Wie man sich zumindest vor Computerviren schützen kann

Das seit 2014 bekannte Computervirus „Emotet“ [1] erreichte 2018 eine neue Gefahrenstufe, als es E-Mails auslesen und deren Adressen und Inhalt zum Angriff verwenden konnte: Man erhält dabei eine E-Mail von einem (bekannten) Absender mit scheinbar echtem Inhalt, der dazu verleiten soll, einen schädlichen Dateianhang (meist im Word-Format) zu öffnen oder einen präparierten Link anzuklicken[2] (sogenanntes *Phishing*).

Foto: Darwin Laganzon/pixabay

Folgen Sie einer solchen Aufforderung, wird Ihr Windows-Rechner infiziert und „Emotet“ kann Ihre Daten, auch durch Nachladen anderer Schadsoftware, verschlüsseln und gegebenenfalls Ihr gesamtes Firmennetz befallen [2]. Sie werden dann aufgefordert, eine große Summe zu zahlen, wonach Sie angeblich einen „Schlüssel“ bekommen, damit Sie wieder an Ihre Daten gelangen. Zu den Opfern solcher Angriffe, die bekannt wurden, zählen öffentliche Einrichtungen [4,6,7] oder auch Unternehmen [2]. Um das Virus wirklich wieder los zu werden hilft in der Regel nur, den Rechner bzw. das ganze Netzwerk neu aufzusetzen [2].

Wie können Sie einem Virenbefall vorbeugen? [6,9,10] Generell gilt: Am allerbesten bleiben Sie vorsichtig! Niemand wird Ihnen ernsthaft via E-Mail mitteilen, dass er Sie mit Millionen Euro beschenkt, sondern vielmehr handelt es sich bei solchen Mails um Versuche, an Ihr Geld zu kommen! Weiterhin sollten Sie folgende Maßnahmen treffen: Führen Sie regelmäßig ein externes Backup auf einer Festplatte durch, die nur zur Datensicherung an Ihren Rechner angeschlossen wird, und am besten noch ein zweites externes Backup auf einer weiteren Festplatte, die ebenfalls nur zur Datensicherung an Ihren Rechner angeschlossen und ansonsten außer Haus verwahrt wird. Führen Sie zudem regelmäßig alle Updates für Windows und andere Programme durch und sorgen Sie kontinuierlich für einen aktuellen Virenschutz. Nicht weniger wichtig: Arbeiten Sie nur als Administrator, wenn es notwendig ist, z.B. bei der Installation von Programmen, sonst nur als „normaler“ Benutzer.

Um das Risiko einer Infektion generell deutlich zu verkleinern empfiehlt es sich, das Betriebssystem zu wechseln [4]. Zu empfehlen ist z.B. eine Linux-Distribution, die Sie kostenlos (auch für Ihren schon vielleicht etwas älteren Rechner) bekommen können [8].

Mögen Sie von allen Viren verschont bleiben!

[1] Überblick: www.heise.de/thema/Emotet (abgerufen am 31.3.2020)
[2] ausführlich: Jürgen Schmidt: Emotet bei Heise. Erste Lehren aus einem Emotet-Trojaner-Befall. In: c't 2019, 13, 36--38
[3] Christian Wölbert: Schmerzhafte Lektion. Was Emotet anrichtet -- und welche Lehren die Opfer daraus ziehen. In: c't 2020,6,14--17.
[4] Peter Siering: Leichte Beute. Wie sich Emotet durch Windows frisst. In: c't 2020,6,18--20
[5] Ronald Eikenberg Peter Siering und Axel Vahldiek: Emotet abwehren. Pragmatischer Schutz vor Emotet & Co. In: c't 2020, 6, 22-26
[6] Martin Wundram: Emotet austreiben. Incident Response: Was tun, wenn man betroffen ist? In: c't 2020, 6, 28--31.
[7] www.heise.de/newsticker/meldung/Uni-Giessen-nach-Cyber-Attacke-groesstenteils-wieder-online-4692730.html (aberufen am 28.3.2020)
[8] de.wikipedia.org/wiki/Linux
[9] weitere Schutzmaßnahmen unter ct.de/check2020 (abgerufen am 5.4.2020), mit Booklet zum Download
[10] IT-Grundschutzkatalog des BSI siehe ct.de/ye7n (abgerufen am 5.4.2020)

Andreas Dafferner
Geschäftsstelle der
Heidelberger Akademie der Wissenschaften
(Digital Humanities, Datenbanken)

Der Beitrag wurde für „*Athene – Magazin der Heidelberger Akademie der Wissenschaften 1/2020*“ verfasst.