Awareness

Torsten Casselt

casselt@luis.uni-hannover.de

29. Januar 2019

„Echte Welt“

Quelle: http://two-color.tumblr.com/post/40887162840/alone-in-the-dark-by-luís-c

„Digitale Welt“

Quelle: https://www.trustwave.com/Resources/SpiderLabs-Blog/Angler-Takes-Malvertising-to-New-Heights/

- Gefährlich?

„Digitale Welt“

Quelle: https://www.trustwave.com/Resources/SpiderLabs-Blog/Angler-Takes-Malvertising-to-New-Heights/

- Gefährlich?
- Infektion durch Aufrufen der Webseite der New York Times (2016)

„Digitale Welt“

Quelle: https://www.trustwave.com/Resources/SpiderLabs-Blog/Angler-Takes-Malvertising-to-New-Heights/

- Gefährlich?
- Infektion durch Aufrufen der Webseite der New York Times (2016)
- $\Rightarrow$ „Gefahr“ im Internet ist nicht offensichtlich
- $\Rightarrow$ Angst vor der Gefahr nicht natürlich vorhanden

Was ist mit Awareness gemeint?

- Wachsamkeit bei der Benutzung von technischen Systemen
- Wichtige Dinge konzentriert erledigen
- Hinterfragen der Schritte, die man gerade unternimmt
- Bei Unsicherheit lieber warten, nachfragen, z.B. LUIS
- Dort ansetzen, wo technische Maßnahmen nicht ausreichen
- Devise: Lieber zu misstrauisch als leicht anfällig
- $\Rightarrow$ Gefühl für Gefahren in der IT lässt sich entwickeln

Aufbau und Ziel des Vortrags

- Erfahrungsbericht aus Awareness-Maßnahmen bei Endnutzern
- Welche Sicherheitsprobleme sind in diesem Kontext relevant?
- Empfehlungen von Herangehensweisen, um Awareness bei anderen zu verbessern
- Ziel: Sie wenden diese Erkenntnisse in den Einrichtungen an!

Welche Gefahren betreffen meine Daten?

- Bösartige Software
- Social Engineering
- (Spear) Phishing
- Diebstahl

Malware

- Altbekannte Schadsoftware, löscht/verändert Daten
- Folge: Datenverlust
- Gegenmaßnahme: Virenschutz
- Problem: Antivirenhersteller reagieren, Heuristiken reichen nicht

Spyware

- Spionagesoftware, „liest“ Daten mit
- Folge: Datenleck
- Gegenmaßnahme: Virenschutz
- Problem wie bei Malware

Ransomware

- Verschlüsselungssoftware, verschlüsselt Daten
- Folge: Daten sind nicht zugreifbar
- Gegenmaßnahme: Virenschutz, Backup
- Problem wieder wie bei Malware, Definition von Backup häufig unklar

Backup

- Was ist das genau?

Backup

- Was ist das genau?
- $\Rightarrow$ Kopie der Daten auf externem Medium an anderem Standort
- Häufiger Fehler: Backup bleibt angeschlossen
- Auch Cloud-Dienste schützen nicht!

Weitere Gegenmaßnahmen

- Verbreitung bösartiger Software häufig durch Fehlverhalten
- $\Rightarrow$ Änderung des Fehlverhaltens löst das Problem am besten
- Ansätze: Anhänge, Downloads, unplausible Schritte
- Bei Unsicherheit nachfragen, am besten über weiteres Medium

Social Engineering

- Einfaches Fragen führt erstaunlich häufig zur gewünschten Information
- $\Rightarrow$ „Gesundes“ Misstrauen Anrufern gegenüber
- Im Zweifel zweite Meinung einholen, persönliches Gespräch suchen, nicht unter Druck setzen lassen
- Informationen sind auch Interna, nicht nur Passwörter

Social Engineering: Beispiel

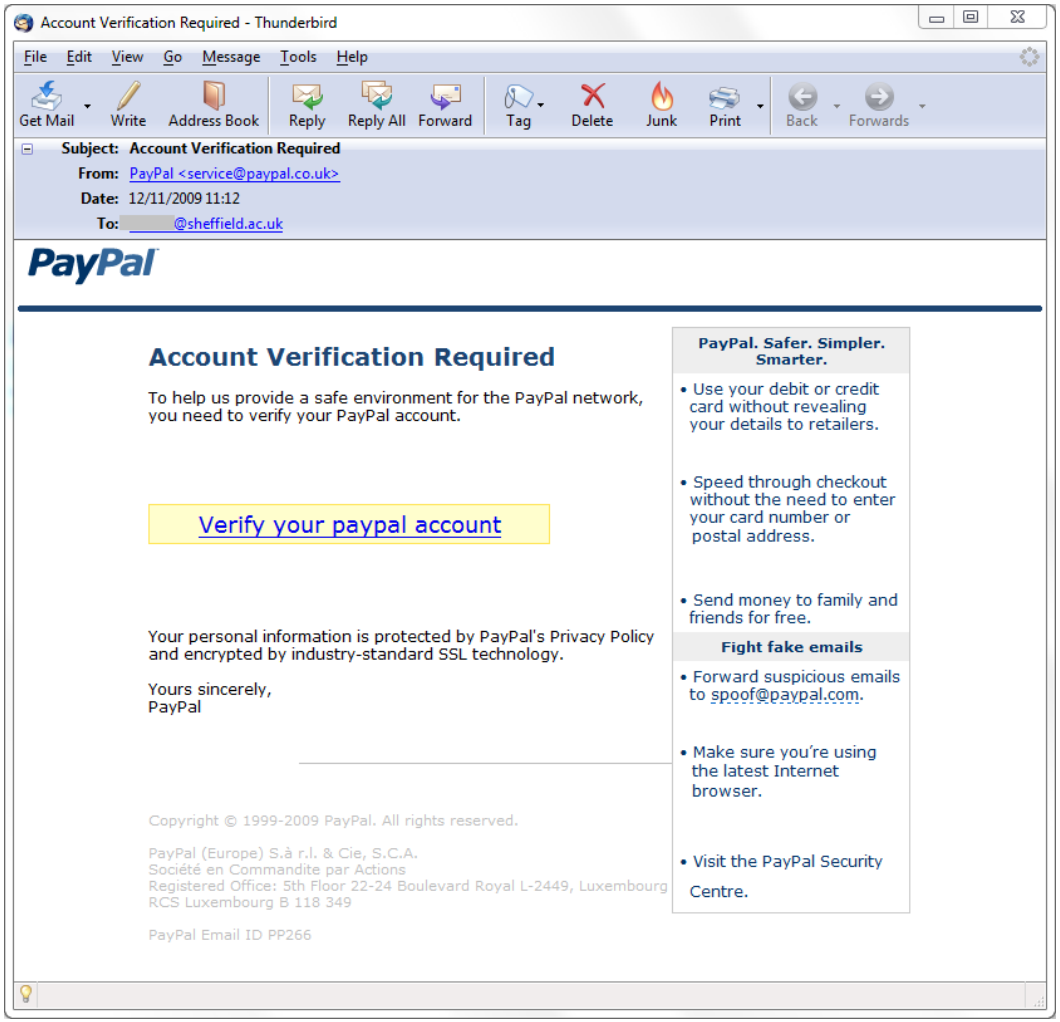
robert.miller@university.teaching-research-group.com

Hallo, ich heiße Robert Miller. Ich bin Professor und möchte mich gerne bei Ihnen bewerben. Bitte teilen Sie mir die E-Mail-Adresse Ihres Personalverantwortlichen sowie die des akademischen Direktors, der für die Einstellung von Fakultäten zuständig ist mit. Vielen Dank im Voraus für Ihre Hilfe. Mit freundlichen Grüßen Robert Miller

Impersonation

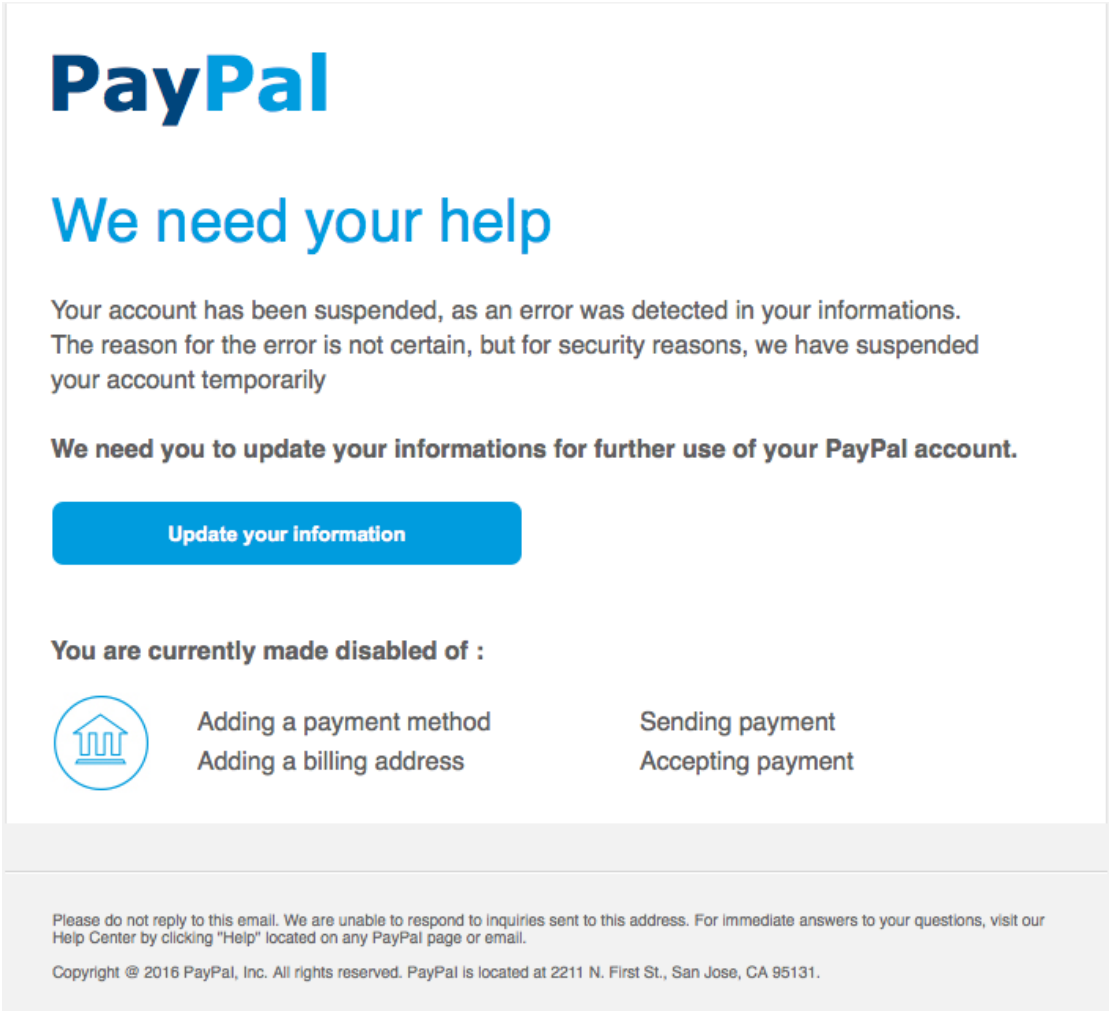
- Erlangtes Wissen einsetzbar, um Mitarbeiter zu imitieren
- $\Rightarrow$ Misstrauen nicht mehr so hoch/nicht vorhanden
- Besonders effektiv per E-Mail
- Häufig sehr hoher Schaden, schwierig abzuwehren
- Gegenmaßnahme: Bei kritischen Vorgängen erneut über weiteres Medium nachfragen, weitere Mitarbeiter hinzuziehen

Phishing



Quelle: https://www.sheffield.ac.uk/cics/phishing/paypalexample

Phishing



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method
Adding a billing address
Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright @ 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

Quelle: https://security.berkeley.edu/news/phishing-example-paypal-we-need-your-help

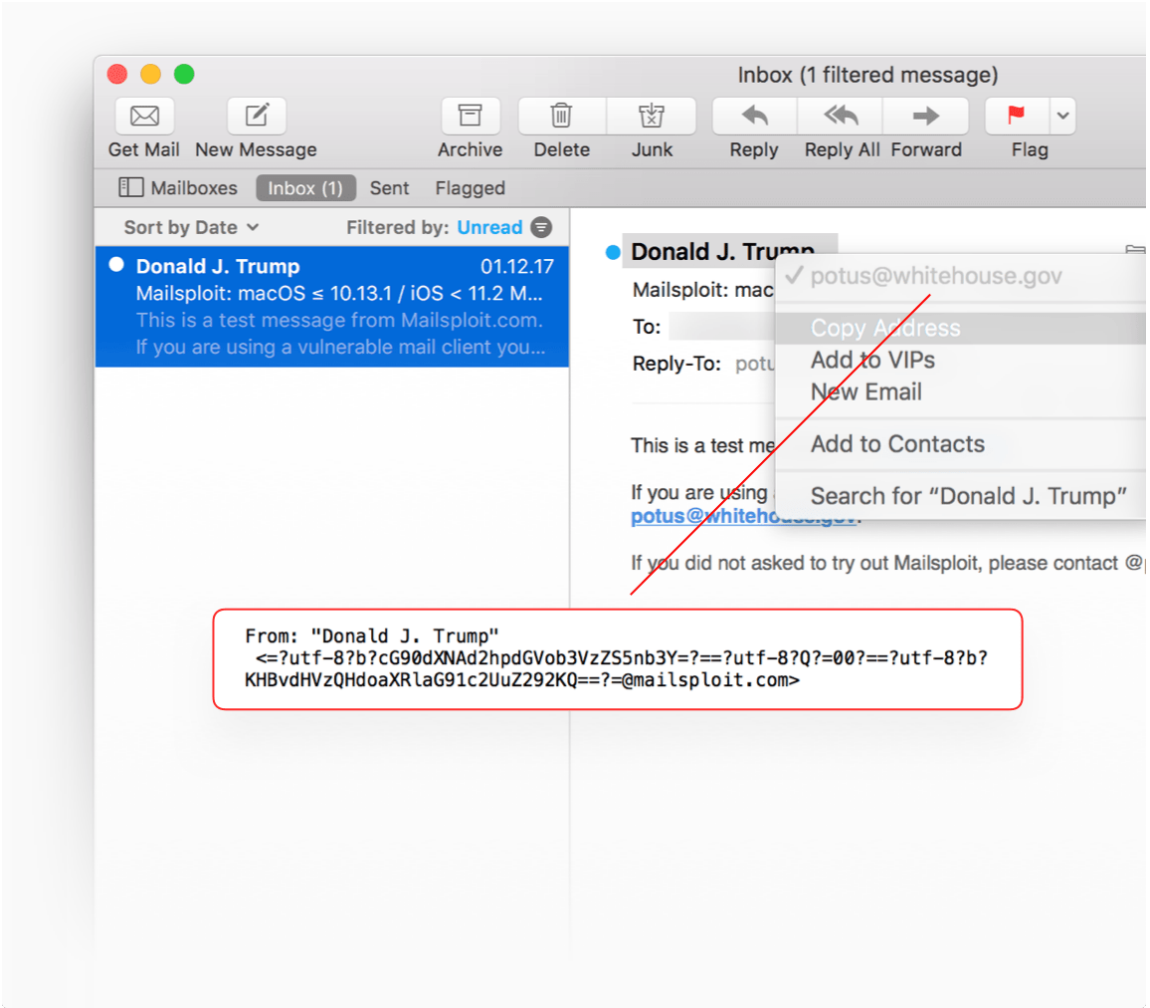
Phishing

- Daten werden durch Userinteraktion abgegriffen
- Häufig kombiniert mit Social Engineering
- Betrifft auch interne Vorgänge $\Rightarrow$ Spear Phishing
- Auch hierbei: Nachfragen, Sicherstellen der Authentizität

Variante: Spam

- Keine Links, reine Kontaktaufnahme
- $\Rightarrow$ Zielt auf Neugier/Pflichtbewusstsein ab
- Infrastruktur wird professioneller
- Misstrauen geringer als bei Phishing

Mailsploit



Quelle: https://mailsploit.com

Mailsploit

- Entdeckt von Sicherheitsforscher Sabri Haddouche 2017, veröffentlicht Dezember 2017
- Problem von Mail-Clients, nicht -Server
- Hersteller wussten Bescheid, schoben das Problem auf die Server
- Teilweise immer noch ungepatchte Clients vorhanden

Mailsploit Teil 1

- Null-Bytes und/oder Zeilenumbrüche in From-Header (z.B. UTF-8)
- Mail-Client dekodiert Zeichenkette fehlerhaft
- Teilweise plattformabhängig, da Systemfunktionen genutzt werden
- Am Beispiel Apple Mail:
  - iOS bricht Parsen nach Null-Byte ab
  - MacOS ignoriert Null-Byte, bricht Parsen aber nach valider Mailadresse ab

Mailsploit Teil 2

- Code Injection durch nicht korrektes Parsen der From-Header bei manchen Clients möglich
- Besonders betroffen: Web Clients
- Nutzbar z.B. für XSS
- Weit weniger verbreitet als der Anzeigefehler

Mailsploit – Abwehrmöglichkeiten

- Quelltext der Mail
- Antworten nur bedingt (reply-to-Header gesetzt bei Phishing-Mails)
- Signieren der Mails (externe Partner?)
- „Übliche“ Awareness-Maßnahmen

Mailsploit im LUIS

Von: Heuchert, Patrick <Patrick.Heuchert@zuv.uni-hannover.de>
An: casselt@luis.uni-hannover.de
Betreff: Aktualisierte rechnung ROI776867

Mailsploit im LUIS

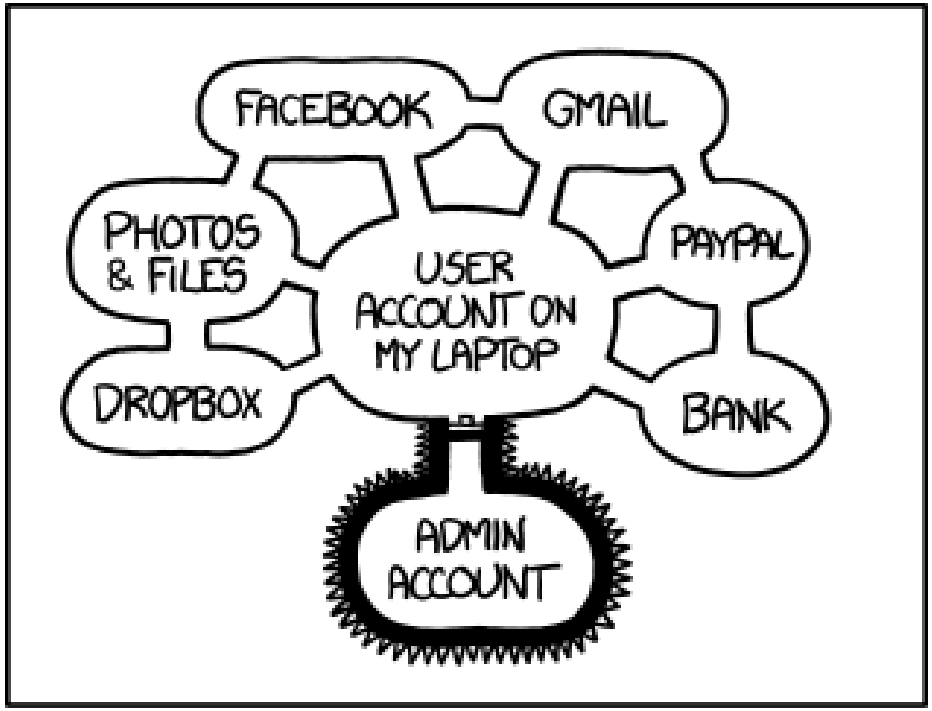
Von: Heuchert, Patrick <Patrick.Heuchert@zuv.uni-hannover.de>
An: casselt@luis.uni-hannover.de
Betreff: Aktualisierte rechnung ROI776867

```
From: Heuchert, Patrick <Patrick.Heuchert@zuv.uni-
    hannover.de> <paty.fernandez@vivelink.com.mx>
```

Diebstahl

- Hardware (Laptop/Smartphone)
- Häufig auch „nur“ verloren
- $\Rightarrow$ Verlust aller Daten
- Gegenmaßnahme: Festplattenverschlüsselung, sicheres Benutzerpasswort

Diebstahl



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Quelle: https://xkcd.com/1200/

Wachsamkeit

- Wichtige Vorgänge nicht „mal eben schnell“ erledigen
- Im Zweifel nachfragen, zweite Meinung einholen
- Software aktuell halten
- Hardware verschlüsseln
- $\Rightarrow$ Keine simple Schablone als Lösung aller Probleme
- $\Rightarrow$ Einstellung ändern: „Security im Kopf“

Danke!

Vielen Dank für die Aufmerksamkeit!

Fragen, Erfahrungsberichte, Fallbeispiele,. . . ?

Fallbeispiel 1

Geschäftszimmer wird per Mail von Professor aufgefordert, per Link einen Ordner freizugeben, da die Zugangsdaten zur Cloud gerade nicht vorliegen.

Fallbeispiel 2

Anfrage per Mail: Passwortrücksetzung in der Projektablage

Fallbeispiel 3

Passwortrücksetzung im IdM nur per Hauspost; Professor befindet sich im Ausland