Gefahren des Internets

Vortrag im Seniorenrat der Stadt Aachen

07.07.2016

Referent: Michael Sahm

- **Selbstständiger technischer Autor in Aachen**
- **Im Internet „unterwegs“ seit den 1990er Jahren**
- **Ehrenamtliche Vorträge zu den Themen**
  - **Internet-Sicherheit**
  - **Neue Medien im Schulunterricht**
  - **Datenschutz und Verschlüsselung**

Ein Wort vorab

- **Nie dagewesene Möglichkeiten für Kreativität und Kommunikation**
- **Nicht krimineller als in der „realen“ Welt**
- **Täglich neue soziale Herausforderungen**
- **Wenig Wissenstransfer von alt nach jung, sondern gleichberechtigtes Lernen**

Themen

- **Sicherheit bei E-Mails**
  - **Grundlagen**
  - **Spam, Phishing, Schadsoftware, Hoax**
- **Enkeltrick 2.0**
- **Kleine Tatsachenkunde**
- **Anhang**

E-Mail-Grundlagen

- **Erste Textnachricht 1971 (USA) bzw. 1984 (D)**
- **Übertragung von Nachrichten nur im Textformat (auch Anhänge etc.)**
- **Anzeige im Text- oder HTML-Format**
- **günstig, bequem und schnell**

Text- vs. HTML-Anzeige

- **Textnachrichten sind nicht „gestaltet“**
- **Textnachrichten sind beim Öffnen/Lesen unschädlich!**
- **HTML-Nachrichten können gestaltet sein**
- **Gefahr bei Anzeige von HTML-E-Mails**
  - **Versteckte Links auf gefährliche Webseiten**
  - **Nachladen von Schadcode**
  - **Überwachung auf Öffnen der E-Mail**

HTML-E-Mails vermeiden

- **Öffnen Sie HTML-E-Mails im Textformat**
- **Verhindern Sie das Nachladen von externen Inhalten (eigtl. Standard-Einstellung)**
- **Versenden Sie möglichst keine E-Mails im HTML-Format**
- **Hinweise dazu im Anhang**

- **Veröffentlichen Sie Ihre E-Mail-Adresse nicht überall**

Sicherheit bei E-Mails

- **Bekannteste Formen von Gefahren**
  - **Spam**
  - **Phishing**
  - **schädliche Dateianhänge**
  - **Hoax**

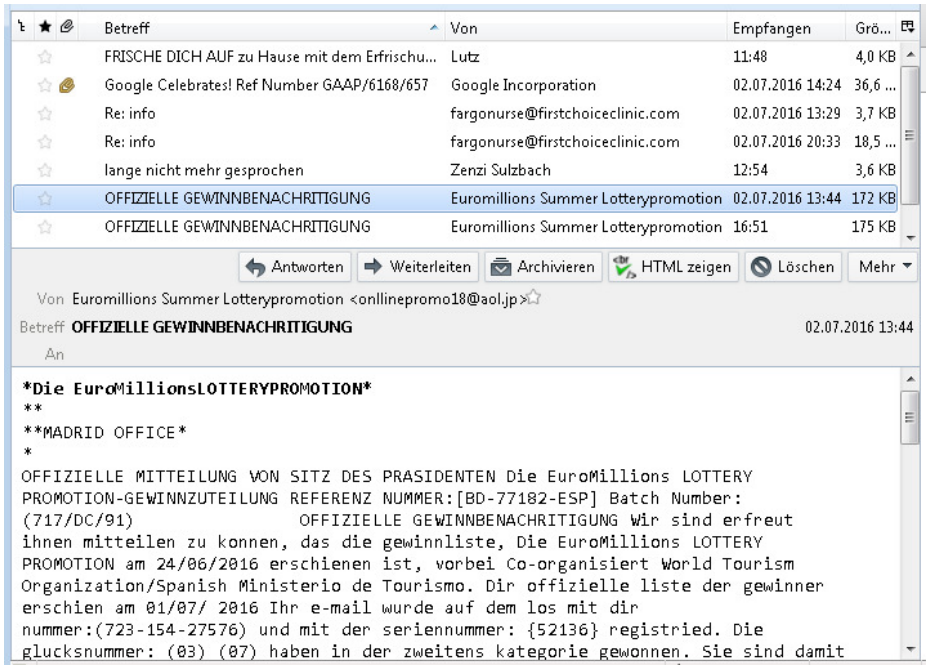
Spam-E-Mails

- **Weltweit täglich mehr als 200 Milliarden E-Mails**
- **Davon mehr als die Hälfte Spam (Versicherung, Abnehmen, Dating, Kredit)**
- **Ärgerlich und lästig, aber weitgehend ungefährlich**
- **Automatische Erkennung orientiert sich an Absendern und Inhalten.**

Spam-E-Mails

- **„False Positives“ und „False Negatives“**
- **Filterung beim E-Mail-Provider oder vom E-Mail-Programm (ggf. online nachschauen)**
- **Newsletter-Spam mit der Aufforderung zur Newsletter-Kündigung nicht beantworten**

Spam-E-Mails



Betreff	Von	Empfangen	Grö...
FRISCHE DICH AUF zu Hause mit dem Erfrischu...	Lutz	11:48	4,0 KB
Google Celebrates! Ref Number GAAP/6168/657	Google Incorporation	02.07.2016 14:24	36,6 ...
Re: info	fargonurse@firstchoiceclinic.com	02.07.2016 13:29	3,7 KB
Re: info	fargonurse@firstchoiceclinic.com	02.07.2016 20:33	18,5 ...
lange nicht mehr gesprochen	Zenzi Sulzbach	12:54	3,6 KB
OFFIZIELLE GEWINNBENACHRITIGUNG	Euromillions Summer Lotterypromotion	02.07.2016 13:44	172 KB
OFFIZIELLE GEWINNBENACHRITIGUNG	Euromillions Summer Lotterypromotion	16:51	175 KB

Antworten | Weiterleiten | Archivieren | HTML zeigen | Löschen | Mehr

Von Euromillions Summer Lotterypromotion <onllinepromo18@aol.jp>

Betreff **OFFIZIELLE GEWINNBENACHRITIGUNG** 02.07.2016 13:44

An

Die EuroMillionsLOTTERYPROMOTION
**
MADRID OFFICE
*
OFFIZIELLE MITTEILUNG VON SITZ DES PRASIDENTEN Die EuroMillions LOTTERY
PROMOTION-GEWINNZUTEILUNG REFERENZ NUMMER:[BD-77182-ESP] Batch Number:
(717/DC/91) OFFIZIELLE GEWINNBENACHRITIGUNG Wir sind erfreut
ihnen mitteilen zu konnen, das die gewinnliste, Die EuroMillions LOTTERY
PROMOTION am 24/06/2016 erschienen ist, vorbei Co-organisiert World Tourism
Organization/Spanish Ministerio de Tourismo. Dir offizielle liste der gewinner
erschien am 01/07/ 2016 Ihr e-mail wurde auf dem los mit dir
nummer:(723-154-27576) und mit der seriennummer: {52136} registried. Die
glucksnummer: (03) (07) haben in der zweitens kategorie gewonnen. Sie sind damit

Phishing

- **„Fishing“ → Angeln: Köder auswerfen und warten, bis jemand anbeißt.**
- **Vortäuschen offizieller Dienste und Angebote (Banken, Amazon, Ebay etc.)**
- **Diebstahl von persönlichen Daten (Kennworte, PIN, TAN)**
- **meistens gut erkennbar, vereinzelt aber täuschend echt.**

Phishing

- **Schlechtes Deutsch und unbekannte Schriftzeichen (z.B. kyrillisch oder falsche Umlaute)**
- **Unpersönliche Ansprache**
- **Aufforderung, eine Webseite zu besuchen und Zugangsdaten einzugeben**
- **Drohungen (Kontosperrung etc.)**
- **Phishing-Mails werden immer besser!**

Phishing-Webseiten

- **Fehlerhafte Webadresse in der Adresszeile des Browsers (z. B. mit Länderkennung „.ru“)**
- **Keine https-Verbindungin der Adresszeile**
- **Unsichere Verbindung (keine Verschlüsselung)**
- **So sollte eine gültige und sichere Verbindung z. B. aussehen:**

Dateianhänge

- **Anhänge können Schadsoftware enthalten**
- **Meist als Rechnung, Mahnung oder Foto getarnt**
- **Dateiendung ist meistens „.exe“ oder „.zip“**
- **Auch Office-Dateien (z. B. „.docx“) können gefährlich sein.**
- **Niemals Anhänge von unbekannten Absendern öffnen!**

Dateianhänge

- **mögliche Schadsoftware**
  - **Viren**
    Verbreiten sich weiter und richten diversen Schaden an.
  - **Trojaner**
    Huckepack in einem anderen Programm
  - **Ransomware**
    Sperrt Rechner, verschlüsselt Daten
  - **Spyware**
    Späht Zugangs- und Kontodaten aus

Schutz vor Schadsoftware

- **Gesundes Misstrauen**
- **Keine Anhänge von unbekannten oder fragwürdigen Quellen öffnen**
- **Regelmäßig Backups erstellen und separat speichern**
- **Virenscanner auf aktuellem Stand halten**
- **Linux-Betriebssysteme sind relativ sicher...**

Nach dem Befall

- **Rechner vom Netzwerk trennen und ausschalten**
- **Für weitere Schritte einen Fachmann hinzuziehen**
- **Suche nach einem Experten: „Computerhilfe Aachen“**

Nach dem Befall

- **Von einem nicht-befallenen Computer aus alle Zugangsdaten vermutlich betroffener Dienste ändern**
- **Kontoauszüge prüfen**
- **Ungewöhnliche Aktivitäten bei Amazon, Ebay etc. prüfen**
- **Bei Ransomware Erpressungsnachricht fotografieren und Anzeige erstatten**

Hoax-E-Mails

- **Verbreitung von Falschmeldungen (Petition gegen Bonsai-Kätzchen, Facebook AGB) oder schädlichen Anweisungen (Einstellungen am Betriebssystem ändern)**
- **Meist inkl. Aufruf zum Weiterleiten**
- **Selten gefährlich für den Computer**
- **Ignorieren, keinesfalls weiterschicken**

Bonsai-Kätzchen

Enkeltrick 2.0

- **Anruf eines „Service-Mitarbeiters“ von Microsoft, Netzanbieter oder Sicherheitsfirma**
- **„Wir haben ein Problem mit Ihrem Betriebssystem festgestellt, das ich gerne mit Ihnen zusammen beheben möchte.“**
- **Installation einer Fernsteuersoftware**
- **Ab dann ist alles möglich!**

Enkeltrick 2.0

- **Lassen Sie sich nicht auf Gespräche ein und legen Sie sofort wieder auf.**
- **Niemand außer Ihnen hat Zugriff auf Ihren Computer (und die NSA … ;-))**
- **Wenn Sie Opfer eines solchen Betrugs geworden sind:**
  - **Trennen Sie den Rechner vom Internet.**
  - **Ändern Sie über einen anderen PC die Zugangsdaten und Passwörter, insbesondere für das Online-Banking.**
  - **Erstatten Sie Anzeige bei der Polizei.**

Kleine Tatsachenkunde

- **Sie nehmen nicht unwissentlich an Verlosungen teil.**
- **Kein afrikanischer Geschäftsmann möchte Ihnen gegen Gebühr zig-Millionen Dollar schenken.**
- **Ihre Bank, Amazon oder Ebay werden Ihnen nicht per E-Mail mitteilen, dass Ihr Konto gesperrt ist.**
- **Kein seriöser Kundendienst wird Sie am Telefon nach Ihrem Kennwort fragen.**

Kleine Tatsachenkunde

- **Facebook, Google, Microsoft und sonstige Multimilliarden-Dollar-Unternehmen möchten Ihnen nichts schenken.**
- **Wenn die Internet-Dienstleistung eines großen Unternehmens nichts kostet, dann sind Sie nicht der Kunde.**

  Dann sind Sie das Produkt!
- **Scheuen Sie sich nicht, auch Tipps für Jugendliche zu beherzigen.**

Anhang

- **Hilfreiche Links**
  - **www.bsi-fuer-buerger.de**
  - **www.surfer-haben-rechte.de**
  - **www.computerbetrug.de**
  - **www.silver-tipps.de**
  - **www.sicher-im-netz.de**
  - **www.klicksafe.de**
  - **www.saferinternet.at**
  - **hoax-info.tubit.tu-berlin.de**

Anhang

- **Anzeige von HTML-E-Mails vermeiden**
  - **Outlook 2010/2013:**
    - **Register „Datei“**
    - **Menüpunkt „Optionen“**
    - **Menüpunkt „Sicherheitscenter“ bzw. „Trust Center“**
    - **„Einstellungen für das Sicherheitscenter / Trust Center“**
    - **Menüpunkt „E-Mail-Sicherheit“**
    - **„Standardnachrichten im Nur-Text-Format lesen“**
    - **„OK“**

Anhang

- **Anzeige von HTML-E-Mails vermeiden**
  - **Outlook 2007:**
    - **Menüpunkt „Extras“**
    - **Menüpunkt „Vertrauensstellungscenter“**
    - **Menüpunkt „E-Mail-Sicherheit“**
    - **„Standardnachrichten im Nur-Text-Format lesen“**
    - **„OK“**

Anhang

- **Anzeige von HTML-E-Mails vermeiden**
  - **Thunderbird:**
    - **Menüpunkt „Ansicht“**
    - **Menüpunkt „Nachrichteninhalt“**
    - **Menüpunkt „Reiner Text“**

Anhang

- **Nachladen von externen Inhalten vermeiden**
  - **Outlook 2010/2013:**
    - **Register „Datei“**
    - **Menüpunkt „Optionen“**
    - **Menüpunkt „Sicherheitscenter“ bzw. „Trust Center“**
    - **„Einstellungen für das Sicherheitscenter / Trust Center“**
    - **Menüpunkt „Automatischer Download“**
    - **„Bilder in HTML-Nachrichten […] nicht automatisch herunterladen“**
    - **„OK“**

Anhang

- **Nachladen von externen Inhalten vermeiden**
  - **Outlook 2007:**
    - **Menüpunkt „Extras“**
    - **Menüpunkt „Vertrauensstellungscenter“**
    - **Menüpunkt „Automatischer Download“**
    - **„Bilder in HTML-Nachrichten […] nicht automatisch herunterladen“**
    - **„OK“**

Anhang

- **Nachladen von externen Inhalten vermeiden**
  - **Thunderbird:**
    - **Menüpunkt „Extras“**
    - **Menüpunkt „Einstellungen“**
    - **Reiter „Datenschutz“**
    - **Option „Externe Inhalte erlauben“ deaktivieren**