Merkblatt 02

Email Phishing Awareness an der UZH

1. Allgemeines

E-Mails sind seit langem ein zentraler Angriffspunkt für die Verbreitung von Schadsoftware, aber auch eine willkommene Plattform für Erpressungs-, Phishing- oder Betrugsversuche. Das wissen wir alle, wird doch in regelmässigem Abstand in den Medien von solchen Fällen berichtet. Und dennoch ereignen sich immer wieder Vorfälle, bei denen Unternehmen durch Datenverlust oder Offenlegung heikler Daten erheblichen Schaden erleiden. Antivirenprogramme und ein fleissiges Aktualisieren der installierten Software helfen zwar einige diese Gefahren zu reduzieren, doch einen 100%igen Schutz gibt es nicht. Ein Bewusstsein (Awareness) dieser Bedrohungen im Umgang mit E-Mails hilft der UZH, wie auch uns selbst, möglichen Schaden zu abzuwenden.

Angreifer interessieren sich für die folgenden Informationen oder Ziele:

- persönliche Informationen über Sie, einschließlich Anmeldeinformationen für Konten, Kreditkarteninformationen, Adresse etc.
- verwertbare Informationen auf dem PC/MAC (z.B. verwundbare Software-Version, heikle Personendaten usw.).
- Umleiten von Informationen zu einem UZH fremden Dienst, so dass alle Informationen, welche übermittelt werden, abgefangen und möglicherweise manipuliert oder verkauft werden können.
- den PC/MAC mit einer Malware infizieren (z.B. über verwundbare Softwareversion), um eines der oben erwähnten Ziele zu erreichen oder einen Fernzugriff zu erlangen.
- Erlangen von Administratorenrechten um tiefer in eine Unternehmensinfrastruktur eindringen zu können.

2. Was ist ein Phishing?

Phishing ist ein einfacher und gefährlicher Angriff und vermutlich hat jeder schon einmal ein Phishing Mail erhalten. Phishing Mails können sehr schlecht gemacht sein oder aber auch täuschend echt aussehen. Sie enthalten einen Link auf eine Webseite oder ein Attachment und man wird meistens zur Eingabe von Passwörtern aufgefordert. In letzter Zeit sind Phishing Attacken immer effektiver geworden, da die gefälschten Nachrichten immer authentischer werden und immer weniger Rechtschreibfehler aufweisen. Dasselbe gilt auch für Weiterleitungen auf Webseiten, welche den Originalen bis auf die Adresse gleichen wie ein Ei dem anderen.

3. 5-Sekunden-Sicherheits-Check

Mit einem 5 Sekunden dauernden Sicherheits-Check können Risiken bereits erheblich reduziert werden. Absender, Betreff, Inhalt, enthaltene Links und Anhänge sind hierbei die fünf kritischen Punkte, die vor dem Öffnen von Anhängen und Links bzw. dem Beantworten von E-Mails beachtet werden sollten:

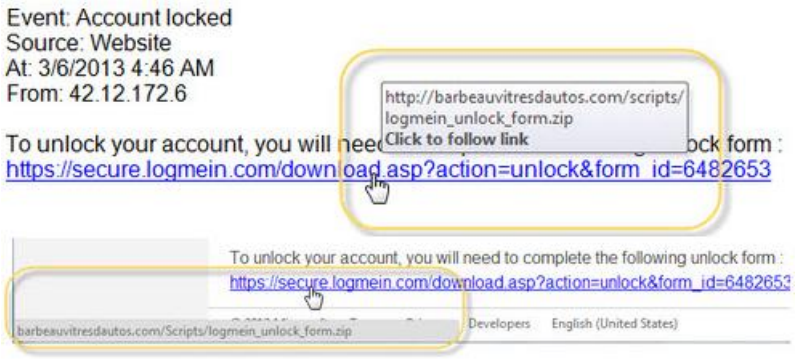
- ist der Absender bekannt?
- stimmt der Absendername mit der E-Mail-Adresse überein?

> Negativ-Beispiel:
> Von: UNIVERSITAT ZURICH uzh bianoda@adv.oabsp.org.br
>
> *Der Absendername weicht erheblich von der Email-Adresse ab und hat in diesem Fall nichts mit der Universität Zürich zu tun.*

- Ist der Betreff sinnvoll?

  Bei folgenden Inhalten ist erhöhte Vorsicht geboten:

  - Unpersönliche Anrede
  - Rechtschreib- und Grammatikfehler / Schreibstil
    - *Falls der Absender ein Bekannter / Vorgesetzter ist, passt der Schreibstil inkl. Abschlussfloskel zu der Person? (Bitte Überweisung avisieren, Cheers….)*
  - nicht landestypische Sprache
  - Andere URL hinter Link
    - *In diesem Beispiel zeigt der Link tatsächlich auf eine andere Seite als der vermeintliche Originallink (wenn man mit dem Mauszeiger über den Link fährt (nicht klicken!))*



- Anhänge – erwarte ich einen Anhang von diesem Absender?
- Zahlungsaufträge – auch wenn diese von Ihrem Vorgesetzten zu kommen scheinen, fragen Sie im Zweifelsfall persönlich nach.
- Fragen nach sensitiven Daten wie z.B. Kennwörter
- Ein deutliches Warnsignal ist, wenn sich in der E-Mail ein Hinweis findet, dass die Daten binnen einer knappen Frist eingegeben werden müssen.
  z.B. „wenn Sie nicht innerhalb der nächsten drei Tage zahlen, dann sperren wir ihr Konto“ oder die Phrasen wie "Ihr Konto wurde manipuliert" oder "Maßnahmen dringend erforderlich" enthalten sind.

In Kombination liefern diese Fragen einen guten Anhaltspunkt ob die E-Mail als vertrauenswürdig einzustufen ist oder nicht. Dabei sollte besonders der „gesunde Menschenverstand“ zum Einsatz kommen. Wenden Sie sich bitte an Ihre IT-verantwortliche Person, den UZH Service Desk oder direkt an it-sicherheit@zi.uzh.ch, sollte der

5-Sekunden-Check kein stimmiges Bild ergeben. Öffnen Sie im Zweifelsfall keinen Anhang, klicken Sie nicht auf Links und geben Sie keine Rückantwort.

4. Wie erkenne ich schädliche Dateianhänge

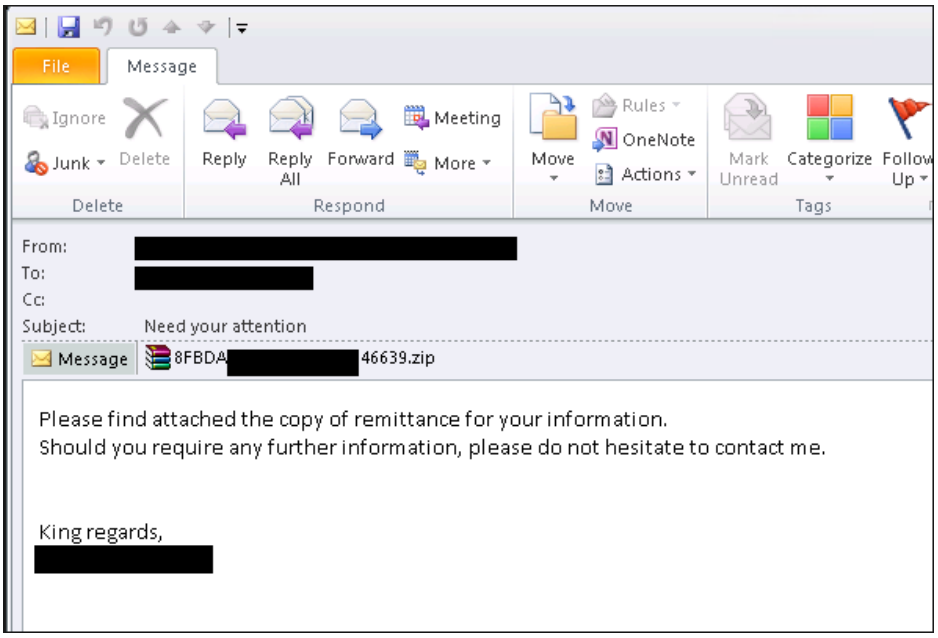
Manchmal landen E-Mails mit Schadsoftware trotz Antivirensoftware in der Inbox. Am gefährlichsten ist derzeit die Bedrohung durch Ransomware, welche den Zugriff auf die eigenen Daten mit einer Verschlüsselung verhindert. Eine Aufschlüsselung der Daten ist in solchen Fällen meistens mit einer Erpressungssumme verbunden. Ein Verschlüsselungstrojaner sperrt lokale Dateien als auch Files auf verbundenen Netzlaufwerken und Servern und es kann passieren, dass innerhalb weniger Minuten sämtliche Dateien am Unternehmensservers unbrauchbar werden. Hier hilft nur eine Sensibilisierung der Mitarbeiter.

Diese Merkmale weisen auf ein Virus-Mail hin:

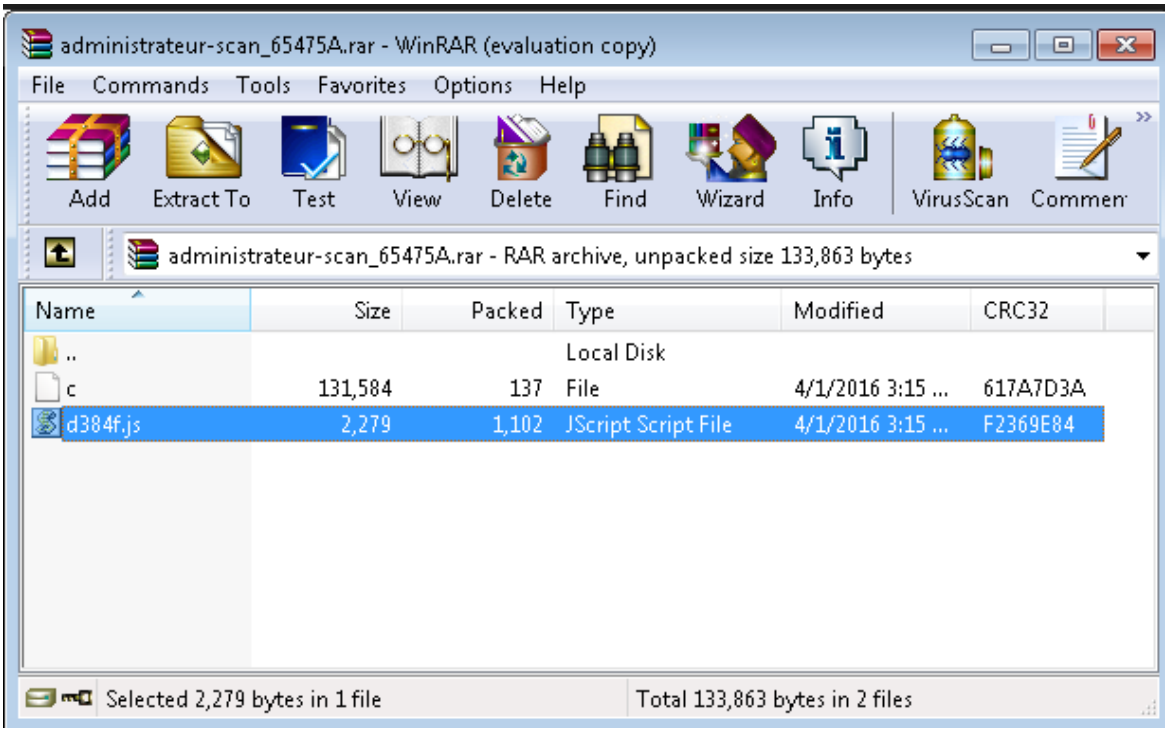
- Anhänge mit ausführbaren Dateien, wie beispielsweise:
  .com, .chm, .cmd, .exe, .jar, .js, .ps1
- Anhänge mit verschlüsselten Archiven:
  .7z, .zip, .rar
- Attachments mit doppelter Dateiendung z.B.:
  .pdf.zip, .doc.exe

Ist im Daten-Explorer die Anzeige von Dateinamenerweiterungen ausgeblendet, so glaubt man es sei ein PDF oder Word Dokument und wird so zum Öffnen verleitet

In diesem Beispiel versteckt sich der Trojaner „Nemucod“ als Java Script in einer zip Datei.



Das ZIP-Archiv enthält dann ein Java Script File.



Doppelklickt man diese Datei, verbindet sich das Schadprogramm zu bestimmten Webseiten und lädt weiteren Schadcode herunter:

```
function loadFile(path) {
  var objStream2 = WScript.CreateObject("ADODB.Stream");
  objStream2.type = 2;
  objStream2.charset = 437;
  objStream2.open();
  objStream2.loadFromFile(path);

  var fileContent = objStream2.ReadText;
  objStream2.close();

  return deobRound1(fileContent);
};

var fileContent = loadFile(tempFileName);
```

5. Schutz vor Phishing und Schadsoftware

Behandelt Euren Rechner/ Euer Mobiltelefon wie einen Tresor!

Passwörter: Für jedes Angebot sollten unterschiedliche Passwörter verwendet werden. Im Schadensfall wird der Schaden dann begrenzt, da der Eindringling nicht weitere genutzte Dienste missbrauchen kann. Auch sollte man seine Passwörter in regelmäßigen Abständen verändern. Passwörter sollten dabei aus einem Mix aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen bestehen, um die Sicherheit zu erhöhen.

E-Mail-Adressen: Man sollte mit mehreren E-Mail-Adressen arbeiten. Die Erstadresse nutzt man für wichtige E-Mails, eine Zweitadresse nutzt man für Anmeldungen bei Online-Diensten wie Verkaufsplattformen, bei Facebook, Twitter, Google+ oder anderen Angeboten.

Sparsamkeit: Weniger ist oft mehr, und wer seine Daten gar nicht erst mitteilt, bietet in der Folge potentiellen Angreifern weniger Missbrauchsmöglichkeiten.

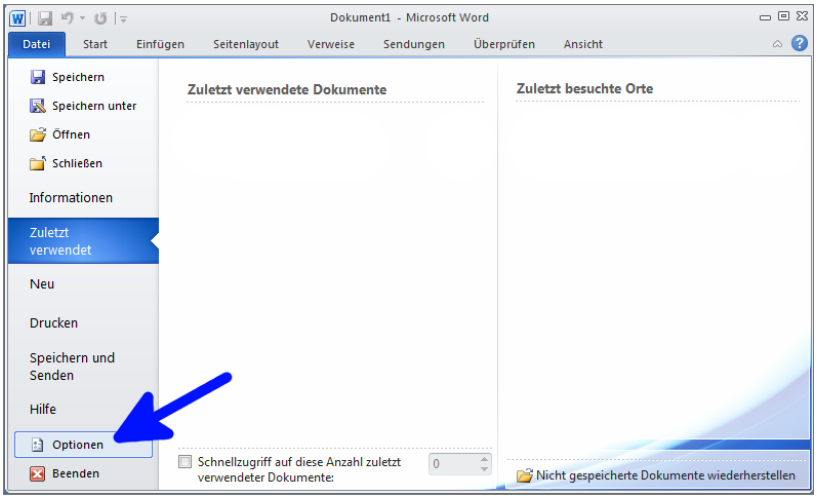
Zusatzdaten: „Reale“ Daten wie Wohn- und Postanschrift oder die eigene Telefonnummer sollten nur angegeben werden, wenn diese für Online-Dienste zwingend erforderlich sind. In vielen Online-Formularen wird die Eingabe dieser Daten als optionale Möglichkeit geführt.

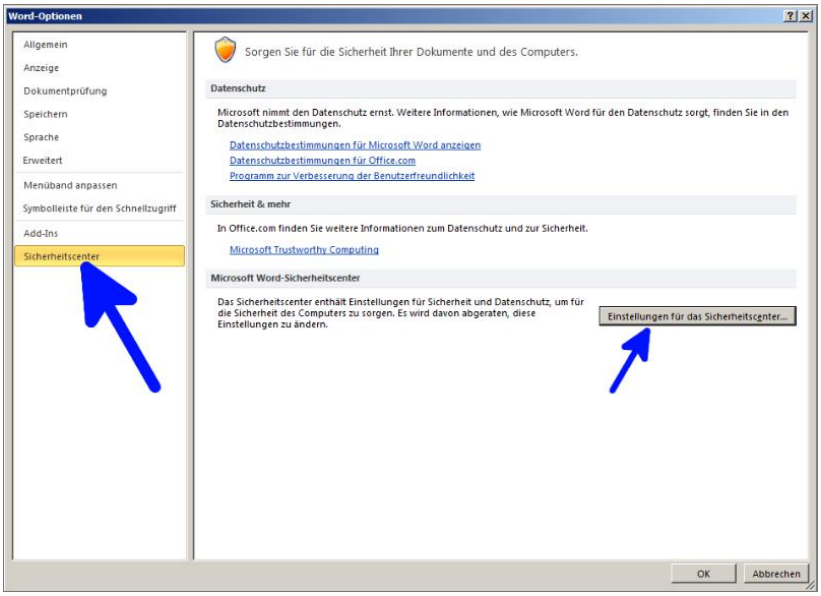
Verschlüsselung: Es existieren viele verschiedene Möglichkeiten, wie man seine Daten bei der Übertragung im Internet verschlüsseln kann. Professionelle Nutzer verwenden oft das Verschlüsselungssystem PGP. Den allermeisten Nutzern wird dies aber zu kompliziert sein. Da aber auch den Anbietern von Online-Diensten, wie Facebook oder Webmailern, diese Problematik bewusst ist, bieten sie ihren Nutzern oft die Möglichkeit, zumindest mit relativ einfach verschlüsselten Verbindungen zu arbeiten.

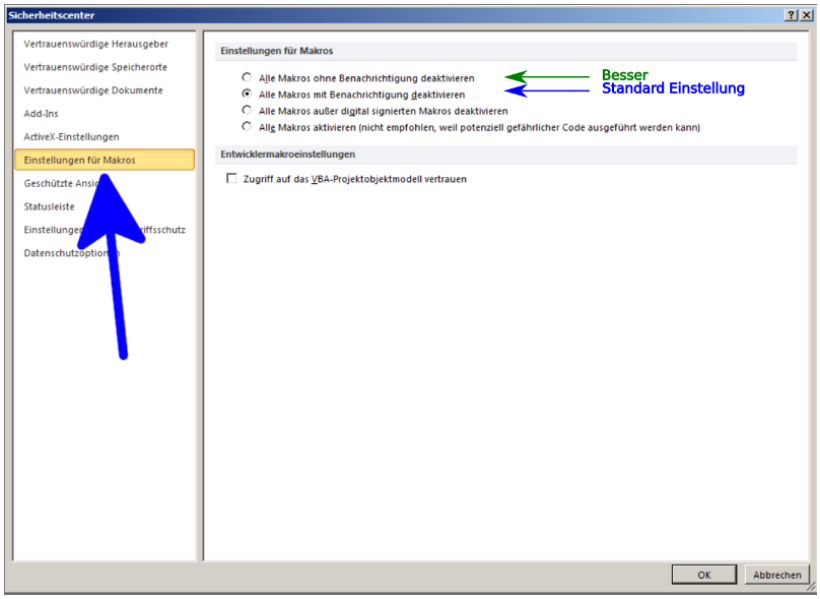
Berechtigung: Programme auf dem Computer nicht mit Administratorenrechten ausführen. Das standardmäßig eingerichtete Administratorkonto sollten Sie für den Alltagseinsatz nicht benutzen, stattdessen richten Sie für sich und andere Benutzer geeignete Benutzerkonten mit eingeschränkten Rechten ein, um Malware und Hackern von vornherein den Zugriff zu erschweren.

Microsoft Office Makro – automatische Ausführung deaktivieren: Makros werden in Excel verwendet, um immer wiederkehrende Abläufe zu automatisieren und somit Zeit und Nerven zu sparen. Makros bieten sich an, auch negative Abläufe, wie das Nachladen von Schadsoftware zu automatisieren, weshalb sie ein beliebtes Werkzeug für Hacker darstellen. In neuen Office-Versionen ist das automatische Ausführen von Makros deshalb standardmässig deaktiviert.

6. Office Makros deaktivieren:







7. Weiterführende Informationen

Reglement über den Einsatz von Informatikmitteln an der UZH (REIM)

Umgang mit PC/MAC im Büroalltag