



openHPI-Kurs „Digitale Identitäten“ Identitätsdiebstähle – Social Engineering Angriffe

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Was ist Social Engineering?

Ausnutzung menschlicher Schwächen, um bestimmte Reaktionen zu provozieren

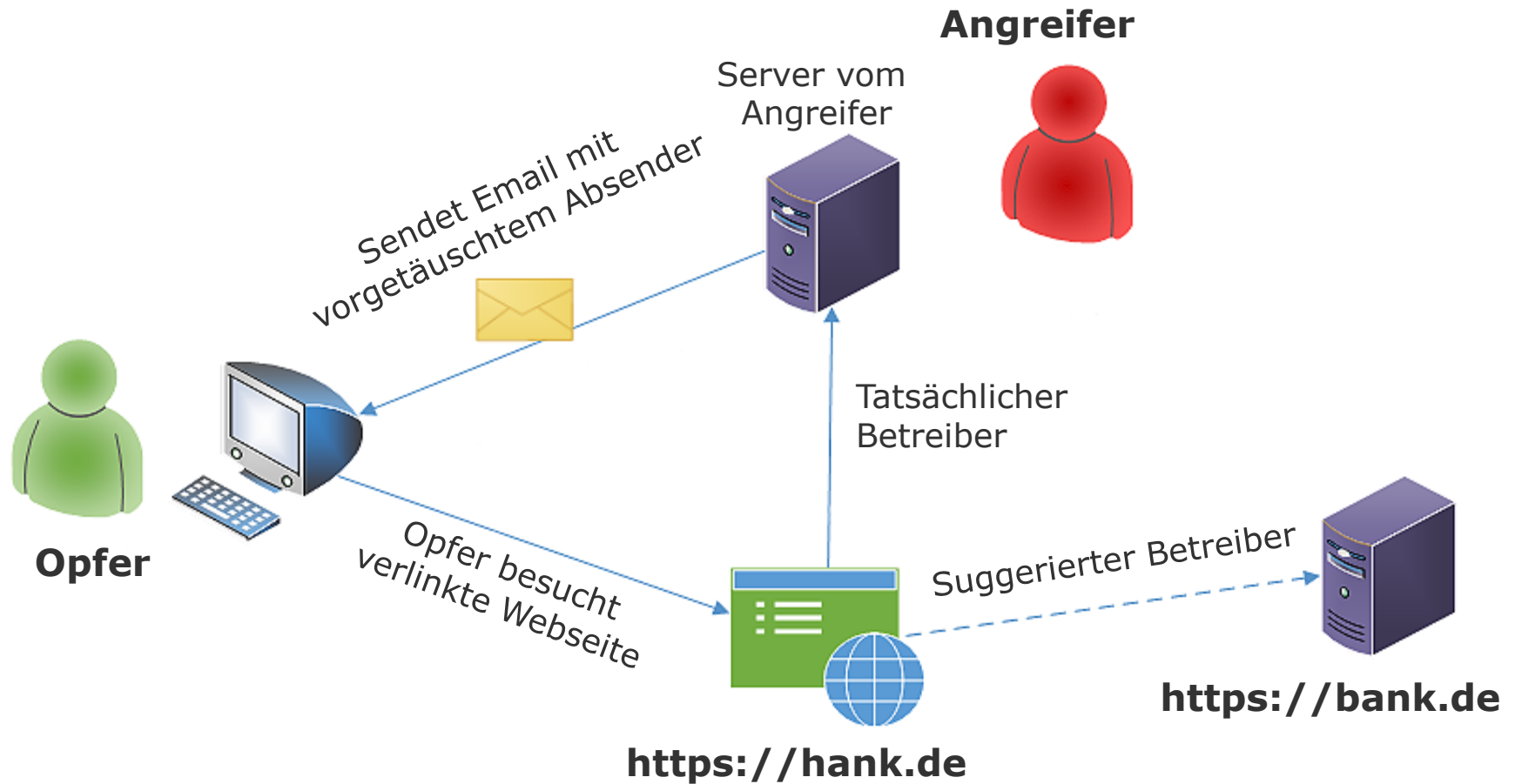
- Unter falscher (z.B. gestohlener) Identität nutzt Angreifer menschliche Schwächen (Vertrauen, Angst, Respekt, Hilfsbereitschaft) eines Opfers aus
- Opfer wird dazu gebracht, etwas zu tun, was es unter normalen Umständen nicht tun würde, z.B.
 - Herausgabe von Informationen, wie z.B. Identitätsdaten
 - Zugang gewähren zu einem geschützten System / Ort
 - ...
- Häufigste Methode im Internet: **Phishing**

Phishing (1/2)

Angriffstechnik zur betrügerischen Erlangung von sensiblen Informationen

- Typisches Vorgehen: Versand betrügerischer Emails
 - Versand mit vertrauenswürdig wirkender Absenderadresse, z.B. Bank, Unternehmen, Behörde, ...
 - Absenderadresse (sind leicht zu fälschen – Spoofing) wird ausgewählt nach der Information, die erschwindelt werden soll
 - Ausnutzen des erlangten Vertrauens, um erwünschte Reaktion zu initiieren, z.B.
 - Herausgabe von Daten
 - Klick auf Link einer gefährlichen Website
 - Installation von Schadsoftware
 - ...

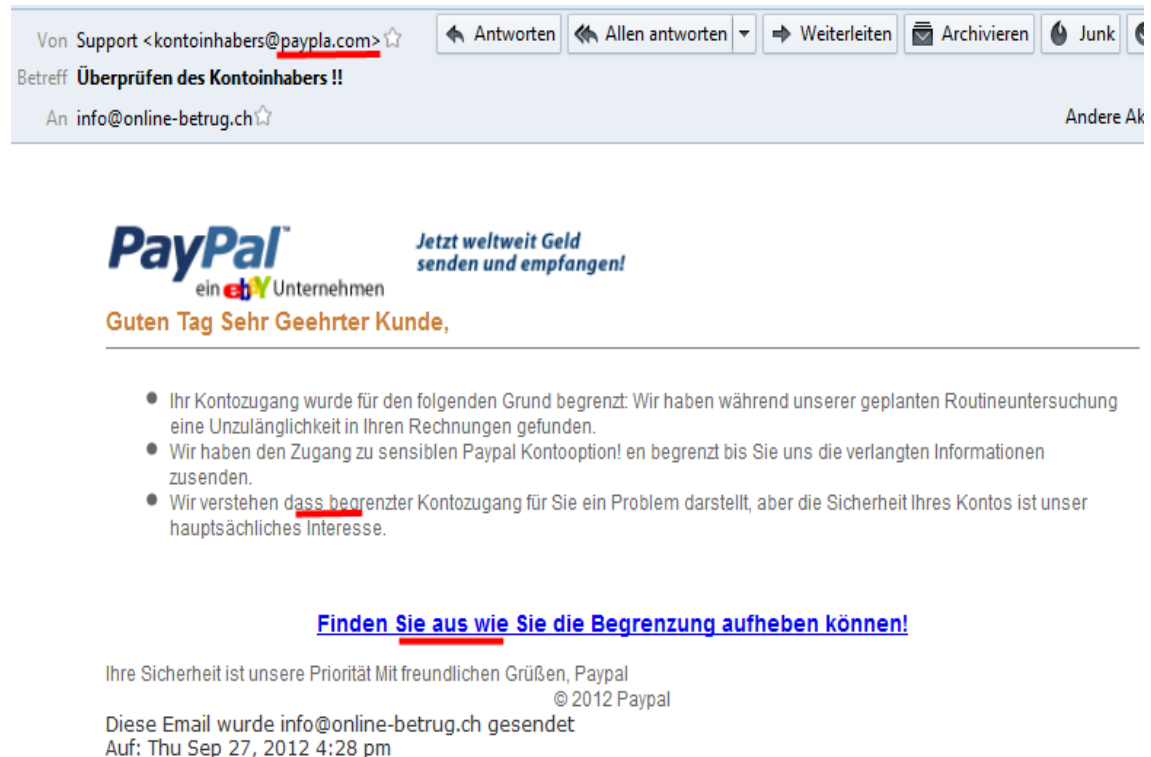
Phishing (2/2)



Phishing - Beispiel (1/2)

Ziel: Empfänger veranlassen, seine Kontodetails preiszugeben, um Konto zurückzusetzen

- Versand einer Email mit vorgetäuschem Absender
- Nachricht stammt angeblich vom Bankinstitut (Paypal) und hat entsprechend ähnliche Emailadresse (paypla.com)
- Phishing oft erkennbar an den sprachlichen Fehlern oder fehlender persönlicher Ansprache („Guten Tag Sehr Geehrter Kunde“)



Phishing - Beispiel (2/2)

- Email leitet weiter auf Webseite mit Eingabeaufforderung der Kontodaten
- Opfer wird aufgefordert, hier sämtliche Details über sein Konto preiszugeben



Restore Your Account

Please fill in all the details that are required to complete this verification process in order to restore your account.

NOTE: All fields are required

Please fill in all the fields.

Email Address:

PayPal Password:

Full Name:

Credit/Debit Card Number

Card Expiration Date

Quelle: <http://labs.m86security.com/>

Breit gestreute Phishing-Angriffe

Herkömmliche Phishing-Angriffe sind relativ **leicht zu erkennen**

- Deshalb werden Phishing-Emails sehr weit gestreut und ungezielt verbreitet – bei vielen Millionen potenziellen Opfern reicht auch eine sehr niedrige Konversionsrate aus, um nennenswerten Erfolg zu erzielen

Probleme für Angreifer

- Internetnutzer werden durch Medien gut gegen gängige Phishing-Maschen sensibilisiert
- Phishing-Mails erreichen viele Empfänger, auf die der Inhalt gar nicht zutrifft und sind daher leicht durchschaubar, z.B.
 - Absender ist Bank, bei der das Opfer gar kein Konto hat

Personalisiertes Phishing (1/2)

Angreifer gehen mehr und mehr zu personalisiertem Phishing, dem **Spear Phishing** über, da sie mit „normalem“ Phishing ihre Ziele nicht mehr erreichen

- Erlangung von sensiblen (Identitäts-)Informationen

In einer Vorphase werden sehr detaillierte, oft private Informationen über das Opfer gesammelt

- hilfreich für vorgetäuschte Vertrauenswürdigkeit, z.B. Nutzung der Identität einer Person, die das Opfer kennt und der es vertraut

Dann wird Phishing-Mail von vorgetäushtem Absender gesendet. Opfer denkt, dass Email von vorgetäushtem Absender kommt, weil Nachricht Informationen enthält, die nur dieser Absender kennt ...

- Erfolgsaussichten bei dieser Masche sind sehr hoch, aber auch Aufwand für Angreifer ist deutlich höher

Personalisiertes Phishing (2/2)

- Viele Angriffe im Internet basieren auf vorangegangenen personalisierten Phishing-Angriffen
- Personalisiertes Phishing ist deshalb sehr gefährlich und richtet sich gezielt an
 - hochrangige Zielpersonen, z.B. Firmenchefs, Politiker, hochrangige Beamte, Prominente, ...
 - sensible Ziele: Militär, Unternehmen, Politik, Finanzindustrie...
 - professionelle Angreifer, z.B. Staaten, Aktivisten, organisierte Kriminalität

Weitere Techniken des Social Engineering

■ Köderung

- Ausnutzung der Neugier/Gier von Opfern
- Verteilung von Geschenken mit böartigen Nebenfunktionen
 - z.B. USB-Sticks mit Schadsoftware, Apps, ...

■ Pretexting

- vorgaukeln von Geschichten/Lügen, die Opfer zur Herausgabe von Informationen oder zu bestimmten Reaktionen bewegen
- Vortrag einer Geschichte unter Vorspiegelung einer Autorität oder eines Eingeweihten

■ Reverse Social Engineering

- Angreifer kontaktiert hilfesuchendes Opfer, um Vertrauen zu erschleichen

- **Sensibilisierung** von Nutzern
 - durch Aufklärung, z.B. durch unseren openHPI-Kurs
 - auch durch gelegentliche Tests mit Phishing-Emails
- **Überprüfung der Identität** des angeblichen Gegenübers
 - bei Zweifel besser misstrauen und ausweisen lassen
- Verwendung **sicherer Authentifizierung**, z.B.
 - über vertrauenswürdige Zertifikate
- **Verantwortungsvoller Umgang** mit persönlichen Informationen
 - Was wird nach außen gegeben? Was wird ins Netz gestellt?

- Gründliche Überprüfung der Absenderadresse - nicht des Anzeigenamens im Email-Programm
- Bei Anforderung von sensiblen Informationen Anfrage bei Dienstanbieter bestätigen lassen
- Beim Folgen eines Links unbedingt die Adresse in der Browser-Adresszeile kontrollieren
 - gängige Browser warnen oftmals schon vor Phishing-Webseiten

Angriffstaktik

- Angreifer manipulieren, nutzen menschliche Schwächen aus und bauen Vertrauen auf, um bei den Opfern bestimmte Verhaltensweisen zu initiieren, z.B.
 - Herausgabe von sensiblen Informationen oder Installation von Schadsoftware
- Häufige Vorgehensweisen: Versand von betrügerischen Emails oder hinterhältige Anrufe

Sonderform: **Spear Phishing** (personalisiertes Phishing)

- Angreifer fokussiert sich auf eine bestimmte Person und sammelt detaillierte Informationen über sein Opfer
- Aufwändiger, aber effektiver als „normales“ Phishing