NoPhish Web Application

Prof. Melanie Volkamer & Simon Stockhardt

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

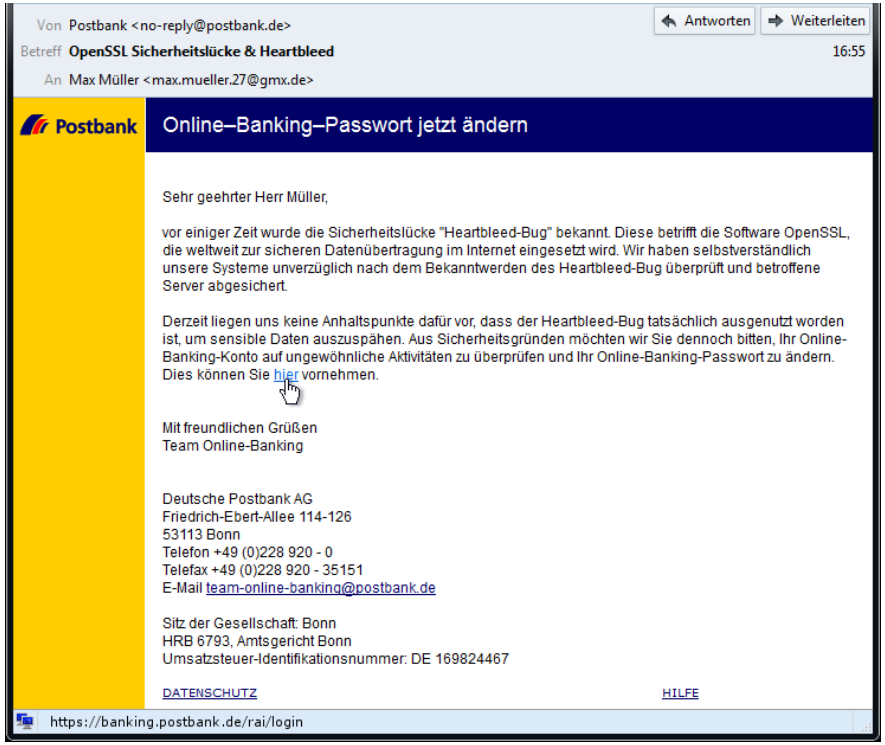
CASED
Usable Security Lab
Crypto Lab

Einführung – Phishing

- **Definition:** Phishing ist der Versuch von Kriminellen, die Opfer dazu zu bewegen, persönliche Informationen auf einer manipulierten Webseite preiszugeben.

- **Konsequenzen:** finanzieller Verlust, Image Verlust (privat und geschäftlich), …
- **Relevanz**
  - **APWG:** 72758 Phishing-Angriffe im ersten Halbjahr 2013
  - **BKA:** 6422 Phishing-Fälle beim Online-Banking in 2011 (25,7 Mio. Euro Schaden)

Phishing oder legitim?



Von Postbank <no-reply@postbank.de>
Betreff **OpenSSL Sicherheitslücke & Heartbleed**
An Max Müller <max.mueller.27@gmx.de>

Antworten Weiterleiten
16:55

Postbank

Online–Banking–Passwort jetzt ändern

Sehr geehrter Herr Müller,

vor einiger Zeit wurde die Sicherheitslücke "Heartbleed-Bug" bekannt. Diese betrifft die Software OpenSSL, die weltweit zur sicheren Datenübertragung im Internet eingesetzt wird. Wir haben selbstverständlich unsere Systeme unverzüglich nach dem Bekanntwerden des Heartbleed-Bug überprüft und betroffene Server abgesichert.

Derzeit liegen uns keine Anhaltspunkte dafür vor, dass der Heartbleed-Bug tatsächlich ausgenutzt worden ist, um sensible Daten auszuspähen. Aus Sicherheitsgründen möchten wir Sie dennoch bitten, Ihr Online-Banking-Konto auf ungewöhnliche Aktivitäten zu überprüfen und Ihr Online-Banking-Passwort zu ändern. Dies können Sie hier vornehmen.

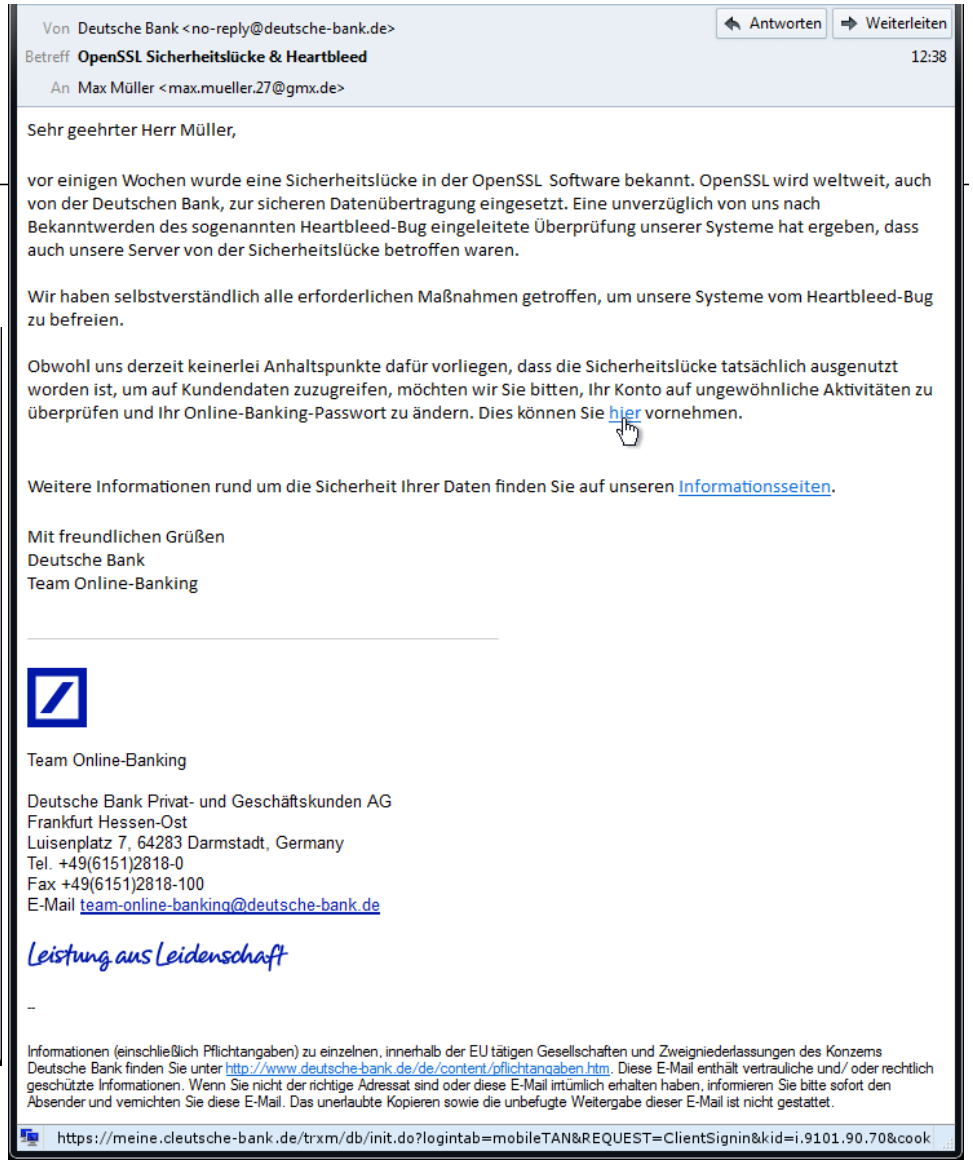
Mit freundlichen Grüßen
Team Online-Banking

Deutsche Postbank AG
Friedrich-Ebert-Allee 114-126
53113 Bonn
Telefon +49 (0)228 920 - 0
Telefax +49 (0)228 920 - 35151
E-Mail team-online-banking@postbank.de

Sitz der Gesellschaft: Bonn
HRB 6793, Amtsgericht Bonn
Umsatzsteuer-Identifikationsnummer: DE 169824467

DATENSCHUTZ HILFE

https://banking.postbank.de/rai/login



Von Deutsche Bank <no-reply@deutsche-bank.de>
Betreff **OpenSSL Sicherheitslücke & Heartbleed**
An Max Müller <max.mueller.27@gmx.de>

Antworten Weiterleiten
12:38

Sehr geehrter Herr Müller,

vor einigen Wochen wurde eine Sicherheitslücke in der OpenSSL Software bekannt. OpenSSL wird weltweit, auch von der Deutschen Bank, zur sicheren Datenübertragung eingesetzt. Eine unverzüglich von uns nach Bekanntwerden des sogenannten Heartbleed-Bug eingeleitete Überprüfung unserer Systeme hat ergeben, dass auch unsere Server von der Sicherheitslücke betroffen waren.

Wir haben selbstverständlich alle erforderlichen Maßnahmen getroffen, um unsere Systeme vom Heartbleed-Bug zu befreien.

Obwohl uns derzeit keinerlei Anhaltspunkte dafür vorliegen, dass die Sicherheitslücke tatsächlich ausgenutzt worden ist, um auf Kundendaten zuzugreifen, möchten wir Sie bitten, Ihr Konto auf ungewöhnliche Aktivitäten zu überprüfen und Ihr Online-Banking-Passwort zu ändern. Dies können Sie hier vornehmen.

Weitere Informationen rund um die Sicherheit Ihrer Daten finden Sie auf unseren Informationsseiten.

Mit freundlichen Grüßen
Deutsche Bank
Team Online-Banking

Team Online-Banking

Deutsche Bank Privat- und Geschäftskunden AG
Frankfurt Hessen-Ost
Luisenplatz 7, 64283 Darmstadt, Germany
Tel. +49(6151)2818-0
Fax +49(6151)2818-100
E-Mail team-online-banking@deutsche-bank.de

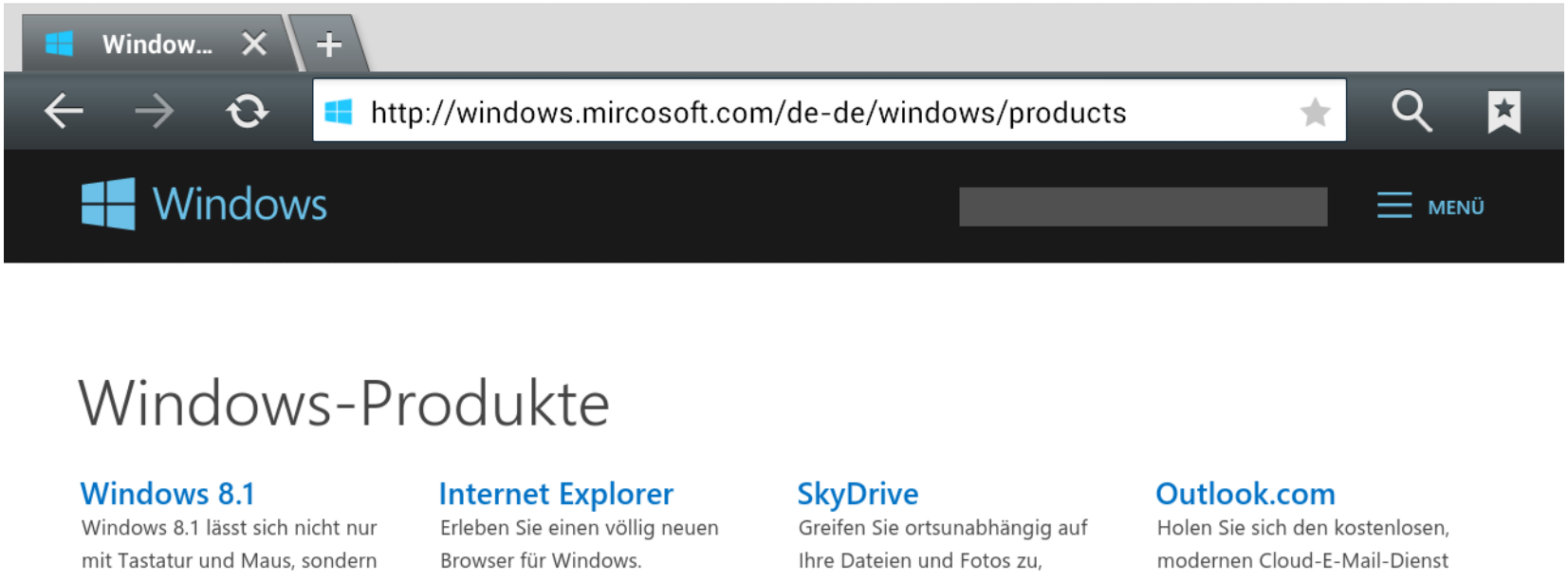
Leistung aus Leidenschaft

--

Informationen (einschließlich Pflichtangaben) zu einzelnen, innerhalb der EU tätigen Gesellschaften und Zweigniederlassungen des Konzerns Deutsche Bank finden Sie unter http://www.deutsche-bank.de/de/content/pflichtangaben.htm. Diese E-Mail enthält vertrauliche und/ oder rechtlich geschützte Informationen. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese E-Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser E-Mail ist nicht gestattet.

https://meine.cleutsche-bank.de/trxm/db/init.do?logintab=mobileTAN&REQUEST=ClientSignin&kid=i.9101.90.70&cook

Phishing oder legitim?



Für Ungeschulte immer schwerer zu erkennen

Status Quo: NoPhish – Android App

- Eingeteilt in 8 Level zu unterschiedlichen Phishing Methoden
- Siehe App Store

- Aufbau der Level:
  1. Erklärung der Regeln des jeweiligen Levels
  2. Darstellungen von URLs
  3. Abfrage ob diese URLs legitime oder phishing URLs sind

Aufgabenstellung

- Übertragen der App-Inhalte in einen Webservice
  - Modularer Aufbau
  - Ergänzung um Screenshots
  - Erweiterung auf E-Mail Beispiele
  - Möglichkeit der Ergänzung um weitere Level
  - Kompatibilität zu Desktop und Mobile Geräten
  - Facebook Connect zum Vergleichen von Highscores/Zeiten

Aufgabenstellung (2)

- Einstiegs- und Abschluss-Test
  - Anpassung des Level-Einstiegs
  - Zertifikatserstellung

- Nutzeridentifikation/Accountmangement
  - Speicherung des Fortschritts zur Wiederaufnahme des Spiels nach vorzeitigem Beenden
  - Reminder E-Mails auch nach Abschluss