

# Phishing Frühwarnsystem

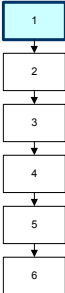
Walter Sprenger  
walter.sprenger@csnc.ch

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch



1. Idee Frühwarnsystem
2. Funktionsweise
3. Demo und Betrieb
4. Kunden-Nutzen
5. Weitere Ideen/Pläne
6. Fragen/Diskussion



## Idee Frühwarnsystem

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch

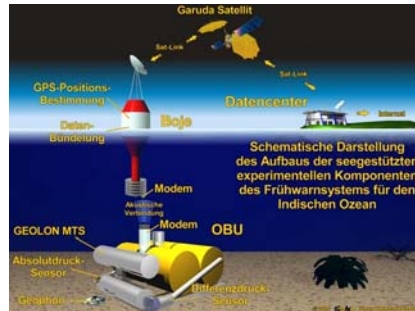
## Phishing noch aktuell?



- Phishing: Der Kampf geht weiter (heise vom 8.3.2006)
  - Phishing Welle hat nicht abgeschwächt
  - Professionellere Phishing-Mails (besseres Deutsch, bessere Geschichten, lokales Wissen enthalten)
  - Auch kleinere Institute betroffen
  - Gezielteres Phishing (Spear-Phishing)
  - Britischer Verlust 2005 wird auf 33.8 Millionen Euro beziffert
  - Technisch keine grossen Fortschritte im Phishing
  - Schwierige Situation für Banken: Bank muss merken, wenn Angriffe erfolgen und soweit möglich verhindern

- 1
- 2
- 3
- 4
- 5
- 6

- Tsunami Early Warning System (TEWS)
  - Tsunamis lassen sich nicht verhindern
  - Vorwarnzeit: Ca. 20 Minuten
  - Eine frühe Warnung kann viele Menschenleben retten
  
- Idee von Compass: Wieso nicht ein Frühwarnsystem bei Phishing-Attacken?



<http://www.weltderphysik.de/de/3474.php>

- 1
- 2
- 3
- 4
- 5
- 6

- Technologie-Transfer HSR <-> Compass Security
  - Compass schreibt jedes Jahr 4 Studien und 2 Diplomarbeiten aus und betreut diese als Lehrbeauftragte
  - Jeweils zwei Studenten des Informatik-Abschlussjahres führen die Arbeit durch
  
- Phishing Warning System
  - Wintersemester 2005/2006
    - Roger Britt
    - Marc Bechtiger



- 1
- 2
- 3
- 4
- 5
- 6

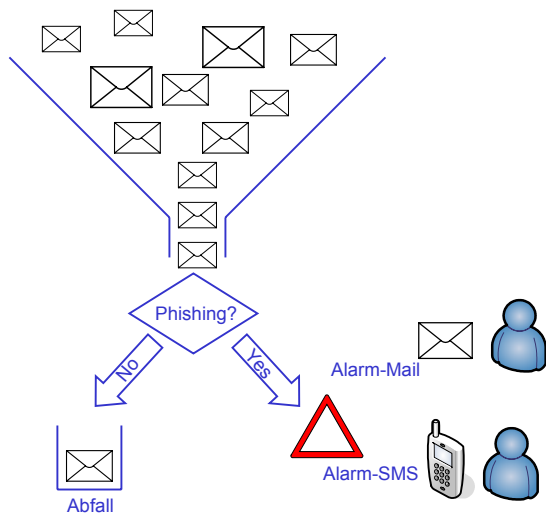
# Funktionsweise

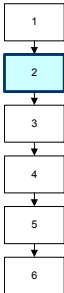
GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch

- 1
- 2
- 3
- 4
- 5
- 6

# Funktionsweise





### ■ Funktionsweise Phishing Frühwarnsystem

- Das System bezieht SPAM- und Phishing-Mails von unbenutzten Mail-Accounts (Mail-Honeypots)
- Anhand von Filterregeln werden die Mails auf Phishing Patterns hin geprüft
- Falls ein Mail die Phishing-Regeln erfüllt, wird dieses plausibilisiert und eine Alarmmeldung abgesetzt

### ■ Vorarbeiten

- Erfassen von Mail-Honeypots und Publikation der Adressen auf Webseiten/Internet-Foren/Mailinglisten
- Konfigurieren von Filterkriterien pro Firma und pro Applikation
- Analyse von neuartigen Phishing-Attacken



### ■ Honeypot Emails

- Adresse wird nicht benutzt -> jegliche Mails sind somit SPAM
- Adresse wird bei Kunden nirgends registriert
- Adressen, welche aufgrund des hohen Anteils an SPAM nicht mehr benutzt werden können

### ■ Phishing Mails erkennen

- Kunden oder Applikationsname kommt im Betreff oder Text vor
- Permutationen des Kunden/Applikationsnamens
- Absender-Adresse = Kundenname
- URL der Applikation
- Cross-Site Scripting auf Webserver/Applikation des Kunden

- 1
- 2
- 3
- 4
- 5
- 6

## Demo und Betrieb

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch

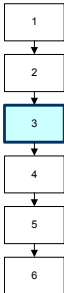
## Demo Phishing Frühwarnsystem

- 1
- 2
- 3
- 4
- 5
- 6

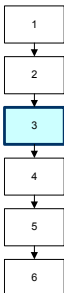
### ■ Demo Phishing Frühwarnsystem

The screenshot displays the 'PWS - Phishing Warning System' interface. On the left, there is a tree view for 'PWS-Verwaltung' with categories like 'Verwaltung', 'Compass Security', 'Filebox', and 'eBay'. The main window shows a list of 'Phishing-Mails' with columns for 'Empfänger', 'Betreff', and 'Datum'. The list contains multiple entries for various email addresses and subjects related to eBay and student portals.

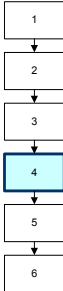
Empfänger	Betreff	Datum
erich.ruf@csnc.ch	***SPAM-CSNC*** Mir EBAY geld...	16.04.2006 06:13
erich.ruf@csnc.ch	***SPAM-CSNC*** Mir EBAY geld...	16.04.2006 06:13
erich.ruf@csnc.ch	***SPAM-CSNC*** Mir EBAY geld...	16.04.2006 06:13
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	16.04.2006 06:22
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	16.04.2006 06:22
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	16.04.2006 06:22
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie r...	18.04.2006 08:27
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie r...	18.04.2006 08:27
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie r...	18.04.2006 08:27
erich.ruf@csnc.ch	***SPAM-CSNC*** Geld verdiene...	18.04.2006 08:31
erich.ruf@csnc.ch	***SPAM-CSNC*** Geld verdiene...	18.04.2006 08:31
erich.ruf@csnc.ch	***SPAM-CSNC*** Geld verdiene...	18.04.2006 08:31
info@studentportal.ch	***SPAM*** So finden Sie bei EBA...	20.04.2006 12:54
info@studentportal.ch	***SPAM*** So finden Sie bei EBA...	20.04.2006 12:54
erich.ruf@csnc.ch	***SPAM-CSNC*** So finden Sie b...	20.04.2006 06:54
erich.ruf@csnc.ch	***SPAM-CSNC*** So finden Sie b...	20.04.2006 06:54
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	20.04.2006 07:15
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	20.04.2006 07:15
info@studentportal.ch	***SPAM*** Selbststaendig werde...	22.04.2006 11:01
info@studentportal.ch	***SPAM*** Selbststaendig werde...	22.04.2006 11:01
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	24.04.2006 08:07
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** So finden Sie b...	24.04.2006 08:07
info@studentportal.ch	***SPAM*** Mir EBAY Geld sparen	25.04.2006 12:16
info@studentportal.ch	***SPAM*** Mir EBAY Geld sparen	25.04.2006 12:16
christoph.schmidrig@csnc.ch	***SPAM-CSNC*** Geld verdiene...	29.04.2006 06:42



- Betrieb des Systems bedeutet
  - 7 x 24 Stunden Überwachung
  - Validierung/Plausibilisierung der Alarmmeldungen
  - Kunden alarmieren und unterstützen (CIRT)
  
  - Trends der Phisher aufspüren
  - Aktualisierung der Filter-Regeln
  - System weiterentwickeln
  
- Voraussetzungen für Betrieb
  - Mehrere Firmen können für das Frühwarnsystem gewonnen werden. Kein Betrieb möglich für wenige Kunden.



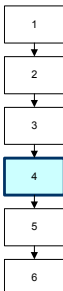
- Einschränkungen
  - Phishing Mail erreicht Honeypot-Adresse nicht, z.B. Bei gezielten Phishing Attacken (Spear-Phishing)
  - Filter-Regeln können umgangen werden (z.B. Mit Bildern in eMails anstatt Text)
  - Benutzer können trotz Warnhinweisen Opfer werden
  - Anzahl SPAM Mails können nicht in Echtzeit verarbeitet werden
  - Keine Möglichkeit SPAM E-Mails beim SMTP Gateway des Kunden an das PWS zu senden (falls dies gewünscht)



## Kunden-Nutzen

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch

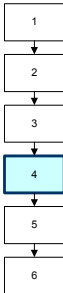


### ■ Kunden-Nutzen

- Früherkennung von Phishing Angriffen
- Reduktion Reaktionszeit der betroffenen Institute (Warnmeldungen, Analyse des Angriffes)
- Voranalyse für CIRT des Kunden erstellen

### ■ Kosteneinsparungen

- Weniger Phishing-Opfer dank rascher Reaktion
- Attacke kann möglicherweise ganz verhindert werden (keine Korrespondenz zu Applikations-Kunden notwendig)
- Erstellen von Awareness-Dokumenten und Durchführen von Awareness-Aktionen durch Compass



■ KnowHow Transfer

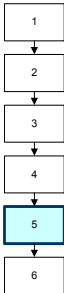
- Informationen über neue Phishing-Varianten
- Anpassung der Sofort-Massnahmen an neue Attacken
- Erfahrungsaustausch PWS Kunden (lessons learned)
- Analyse von Trojanern/Keyloggern



## Weitere Ideen/Pläne

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch



- Integration existierende Phishing Portale
  - Regelmässige Prüfung der Kunden URL gegenüber vorhandenen Anti-Phishing Datenbanken (Microsoft mit IE7.0 oder opdb.berlios.de)
- Phishing-Awareness für Endkunden
  - Regelmässige Awareness-Beiträge über Phishing in Medien (Zeitschriften, Fernsehen, Radio)
  - Informationsportal über Anti-Phishing (Endkunden finden alles Wissenswerte an einem Ort)
- Radio-Alarmierung
  - Z.B. Wie die Staumeldungen und Radarwarnungen: "Vorsicht: Phishing Attacke auf Online Banking XY"



## Fragen/Diskussion/Interesse

GLÄRNISCHSTRASSE 7  
POSTFACH 1671  
CH-8640 RAPPERSWIL

Tel.+41 55-214 41 60  
Fax+41 55-214 41 61  
team@csnc.ch www.csnc.ch

- 1
- 2
- 3
- 4
- 5
- 6

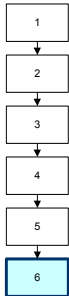
### ■ Interesse vorhanden?

- Wo sehen Sie den Nutzen für Ihre Firma?
- Würde Ihre Firma diese Dienstleistung bestellen?
- Haben Sie weitere Ideen oder andere Bedürfnisse?

- 1
- 2
- 3
- 4
- 5
- 6

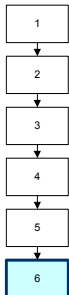
### ■ Weiteres Vorgehen

- Bedürfnisabklärung bei Kunden
- Vorbereiten produktiver Betrieb PWS
- Pilotphase I
- Produktion ab 1.1.2007



### ■ Referenzen

- Studienarbeit HSR -> Phishing Warning System  
<http://www.pwsys.ch/>
- Heise Security -> Phishing: Der Kampf geht weiter  
<http://www.heise.de/security/result.xhtml?url=/security/news/meldung/70547&words=Phishing>
- Welt der Physik -> Tsunami Early Warning System)  
<http://www.weltderphysik.de/de/3474.php>
- Castle Cops -> Fried Phish  
<http://castlecops.com/pirt>
- Open Phishing Group  
Browser Anti-Phishing Plugin  
<http://opdb.berlios.de/>
- Microsoft Internet Explorer 7.0  
Anti-Phishing
- Phishing Threats  
<http://www.cgisecurity.com/phishing/>



### ■ Abkürzungen

- CIRT: Computer Incident Response Team
- HSR: Hochschule für Technik in Rapperswil
- PWS: Phishing Warning Systems
- TEWS: Tsunami Early Warning System