Empfehlungen zur Erkennung von Spam- und Phishing-E-Mails

Spam-E-Mail (auch Junk-E-Mail) steht als Sammelbegriff für alle Formen von massenhaft versandten, unerwünschten E-Mails, elektronischen Kettenbriefe oder Werbeposts in sozialen Netzwerken. Unter dem Begriff Phishing versteht man Versuche, über E-Mails oder gefälschte Webseiten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

Emotet wird von Kriminellen vor allem über groß angelegte Spam-Kampagnen verteilt. Dabei wird derzeit vor allem das sogenannte Clone-Phishing eingesetzt. Bei diesem Angriff erstellen Kriminelle eine Kopie von zuvor gesendeten legitimen E-Mails, die entweder einen Link oder einen Anhang beinhalten. Anschließend ersetzen die Angreifer die Links oder Dateianhänge mit bösartigen Ersatzimitaten, die aussehen, als seien sie echt. Die ahnungslosen Benutzer klicken entweder auf den bösartigen Link oder öffnen den bösartigen Anhang, was dazu führt, dass Schadprogramme ausgeführt werden.

Bei einem bereits infizierten Computer liest Emotet E-Mails im Posteingang und antwortet darauf, ohne dass der Nutzer es mitbekommt. Besonders tückisch wird es, wenn der Absender der E-Mail offenbar jemand ist, dem Sie kürzlich geschrieben haben. Denn Emotet sammelt vorhandene E-Mail-Adressen und verschickt sich selbst als Anhang oder Link in neuen Nachrichten. Dazu ist die Schadsoftware in verschiedenen E-Mail-Programmen in der Lage. Im E-Mail-Programm Outlook kann Emotet sogar noch mehr: E-Mail-Inhalte auslesen und für seine selbst verschickten neuen E-Mails nutzen. Die E-Mails, die Emotet verschickt, können dadurch aussehen wie eine Antwort auf eine E-Mail, die Sie selbst kürzlich an die betroffene Person geschickt haben.

Es ist nicht immer einfach, solche Phishing-Versuch zu erkennen. Mit den folgenden Tipps, ein wenig Disziplin und gesundem Menschenverstand kann man aber viel erreichen. Achten Sie auf alles, das ungewöhnlich oder seltsam wirkt. Fragen Sie sich, ob irgendetwas in der E-Mail nach Betrug aussieht. Vertrauen Sie auf Ihre Intuition, Sie brauchen nicht überängstlich zu sein. Phishing-Angriffe setzen oft auf diese Angst, um Ihr Urteilsvermögen zu trüben.

Das können Sie ab sofort konkret tun, um nicht auf Emotet-Cyberangriffe per E-Mail hereinzufallen:

- Löschen Sie offensichtliche Spam- und Phishing-E-Mails sofort – ohne sich diese im Detail anzusehen!
- Öffnen Sie keine E-Mail-Anhänge und klicken Sie nicht auf Links in E-Mails von unbekannten Absendern! Fragen Sie im Zweifel telefonisch nach, ob Ihnen tatsächlich z. B. eine Rechnung per E-Mail geschickt wurde.
- Achten Sie stets auf den Anhang in einer E-Mail. Handelt es sich nicht um eine angehängte Datei, sondern um ein eingefügtes Bild, das den Anschein eines Anhanges erweckt (eingebettet in die E-Mail), lassen Sie die Finger davon.
- Sie sollten stutzig werden, wenn Sie auf einen scheinbaren E-Mail-Anhang klicken und Sie dann auf eine externe Seite weitergeleitet werden. Hier sind garantiert Betrüger am Werk.
- Öffnen Sie auch keine unerwarteten oder ungewöhnlichen Anhänge oder ungewöhnliche Links (Internetadressen) von bekannten Absendern! Auch hier gilt: Fragen Sie im Zweifel telefonisch nach.
- Die E-Mail-Nachricht beinhaltet Links, die etwas seltsam aussehen. Auch wenn Ihr siebter Sinn Sie nicht bei einer der obigen Punkte gewarnt hat, nehmen Sie nicht alle eingebetteten Hyperlinks für bare Münze. Bewegen Sie stattdessen Ihren Cursor über den Link und sehen Sie sich die tatsächliche URL (Internetadresse) an.
- Achten Sie – nach dem Klicken auf einen vertrauenswürdigen Link – besonders auf subtile Schreibfehler auf einer ansonsten bekannt aussehenden Website, da dies ein Hinweis auf eine Täuschung ist. Es ist immer besser, die Internetadresse direkt selbst einzutippen, anstatt auf den eingebetteten Link in der E-Mail zu klicken.

- Prüfen Sie auch E-Mails von Ihnen bekannten Absendern kritisch. Stimmt die Sprache? Ist das Anliegen realistisch?
- Lassen Sie sich immer alle Informationen zur E-Mail (den Absendernamen und die Absender-E-Mail-Adresse, den vollen Dateinamen und das Dateiformat von Anhängen usw.) im Detail anzeigen!
- Misstrauen Sie E-Mails, die die Aufforderung enthalten, Software zu installieren.
- Antworten Sie nicht auf E-Mails mit unerwünschtem oder zweifelhaftem Inhalt, auch nicht, um die Versendung dieser E-Mails abzubestellen.
- Wenn Sie vermuten, dass eine E-Mail nicht legitim ist, nehmen Sie einen Namen oder Text aus der Nachricht und kopieren Sie sie in eine Suchmaschine um zu sehen, ob es bekannte Phishing-Angriffe mit dieser Methode gibt.
- Selbst wenn der Name des Absenders Ihnen bekannt ist: Seien Sie misstrauisch, wenn es jemand ist, mit dem Sie gewöhnlich nicht kommunizieren, vor allem, wenn der Inhalt der E-Mail nichts mit Ihren normalen Arbeitspflichten zu tun hat. Dies gilt auch, wenn Sie in einer E-Mail auf CC gesetzt wurden.
- Lassen Sie sich nicht verführen! In einer E-Mail wird Ihnen ein Angebot gemacht, das zu gut ist, um wahr zu sein. Sie haben z. B. angeblich ein teures Produkt gewonnen (obwohl Sie an keiner Verlosung teilgenommen haben).
- Die Nachricht ist beunruhigend. Seien Sie vorsichtig, wenn in der E-Mail eine intensive oder alarmierende Sprache verwendet wird, die Dringlichkeit vermitteln und Sie dazu bringen soll zu klicken und jetzt zu handeln, bevor Ihr Onlinezugang geschlossen wird oder die Frist in der der Downloadlink funktioniert endet. Denken Sie daran, dass verantwortungsbewusste Organisationen nicht persönliche Daten über das Internet anfordern.
- Wenn Sie aufgefordert werden, sensible Informationen preiszugeben, prüfen Sie, ob die URL der Seite mit HTTPS anstatt nur mit HTTP beginnt. Das „S" steht für „secure" (sicher). Dies ist zwar keine Garantie, dass eine Website legitim ist, aber die meisten legitimen Seiten verwenden HTTPS, weil es sicherer ist. HTTP-Websites, auch legitime, sind anfällig für Angriffe durch Hacker.

Wenn Sie eine E-Mail zugeschickt bekommen haben, bei der Sie vermuten, dass es sich um einen Cyberangriff handelt oder Sie unsicher sind, ob Sie den Anhang der E-Mail gefahrlos öffnen können oder ob Sie auf den Link in der E-Mail gefahrlos klicken können, wenden Sie sich als Mitarbeiter der TU Ilmenau bitte vertrauensvoll an Ihren Systemadministrator.