Sicheres Verhalten im elektronischen Verkehr

Wir sind stets bemüht, unsere datenverarbeitenden Systeme auf dem neuesten und sichersten Stand der Technik zu halten, um ein reibungsfreies und ungestörtes Arbeiten zu ermöglichen. Nach "außen" sind wir hierbei durch mehrere Firewalls und aktuelle Software zur Angriffsabwehr nach aktuellem Wissensstand gut geschützt.

Leider erfolgen immer mehr Angriffe auf Firmennetzwerke von "innen" heraus mit (unbewusster) Beteiligung von Computerbenutzern. Großer Schaden entsteht dabei regelmäßig durch die Einfallstore Web-Browser und E-Mail-Verkehr, durch welche Arbeitsplätze mit Schadsoftware infiziert werden können.

Im Folgenden stelle ich einige Verhaltensweisen zusammen, die das Risiko, mit bösartiger Software infiziert zu werden, erheblich verringern können:

Umgang mit E-Mails

Die altbewährte Methode, **dubiose E-Mails einfach nicht zu öffnen**, und schon gar nicht auf Verweise, oder Anhänge in diesen zu klicken, ist immernoch als wirksam einzustufen, allerdings wird es immer schwieriger, bösartige Mails von normalem Geschäftsverkehr zu unterscheiden.

Angreifer benutzen inzwischen selbstlernende, neuronale Netze, um Kontakte und Geschäftsverkehr infizierter Benutzer zu analysieren. Basierend auf dem Erlernten werden E-Mails und Dokumente versandt, die für den Empfänger immer schwerer vom üblichen Mailverkehr zu unterscheiden sind. Daraus ergeben sich für uns einige verschärfte Verhaltensweisen, mit denen wir uns anfreunden müssen:

Trauen Sie keinem Absender, nur weil Sie dessen Namen und Emailadresse kennen!
Wenn ein Computer eines bekannten Freundes, Arbeitskollegen oder Geschäftsparners infiziert wurde, kennt der Angreifer unter Anderem *ihre Mailadresse, sowie den gesamten Inhalt ihres bisherigen E-Mail-Verkehrs*. Sie werden also i.d.R. mit korrektem Namen und korrekter Anrede angeschrieben, wobei die Grußformel und der Name des Unterschreibenden ebenfalls "korrekt" erscheinen.

Trauen Sie nicht automatisch E-Mails, nur weil deren Inhalt auf den ersten Blick normaler Geschäftsverkehr ist!

Noch schlimmer: Hat ihnen die Gegenstelle zumeist Rechnungen, Lieferscheine, oder Aufträge als PDF gesendet, so können Sie davon ausgehen, dass sie E-Mails erhalten werden, die den bisherigen Rechnungen exakt bis auf gefälschte Rechnungs- Kunden- oder Vorgangsnummern gleichen - nur dass die Dokumente beim Öffnen ihren Computer infizieren werden. Denken Sie hierbei auch an Amazon-Auftragsbestätigungen, Lieferupdates, DHL-Sendungsbenachrichtigungen, Rechnungen von Geschäftspartnern, Hallöchens von alten Freunden ...

Wie beurteile ich nun eingehende Mails?

- Soweit nicht schon in der Standardansicht verdächtig: Lassen Sie sich ausführliche Infos der Mail anzeigen. Benutzen Sie dafür die entsprechende Funktion ihres E-Mail-Programmes: Mail-Header / Kopfdaten / Originaltext anzeigen etc.
- Ist der korrekte Adressat im Kopf der Mail angegeben, also nicht nur Vor-und Zuname, sondern die gesamte Mailadresse? Ist mir die Mailadresse bekannt? Nein -> Verdacht, Ja -> noch keine Entwarnung
- An wen wurde die Mail noch versandt? Macht es Sinn, dass eine private, bzw. geschäftlich an mich adressierte Mail noch an mehrere andere Personen versandt wurde, die ich nicht kenne? Ja -> Vorsicht!
- Enthält die Mail Verweise auf Webseiten oder angehängte Dokumente? Ja -> Vorsicht!
  (Die erste Frage hierzu: Ändert sich irgendwo über der Mail der Mauszeiger, so, als ob sie über einem Verweis sind?)
  In den meisten Mailprogrammen genügt es, mit dem Mauszeiger über den entsprechenden Verweis zu gehen (**ohne diesen jedoch anzuklicken!**). In der Regel wird im unteren Bereich die Verweisadresse angezeigt, die beim Anklicken aufgerufen würde. Sehen diese kryptisch aus, oder verweisen auf Länderkennzeichen, wo der rechnungslegende Klempner garantiert nicht ansässig ist (z.B. ckickmail.to xyz.ru adnet.cn o.ä.), lassen Sie Vorsicht walten!
- Auch wenn es sich befremdlich liest: Benutzen Sie ihr **Bauchgefühl** ebenso, wie ihren **gesunden Menschenverstand** - beide unterscheiden uns (noch) von Algorithmen / Maschinen! Auch, wenn Sie nicht genau wissen, *was* es ist - wenn ihnen etwas "komisch" vorkommt, suchen sie Rat!

Sind Sie sich nicht sicher, **kontaktieren Sie den Absender auf einem anderen Kanal, z.B. telefonisch oder per Fax** und lassen sich bestätigen, dass er die Mail zur betreffenden Zeit an Sie versandt hat.

Sollte sich die Mail als gefälscht erweisen, leiten Sie diese mit ensprechendem Vermerk an das CMS (cms-benutzerberatung@hu-berlin.de) weiter, und löschen sie Sie anschließend!
Weiterhin informieren Sie den "echten" Absender darüber, dass er höchstwahrscheinlich Opfer eines Angriffs geworden ist, so dass er entprechende Maßnahmen ergreifen kann.

Haben Sie den Verdacht, dass sie bereits infiziert wurden?

Nehmen Sie umgehend Kontakt mit ihrem IT-Betreuer auf, wenn Sie Unregelmäßigkeiten oder sonst irgenwie seltsames Verhalten ihres Computersystems feststellen!

Weitere Maßnahmen:

- Öffnen Sie keine Dokumente, über dessen Ursprung sie Zweifel haben - auch Videos, Bilder, PDFs und Audiomaterial.
- Textansicht von Mailtexten erzwingen. Grafiken, und ggf. kontaminierende Darstellungselemente werden nicht angezeigt. Dies hat einige Nachteile, ggf. werden einige Informationen nicht (korrekt) angezeigt, erhöht aber die Sicherheit.
- Globales Deaktivieren von Makros in Office-Dokumenten.
  Führen Sie niemals Makros in Dokumenten aus, deren Quelle sie nicht kennen, und ignorieren Sie niemals entsprechende Warnungen - Lesen Sie genau, bevor Sie

eine Warnung "wegklicken"!

Bitten Sie hierzu ggf. ihren IT-Betreuer um Rat.

Surfen im Web

- Benutzen Sie nur Websites, denen Sie vertrauen.
- Haben Sie immer einen Blick auf die Adresszeile im Webbrowser (Ist das die Website, die sie besuchen wollten, oder ist sie nur ähnlich? (z.B. http://googe.de oder http://sparkasse-berlin.de.*cn*)).
  Ignorieren Sie niemals Sicherheitswarnungen ihre Browsers!
  Holen Sie sich Hilfe, wenn Sie sich nicht sicher sind!
- Klicken Sie nicht wahllos auf alles, was Sie dazu auffordert (s.o. -> gesunder Menschenverstand)

Schauen Sie in regelmäßigen Abständen auf diese Seite! Bei neuen Erkenntnissen wird diese umgehend aktualisiert.
Haben *Sie* neue Erkenntnisse, die Sie an dieser Stelle sehen möchten, kontaktieren Sie uns bitte (s. Impressum)

Beste Grüße und einen friedlichen Arbeitsalltag

Martin Mammel

Links zur aktuellen Lage:

- BSI: Aktuelle Information zur Schadsoftware Emotet
  https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html
- Heise.de: Schutz vor Emotet: Besserer Umgang mit Doc-Dateien:
  https://www.heise.de/security/meldung/Schutz-vor-Emotet-Besserer-Umgang-mit-Doc--ateien-4452870.html