Bayerisches Staatsministerium
für Unterricht und Kultus

Bayerisches Staatsministerium für Unterricht und Kultus, 80327 München

Per E-Mail

Alle Schulen in Bayern (per OWA)

Ihr Zeichen / Ihre Nachricht vom	Unser Zeichen (bitte bei Antwort angeben)	München, 25.09.2020
	I.3-M7262/63/2	Telefon: 089 2186 2878
		Name: Herr Rapp

Aktuelle Emotet Phishingwelle an bayerischen Schulen

Sehr geehrte Damen und Herren,

seit Anfang September ist verstärkt der Bildungssektor ein neues Ziel dieser Schadcode-Kampagne. Daher sieht das Landesamt für Sicherheit in der Informationstechnik momentan eine erhöhte Gefährdungslage für bayerische Schulen, Universitäten und andere Bildungseinrichtungen.

Die Verteilung des Emotet-Schadcodes erfolgt ausschließlich per Phishing-E-Mail. Die Aufmachung der E-Mails wirkt authentisch und professionell. Emotet liest neben Kontaktbeziehungen auch E-Mail-Inhalte aus Postfächern bereits infizierter Systeme aus und die daraus gewonnenen Informationen werden genutzt, um den Schadcode weiterzuverbreiten.

Hierbei werden verschiedene Varianten hinsichtlich der Aufmachung und Inhalt der Phishing-E-Mails verwendet. Diese Varianten werden fast täglich gewechselt, haben aber im Kern meist folgende Erkennungsmerkmale:

Absender:

- Der Anzeigename der Absender E-Mail-Adresse ist unterschiedlich zu der eigentliche Absender-Adresse
  z.B. „Mustermann, Max (Behörde)“
  <irgendeineSpamAdresse@mail.tld>

Betreff:

- Leere Betreffzeile mit ausschließlich „RE:“: oder „AW:“
- „RE:“ oder „AW:“ + Name des Empfängers
- „RE:“ oder „AW:“ + der Betreff des angehangenen E-Mail-Verlaufs

Telefon: 089 2186 0
Telefax: 089 2186 2800
E-Mail: poststelle@stmuk.bayern.de
Internet: www.km.bayern.de
Salvatorstraße 2 · 80333 München
U3, U4, U5, U6 - Haltestelle Odeonsplatz

Inhalt + Anhang:

- Der eigentliche Phishingtext besteht meist nur aus 1-2 Sätzen, ist sehr allgemein gehalten und bezieht sich kontextfrei auf die vorherige Kommunikation.
- Im Phishingtext wird sehr auffällig auf einen Link oder den Anhang verwiesen
- Meist ist der Anhang ein Word-, Excel-Dokument oder eine Zip-Archiv mit oder ohne Passwortschutz
- Bei einem passwortgeschützten Anhang befindet sich das Kennwort direkt im Phishingtext.

- Der Schadhafte-Link wird meist via HTML durch einen legitim wirkenden Link getarnt
  z.B.
  https://Behörde.xyz.de/DE/Dokumente/0815_April_08_2020.doc

- Der Anzeigename der Absender E-Mail-Adresse oder die Domain des Empfängers ist der Name in der Signatur sowie die E-Mail-Adresse direkt darunter (vgl. Beispiele für typische Phishing-E-Mails)

- Unterhalb des Phishing-Textes wird meist ein zuvor abgegriffener reeller E-Mail-Verlauf hinzugefügt.

Generell kann eine Überprüfung der E-Mails beispielsweise anhand folgendem "3-Sekunden-Sicherheitscheck" vorgenommen werden:

- Ist die Absender-Mailadresse bekannt?
- Weicht die Absender-Adresse vom Anzeigename ab?
- Ist der Betreff sinnvoll?
- Wird zu diesem Zeitpunkt ein Anhang von dieser E-Mail-Adresse erwartet?
- Hat der Inhalt Bezug zum E-Mail-Verlauf?

Melden Sie bitte verdächtige Mails an it-sicherheit@stmuk.bayern.de

Mit freundlichen Grüßen
gez. Christian Rapp
Ressort-Informationssicherheitsbeauftragter des Bayerischen Staatsministeriums für Unterricht und Kultus