UNIVERSITÄTS RECHENZENTRUM

TECHNISCHE UNIVERSITÄT ILMENAU

3.2.2020

Mitteilung 1/2020 des CIO

Vorsichtsmaßnahmen vor Schadsoftware Emotet

Die laut Sicherheitsbehörden gefährlichste Schadsoftware Emotet ist wieder verstärkt im Umlauf. Der Trojaner infiziert sowohl Behörden-, Firmen- als auch Privatcomputer und hat bereits zu Schäden in Millionenhöhe geführt. Diese neue Welle von Cyberangriffen hat im Dezember dazu geführt, dass u.a. die Justus-Liebig-Universität Gießen mit einem nahezu vollständigen Ausfall aller IT-Systeme zu kämpfen hatte.

Was macht den Schädling so gefährlich? Emotet ist in der Lage, herkömmliche Antivirenprodukte zu täuschen und die Erkennung durch gängige Virenschutzprogramme zu umgehen. Emotet verbreitet sich wie ein Computerwurm und kann auf diese Weise schnell weitere Computer infizieren. Dadurch wird die rasante Ausbreitung der Schadsoftware zusätzlich unterstützt. Ist Emotet erst einmal auf den Computer gelangt, nimmt das Unheil seinen Lauf: Der Trojaner lädt weitere Schadsoftware wie den Verschlüsselungstrojaner Ryuk nach. Dessen perfide Spezialität ist neben dem Verschlüsseln von Dateien das Löschen von Backups, falls er auf dem Computer welche findet. Darüber hinaus erkennt der Virus, wenn er in einer virtuellen Maschine (VM) ausgeführt wird. Wenn Emotet eine geschützte (Sandkasten)Umgebung erkennt, legt er sich dort „schlafen“ und bleibt zunächst untätig. Emotet verwendet auch spezielle Server, um Updates zu erhalten. Das funktioniert automatisch und nahtlos im Hintergrund auf die gleiche Weise, in der zum Beispiel auch das Betriebssystem auf Ihrem PC aktualisiert wird. So können die Angreifer die einmal vorhandene Schadsoftware regelmäßig aktualisieren, neue Versionen und zusätzliche Schadprogramme installieren. Zudem besteht die Gefahr, dass auf einem infizierten Computer auch gestohlene Daten von anderen Opfern gespeichert werden.

Was ist Emotet? Emotet ist ein Trojaner, der vor allem durch Spam-E-Mails verbreitet wird. Die infizierte E-Mail enthält entweder ein bösartiges Skript, ein Office-Dokument mit aktivierten Makros oder einen bösartigen Downloadlink. Emotet-E-Mails sind oft gut gefälscht und täuschend echt als reguläre E-Mails getarnt. Sie versuchen ganz gezielt, die Benutzer zum vorsätzlichen Anklicken der bösartigen Dateien zu animieren. Da Emotet auch Kontaktinformationen und -beziehungen sowie Kommunikationsinhalte aus E-Mail-Programmen abgreift, kommen authentisch wirkende Spam-Mails zustande. Es handelt sich um einen teils automatisierten Social-Engineering-Angriff, der auch deshalb so erfolgreich ist, weil Spam-Mail-Empfänger vorgeblich von Absendern Nachrichten erhalten, mit denen sie tatsächlich zuletzt in Kontakt standen.

Wie kann man sich selbst vor Emotet schützen? Indem Sie diese CIO-Mitteilung aufmerksam lesen, unternehmen Sie bereits den ersten Schritt, um sich und andere vor Emotet zu schützen.

Zusätzliche Schritte umfassen:

- Laden Sie keine dubiosen Dateien bzw. E-Mail-Anhänge herunter, und klicken Sie niemals auf verdächtige Links. Fallen Sie nicht auf gefälschte E-Mails herein - denn so bieten Sie Emotet keine Einstiegspunkte in Ihr System oder Netzwerk. Detaillierte Informationen zum Erkennen von Spam-E-Mails finden Sie im beigefügten PDF Empfehlungen zur Erkennung von Spam-E-Mails.
- Schalten Sie Makros in Office-Programmen ab. Schädliche Software wird oft auf diesem Weg auf Computer geschleust. Sofern Sie nicht zwingend mit Makros arbeiten müssen, schalten Sie sie gänzlich ab. Wie Sie dabei vorgehen, finden Sie im beigefügten PDF Deaktivieren von Makros in Microsoft Office-Dateien.
- Surfen Sie niemals als Admin. Legen Sie bei Windows ein Nutzerkonto ohne Admin-Rechte an und nutzen Sie das Internet, E-Mails und Office-Programme nur damit. So kann keine Software ohne Rückfrage des Betriebssystems installiert werden.
- Grundsätzlich ist es ratsam, regelmäßig alle ihre Daten auf einem externen Datenträger zu sichern (sofern diese nicht vom einem zentralen Backup an der TU Ilmenau erfasst sind).
- Halten Sie Betriebssystem, Virenschutzprogramm und Ihre anderen Programme insbesondere die Microsoft Office Programme immer aktuell und installieren Sie die empfohlenen Sicherheitsupdates.

Welche vorbeugenden Maßnahmen trifft das UniRZ vor Emotet? Aufgrund der akuten Bedrohungslage wurde das Sicherheits-/Virenschutzniveau angepasst. Bei E-Mail-Eingängen werden alle potentiell sicherheitskritischen Dateianhänge entfernt. Der Text der E-Mail wird selbstverständlich wie gewohnt zugestellt und enthält zusätzlich die Information, dass der Anhang aus Sicherheitsgründen entfernt wurde. Dies entspricht bei TUILM-Exchange E-Mail-Postfächern bereits dem Vorgehen bei positiv erkannten Viren. Sollten Sie Office-Dateien mit Makros oder andere als derzeit sicherheitskritisch eingestufte Dateiformate mit vertrauenswürdigen Dritten austauschen wollen, empfehlen wir Ihnen die Nutzung der TU Ilmenau NextCloud. Bei nicht mehr aktuellen Office-Dateiformaten empfehlen wir vor dem Versenden die Umwandlung bzw. Neuspeicherung der Datei in einem aktuellen Office-Dateiformat. Die gängigen Dateiformate wie PDF, .docx (Word-Dateien), .xlsx (Excel-Dateien), .pptx (PowerPoint-Dateien) oder Bilddateien betrifft diese Regelung derzeit nicht.

Was sollten Sie tun, wenn ein verdächtiger E-Mail-Anhang aus Unachtsamkeit versehentlich geöffnet wurde oder ein Download über einen verdächtigen Link erfolgt ist? Geraten Sie nicht in Panik, wenn Sie den Verdacht haben, dass Ihr Computer mit Emotet infiziert sein könnte. Wenn Ihr Computer mit einem Netzwerk verbunden ist, trennen sie ihn unverzüglich davon. Arbeiten Sie auch nicht mit Ihrer virtuellen Maschine (VM) an einem anderen Computer weiter! Nachdem Sie das infizierte System isoliert haben, wenden Sie sich ohne Zeitverzögerung an Ihren Systemadministrator. Informieren Sie den IT-Service-Desk im UniRZ (03677-69-1111) auch wenn Sie noch keine offensichtliche Veränderung an Ihrem Computer festgestellt haben. Computer mit einer Emotet-Infektion müssen neu aufgesetzt werden, weil der Trojaner und nachgeladene Schadsoftware teils tiefgreifende und sicherheitsrelevante Änderungen am System vornehmen. Zudem müssen alle Passwörter geändert werden, die auf dem befallenen Computer gespeichert waren - etwa in Browsern.

Bleiben Sie wachsam!

gez. Günter Springer