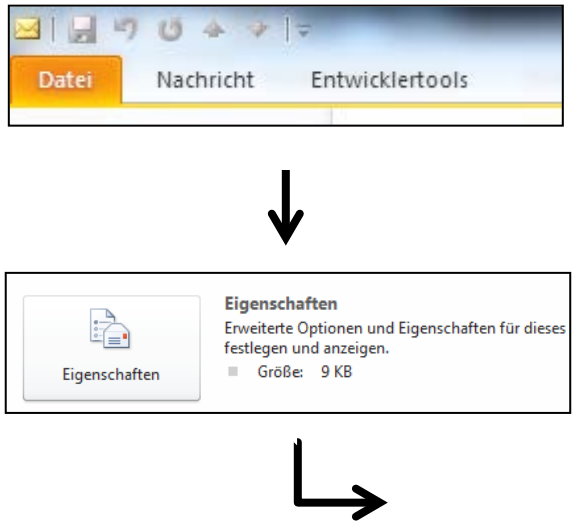
Gefälschte E-Mails im Umlauf: Niemals Benutzername und Passwort angeben!

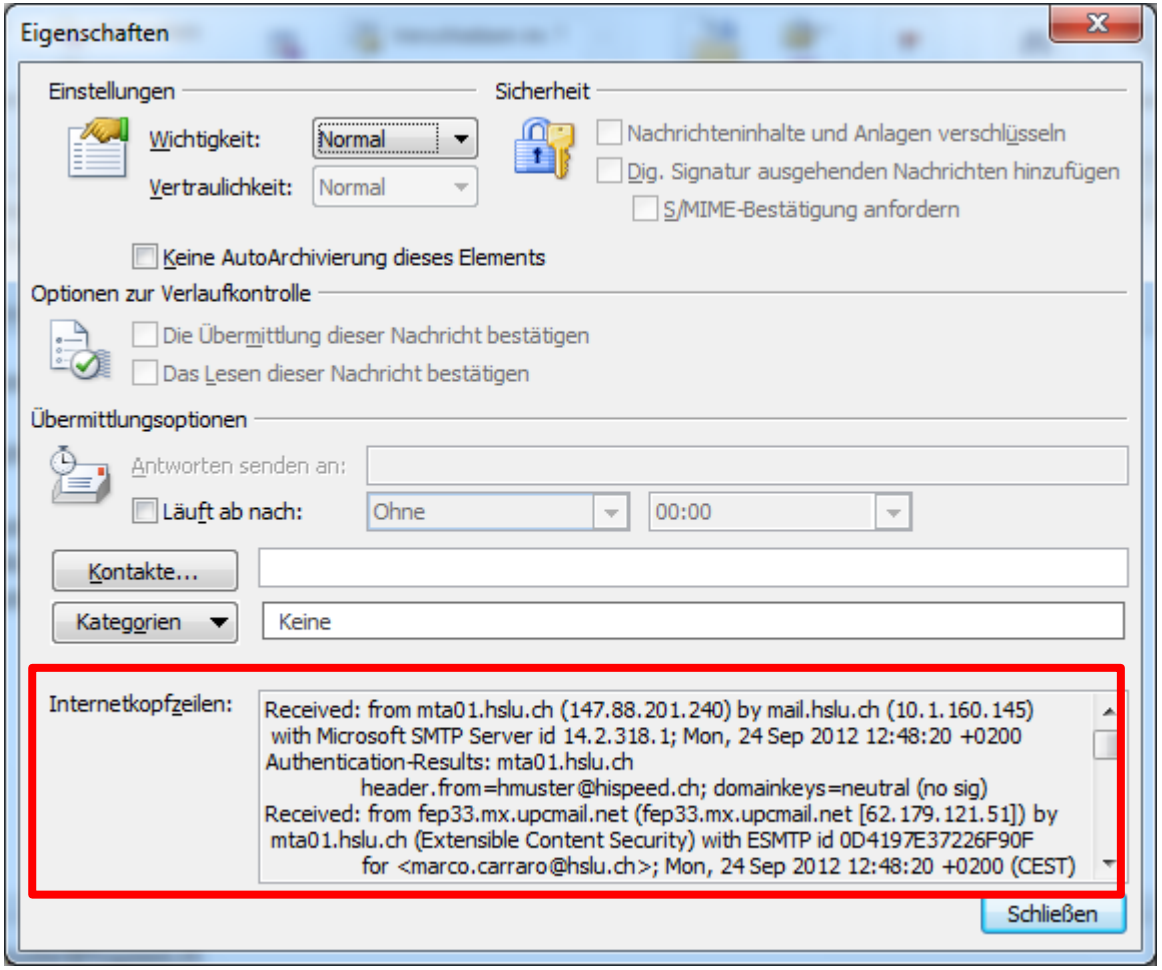
Liebes ricardo.ch-Mitglied

Leider sind neue Phishing-Mails im Umlauf. Mit Phishing-Mails möchten Betrüger an Ihr
gelangen. Falls Sie ein angeblich von ricardo.ch stammendes E-Mail in schlechtem Deu
Sie auffordert, Ihr Passwort oder andere Daten bekannt zu geben, dann seien Sie bitt
es sofort oder falls Sie nicht sicher sind, leiten Sie es an unseren Kundendienst weiter
Phishing-Mails lautet wie folgt:

Rückverfolgung einer E-Mail







Unter Windows 7: Menüeintrag Datei / Eigenschaften

Internetkopfzeilen

Received: from **mta01.hslu.ch** (147.88.201.240) by **mail.hslu.ch** (10.1.160.145)

Received: from **fep33.mx.upcmail.net** (fep33.mx.upcmail.net [62.179.121.51]) by **mta01.hslu.ch**

Received: from **edge03.upcmail.net** ([192.168.13.238]) by **fep33.mx.upcmail.net**
Received: from **viefep25** ([192.168.14.250]) by **edge03.upcmail.net**

id 2yoD1k01G5PiXJQ03yoDQC; Mon, 24 Sep 2012 12:48:13 +0200

X-SourceIP: 192.168.14.250

Message-ID: <20120924124813.16XVH.15162.root@viefep25>

Date: Mon, 24 Sep 2012 12:48:13 +0200

From: <hmuster@hispeed.ch>

To: <marco.carraro@hslu.ch>

Subject: Test E-Mail

X-Originating-IP: from **147.88.200.144** by www.upcmail.net; Mon, 24 Sep 2012 12:48:13 +0200

Rückverfolgung einer IP-Adresse

- IP-Adresse dienen der eindeutigen und einheitlichen Identifikation einzelner Geräte im Netzwerk/Internet.

- Für die Vergabe von IP-Adressen sind in den verschiedenen Regionen der Welt unterschiedliche Organisationen verantwortlich.
  - IANA / RIRs / LIRs (=ISPs)

- Die für Europa zuständige RIR ist RIPE NCC (Résaux IP Européens Network Coordination Centre www.ripe.net)

Resultat Whois-Abfrage auf www.ripe.net

- Suchanfrage 147.88.200.144

This is the RIPE Database search service.

The objects are in RPSL format.

The RIPE Database is subject to Terms and Conditions.

See http://www.ripe.net/db/support/db-terms-conditions.pdf

```
inetnum:        147.88.0.0 - 147.88.255.255
netname:        ZTL
descr:          Hochschule f►r Technik + Architektur Luzern
descr:          Horw, Switzerland
country:        CH
admin-c:        AW1923-RIPE
tech-c:         PW16-RIPE
status:         ASSIGNED PI
mnt-by:         SWITCH-MNT
mnt-irt:        IRT-SWITCH-CERT
source:         RIPE #Filtered

person:         Armin Wehinger
address:        Hochschule Luzern
address:        Fachhochschule Zentralschweiz
address:        Technikumstrasse 21
address:        CH-6048 Horw
address:        Switzerland
phone:          +41 41 349 3840
nic-hdl:        AW1923-RIPE
mnt-by:         SWITCH-MNT
source:         RIPE #Filtered
```

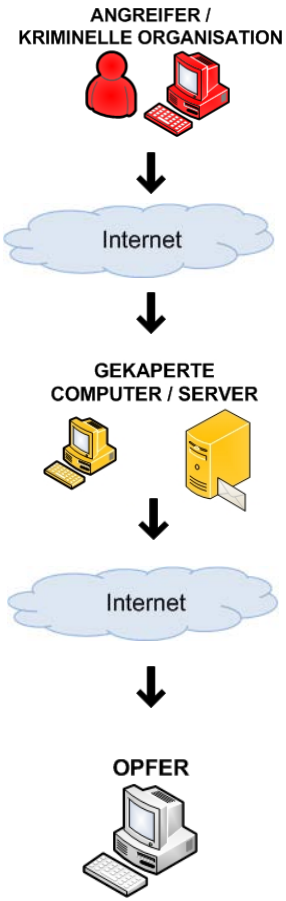
1. Bereich – Gefälschte Webseite

- Bereitstellen eines Webservers mit einer gefälschten Webseite
- Übernehmen eines Webservers für die gefälschte Webseite

⇒ IP-Adresse des Webservers kann zurückverfolgt werden!

- Problematik?

2. Bereich – Versenden der Phishing-Mails

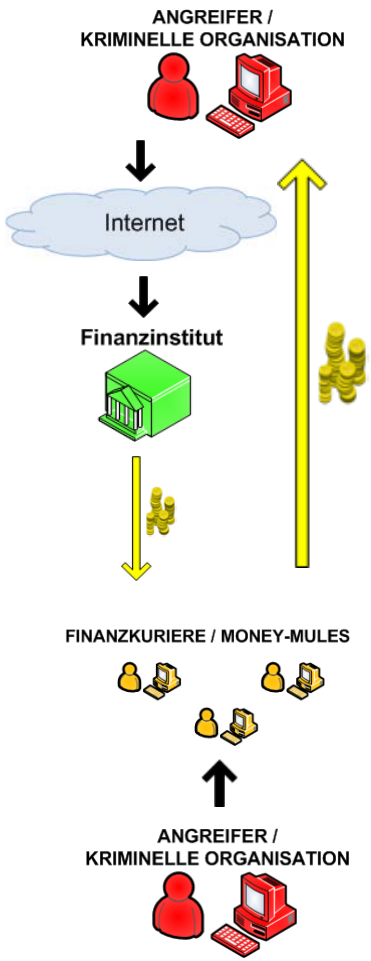


- Direktes Versenden der Phishing-Mails
- Übernehmen eines Computers/Servers für den Massenversand der Phishing-Mails

⇒ E-Mail kann anhand der E-Mail-Header (Internetkopfzeilen) zurückverfolgt werden.

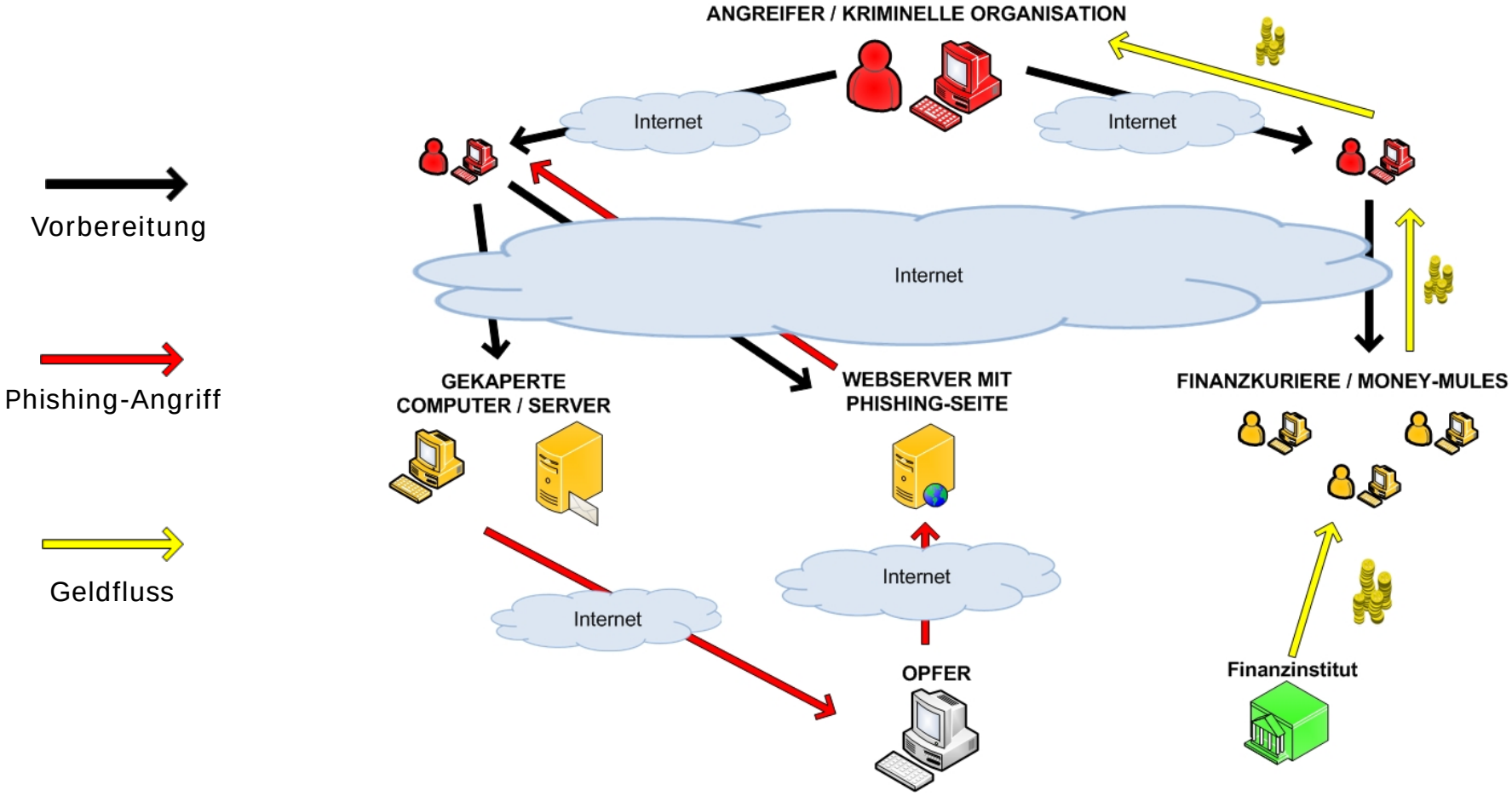
- Probleme?

3. Bereich - Geldfluss



- Angreifer muss sich beim Finanzdienstleister einloggen => IP-Adresse?
- Angreifer überweist sich das Geld direkt
- Angreifer überweist das Geld an Finanzkuriere
- Wie wurden Finanzkuriere rekrutiert? E-Mail-Analyse? Telefon?

Phishing-Ablauf



Schutzmöglichkeiten

- Prävention durch richtiges Surfverhalten
  - Nie einen Link verwenden, der per E-Mail zugeschickt wurde, um sich bei einem Online-Dienstleister anzumelden.
  - Keine Felder in E-Mail-Formularen von Online-Dienstleistern ausfüllen.
  - Online-Dienstleister verschicken nie solche E-Mails.
  - Die sichere Navigation zur Login-Seite eines Online-Dienstleisters erfolgt über eine manuelle Eingabe der Adresse in der Adresszeile des Browsers.

Merkmale einer korrekten Verbindung

- Der Browser zeigt beim Aufbau der SSL-Verbindung **keine Fehlermeldung**.
- Am Anfang der Adresszeile steht **https//:**
- Am Ende der Adresszeile (Internet Explorer) oder in der Fusszeile (Firefox) ist ein **Schloss** sichtbar. (ab Firefox 4 fehlt das Schlosssymbol!)
- Die **Adresszeile** wird abhängig vom verwendeten Browser und Zertifikatstyp **grün** oder **weiss** hinterlegt
- Der Domänenteil der Adresse zum kontaktierten Finanzinstitut ist **korrekt**.
- Für weitere Informationen www.ebankingabersicher.ch

Fragen