Gute Mails, böse Mails

Gefahrloser Umgang mit E-Mails

Bild: Andreas Martini

Gefährliche Mails sollte man nicht öffnen – aber ob eine Mail harmlos ist oder nicht, weiß man oft erst, nachdem man sie geöffnet hat. Und manchmal nicht mal dann. Damit Sie trotzdem nicht in die Phishing-Falle tappen, müssen Sie ein paar Sicherheitsvorkehrungen treffen, die wir Ihnen hier geben.

Von Ronald Eikenberg

E-Mails zu öffnen ist wie Russisch Roulette – man weiß nie, ob es knallt. Meist hat man keine Wahl, ob man mitspielen möchte. Versuchen Sie doch mal, Ihrem Chef zu erklären, dass Sie ab sofort keine E-Mails mehr öffnen. Schlagkräftige Argument hätten Sie zuhauf: E-Mails sind gefährlich und der wichtigste Verbreitungsweg für Schädlinge. Allein die berüchtigte, hauptsächlich per Phishing-Mail verbreitete Emotet-Malware hat weltweit unzählige Unternehmen, Behörden, Krankenhäuser & Co. lahmgelegt und dabei Schäden in Milliardenhöhe angerichtet.

Ein weiteres Argument ist, dass Sie Ihrem Chef nicht versprechen können, dass Sie alle Phishing-Mails aussortieren und nicht darauf reinfallen. Denn die Zeiten, in denen man solche Mails schon von Weitem erkennen konnte, sind längst vorbei. Angreifer nutzen immer häufiger echte – gestohlene – Daten, um Sie in die Falle zu locken, zum Beispiel plausible Absender, mit denen Sie bereits Kontakt hatten. Phishing-Mails zitieren mitunter sogar aus vorangegangenen Mailwechseln mit Kollegen, Partnerfirmen oder Kunden.

Zwickmühle E-Mail

Wer beruflich mit Mails arbeitet, muss nicht selten Dutzende oder gar Hunderte davon Tag für Tag bearbeiten – und genauso viele Entscheidungen treffen. Das ist ganz schön viel Verantwortung, denn jede Fehlentscheidung, jeder falsche Klick kann die ganze Firma über Wochen lahmlegen. Die Krux ist, dass man es sich aber auch nicht leisten kann, eine Kundenanfrage oder eine Auftragsmail zu übersehen. Jede Mail muss daher gecheckt werden.

Sie ahnen es vielleicht bereits: Auch mit den besten Argumenten kommen Sie aus der Nummer nicht raus. E-Mail ist der kleinste gemeinsame Nenner bei der Online-Kommunikation und daher weiterhin unverzichtbar. Die interne Kommunikation kann man inzwischen gut über moderne Kollaborationssoftware wie Rocket.Chat, Slack oder Teams abwickeln, für die Kommunikation mit der Außenwelt gibt es jedoch keinen Ersatz mit breiter Akzeptanz.

Im Privatleben sieht es ähnlich aus: Freunde und Verwandte können Sie problemlos über Messenger-Apps wie WhatsApp oder Signal erreichen – Ende-zu-Ende-verschlüsselt nach Stand der Technik und mit überprüfbarem Absender. Für die Kontaktaufnahme mit Firmen, Behörden und vielen mehr müssen Sie jedoch oft noch eine Mail schreiben. Rechnungen, Versandbestätigungen, Benachrichtigungen über verdächtige Aktivitäten et cetera landen in Ihrem Posteingang, neben Phishing-Mails aller Art. Und es bleibt an Ihnen hängen, die guten Mails von den bösen zu unterscheiden.

Phishing auf den zweiten Blick: Mittlerweile muss man genau hinsehen, um die Rechtschreibfehler von Online-Ganoven zu finden. In der Anrede wird hier sogar ein bisschen gegendert.

Aber was tun? Phishing zählt zur Angriffskategorie „Social Engineering" – die Angreifer zielen also nicht auf technische Sicherheitslücken ab, sondern auf die Schwachstelle Mensch. Genau hier setzen die folgenden Artikel an: Wir möchten Ihnen das nötige Wissen und einige praktische Tipps an die Hand geben, damit Sie leicht die Spreu vom Weizen trennen können und für Phishing-Mails nur noch ein müdes Lächeln übrig haben.

Mails entschärfen

Es geht nicht nur darum, wie Sie verdächtige Mails anhand offensichtlicher und versteckter Merkmale bewerten können (siehe S. 18), sondern auch um die kniffligen Fälle. Manchmal bleiben auch nach einer eingehenden Prüfung Restzweifel, ob es sich um Spreu oder Weizen handelt und ob die angehängte Datei unentbehrlich ist oder ernstzunehmenden Schaden anrichtet.

In solchen Fällen können Sie den Anhang vor dem Öffnen mit einem Tool wie Dangerzone entschärfen, indem Sie ein harmloses PDF daraus machen – garantiert ohne Office-Makros. Oder Sie analysieren die Datei mit speziellen Tools, um vorab gefahrlos zu überprüfen, ob sich darin Makros oder eingebettete Dateien verstecken (siehe S. 28).

Wir möchten Sie dazu anregen, dieses Wissen auch mit Kollegen, Freunden, Familie und Geschäftspartnern zu teilen – in ihrem eigenen Interesse. Denn den größten Einfluss auf Ihren Posteingang haben nicht Sie, sondern die Absender der Mails. Wenn jeder die wichtigsten Dos & Don'ts kennt und beim Verschicken beherzigt, wird E-Mail für alle sicherer.

Wir haben die wichtigsten Tipps für den Mailversand daher als kompakte und leicht verdauliche Checkliste auf Seite 26 zusammengestellt. Die Checkliste ist online frei abrufbar, damit Sie sie leicht weitergeben können. Wenn Sie mögen, können Sie in Ihrer Mailsignatur darauf verweisen: ***https://ct.de/sicher-mailen***

(rei@ct.de) c't