Woran kann man verdächtige E-Mails erkennen? [HVF&PH]

14.07.2025 22:53:22

FAQ-Artikel-Ausdruck

Kategorie:	E-Mail & Groupware	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	14:26:13 - 26.06.2020

Schlüsselwörter

E-Mail Spam Viren Phishing

Symptom (öffentlich)

Wer sich im Internet bewegt kann leicht zum Angriffsziel von Betrügern und Hackern werden. Die meisten Angriffsversuche finden per E-Mail statt. Um ein Ziel zu werden kann es schon reichen, wenn eine E-Mail-Adresse auf einer Webseite steht, man in einer E-Mail als Mitempfänger angegeben wird oder aber wenn jemand mit dem man sonst in Kontakt steht, das Adressbuch des Mobiltelefons in einer unsicheren App hochlädt. Ist die eigene E-Mail-Adresse erst einmal auf den Listen von Betrügern gelandet, lässt sich dies nicht wieder umkehren und es ist sehr wahrscheinlich, dass die Adressen auch an weitere Missetäter weitergegeben/veräußert werden.

Problem (öffentlich)

Die Gefahren die entstehen können verschiedenster Art sein. Dies kann das Abfischen (Phishing) von Login-Daten sein, die böswillige Verschlüsselung der Daten um Entschlüsselungsgeld zu erpressen (Ransomware), Datendiebstahl, die Einbindung in ein maliziöses Botnet (auch Zombies genannt) oder es kann ganz anderen Zwecken dienen.

Manche dieser Nachrichten enthalten schadhafte Dateien wie Virenprogramme oder auch Office-Dokumente die Virenprogramme beim Öffnen nachträglich aus dem Internet laden. Andere verweisen auf Internetseiten auf denen man sich bei einer vermeintlich freundlichen Seite (Banken, Webmail, etc) anmelden kann um dadurch an Login-Daten zu kommen. Ganz andere erwarten, dass man in Kommunikation mit dem Absender tritt, sei es im Rahmen einer Partnersuche/-vermittlung oder um zu helfen ein Vermögen in ein sicheres Land zu transferieren, wofür man zur Begleichung von Gebühren einen geringeren Betrag überweisen soll (Vorschussbetrug).

In der Regel handelt es sich bei so etwas um Massenangriffe, was es leichter macht diese zu erkennen.

Das MIT und die Partner des MIT betreiben diverse Sicherungsmechanismen, um zu verhindern, dass betrügerische E-Mails bei Ihnen, den Empfängern, ankommen. Leider ändern sich die Betrugsmaschen, die verwendeten Texte und die Absenderadressen ständig, so dass leider nicht jeder Betrugsversuch automatisch erkannt und herausgefiltert werden kann.

Lösung (öffentlich)

Die letzte und wichtigste Schutzbarriere sitzt vor dem Bildschirm!

Meist lässt sich eine verdächtige E-Mail schon am Inhalt erkennen. Seltsamer Schreibstil, schlechte Grammatik und Orthografie, eine falsche oder ungewöhnliche Anrede bzw. Grußformel oder ein Text der einfach schlecht übersetzt wirkt, sind deutliche Anzeichen dafür, dass etwas nicht stimmen kann.

Der Absender einer E-Mail liefert meist auch eindeutige Hinweise. Oftmals ist es so, dass der angezeigte Name und die E-Mail-Adresse nichts miteinander zu tun haben. So könnte der angezeigte Name „IT-Support“ sein, die verwendete E-Mail-Adresse aber „fremder.name@gmail.com“. In manchen E-Mail-Programmen ist dies leicht zu erkennen, da Anzeigename und E-Mail-Adresse zusammen angezeigt werden. In anderen E-Mail-Programmen muss man mit der Maus über dem Absender schweben oder den Namen anklicken um die verwendete E-Mail-Adresse zu sehen.

Oftmals fordern diese E-Mails zu einem schnellen Handeln auf, z.B. aufgrund einer Umstellung der Systeme. Wenn das MIT eine größere Umstellung plant, welche die Mitarbeit der Nutzer*innen erfordert, werden wir darüber über die üblichen Hochschulkanäle mit zeitlichem Abstand vorab informieren und dies auch auf der Homepage ankündigen. Eine Ausnahme hierbei bilden die Mails die zur regelmäßigen Passwortänderung auffordern. Um sicher zu gehen, dass man die richtigen Methoden verwendet, kann man statt den Anweisungen in den E-Mails auch einfach den in den FAQ beschriebenen Wegen folgen (Passwortänderung für die [1]HVF und [2]PH).

Wenn Webseiten verlinkt sind, sollte man diese Adressen genau anschauen. Hierfür kann man mit der Maus über dem Link schweben, worauf die tatsächlich verlinkte Adresse (meist) im unteren Bereich des Mailprogramms bzw. Browsers angezeigt wird. So könnte es sein, dass ein Angreifer vortäuscht einen Link auf https//service.campus-lb.de/ zu verwenden, der aber eigentlich zu https//service.campus-lb.de--virenschleuder.xyz/ verweist.

Wer unsicher ist, kann eine verdächtige E-Mail gerne an das MIT weiterleiten. Wir prüfen diese dann und melden unsere Einschätzung zurück.

Weitere ausführliche Informationen findet man auf:
- [3]https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/Phishing_E-Mails_erkennen/wie-erkenne-ich-phishing-e-mails_node.html

- [4]https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073

- [5]https://bleib-wachsam.de/

[1] https://service.campus-lb.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=13
[2] https://service.campus-lb.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=3
[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/Phishing_E-Mails_erkennen/wie-erkenne-ich-phishing-e-mails_node.html
[4] https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/merkmale-einer-phishingmail-6073
[5] https://bleib-wachsam.de/