Bei den Schutzmaßnahmen muss man sich auch vor Augen halten, dass etwa eine Milliarde Viren und andere Schadprogramme bekannt sind und täglich mehrere hunderttausend neu entdeckt werden.

Antivirenprogramme reagieren auf bekannte Viren. Beim Durchsuchen von Daten werden verdächtige Codes mit einer umfangreichen Datenbank bekannter Schadprogramme abgeglichen. Gibt es einen Treffer, schlägt das Programm Alarm und blockiert die weitere Ausführung des Schadprogramms. Das bedeutet, ein Antivirenprogramm ist nur gut, wenn die dahinterliegende Datenbank auf dem neuesten Stand ist. Daher müssen die Hersteller von Antivirenprogrammen ihre Datenbanken täglich mit den neuen Schadsignaturen ergänzen und die Antivirenprogramme aktualisieren. Trotzdem besteht immer die Gefahr, dass ganz neue Schädlinge nicht erkannt werden.

TIPP

Wie können Sie sich schützen? Wir greifen hier auf Empfehlungen der deutschen Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) (siehe Adressen/Links) zurück:

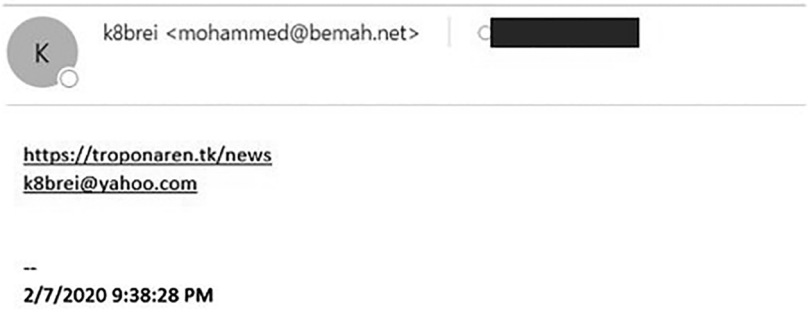
- ➜ Nutzen Sie Virenschutz-Software und führen Sie automatische Updates durch.
- ➜ Laden Sie/kaufen Sie Virenscanner nur bei vertrauenswürdigen Anbietern.
- ➜ Löschen Sie verdächtige E-Mails, das ist immer ohne Gefahr möglich. Verdächtig sind E-Mails, wenn sie Folgendes aufweisen:
  - Unbekannter Absender mit Sonderzeichen in der Adresse
  - Unbekannter Absender ohne Betreff
  - Unbekannter Absender, verwendet Englisch oder eine andere Fremdsprache
  - Unbekannter Absender, der die Mail an „Recipients“ etc., d.h. nicht an Sie persönlich versendet hat
- ➜ Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass ein Script nicht automatisch ausgeführt wird.
- ➜ Öffnen Sie niemals eine ZIP-Datei, die Sie von einem unbekannten Absender erhalten haben. Bei ZIP-Dateien von einem bekannten Absender fragen Sie ggfs. nach, was der Inhalt ist.

- ➜ Öffnen Sie keine ausführbare Datei, die Sie an Endungen wie „.exe“, „.bat“, „.com“ oder „.vbs“ erkennen, ungeprüft. Fragen Sie im Zweifelsfall beim Absender nach.
- ➜ Seien Sie vorsichtig im Umgang mit HTML-E-Mails.
- ➜ Versenden Sie selbst auch keine Anhänge, die Sie aus unsicheren Quellen haben.

Mails mit Links zu schädlichen Webseiten

BEISPIEL

Katharina Li bekam einen Anruf von einem guten Freund: „Du, dein E-Mail-Account wurde gehackt. Bitte warne alle deine Kontakte.“ Im Nachgang schickte ihr Freund auch das fragliche E-Mail:



Was war geschehen? Katharina hatte ihrerseits von einem Freund eine E-Mail ähnlichen Inhalts und Aussehens erhalten – und aufgrund des bekannten Namens auch den Link angeklickt und sich hierdurch infiziert, Schadsoftware auf ihren Computer geladen. Und diese Schadsoftware verschickt seitdem an die Adressen in ihrem Mail-Adressbuch diese Mails.

Eine andere Masche von Betrügern ist es, ihre Mail einem aktuellen Thema zu widmen, z.B.: „So schützen Sie sich gegen das Coronavirus“, „Die ersten

Unfallbilder von Michael Schumacher“. Diese sollen einen seriöseren Eindruck vermitteln, den Leser neugierig machen und dazu verleiten, die Mail und anschließend auch den Link zu öffnen.

TIPP

Schützen können Sie sich gegen diese Art von Mails durch ein gesundes Misstrauen. Wir gehen hierbei kurz auf einige Punkte der konkreten Mail ein, die Sie stutzig machen sollten:

Absender

Den Absender in Klarschrift (hier: „K8brei“) kennen Sie und vertrauen ihm. Dieser erscheint auch in der Mailliste. Gehen Sie jedoch in die Mail, so sehen Sie auch den Absender, der oft nicht gefälscht wird. In diesem Fall ist dies mohammed@bemah.net, der mit dem scheinbaren Absender wahrscheinlich nichts gemein hat.

Betreffzeile

Zumeist ist diese leer. Entspricht es der Gewohnheit Ihres Bekannten, Ihnen eine Mail ohne Betreff zu schicken? Oder ist der Betreff sehr reißerisch und soll Sie neugierig machen?

Inhalt der Mail

In der Mail befindet sich nur ein Link zu einer Webseite. Keine Anrede, kein Text, kein freundliches Wort vom Absender, keine Unterschrift. Entspricht es der Gewohnheit Ihres Vertrauten, Ihnen eine Mail ohne jede Freundlichkeitsformel zu senden?

Bei auch nur geringstem Misstrauen sollten Sie den Link in dieser Mail nicht anklicken! Greifen Sie lieber zum Telefon und fragen Sie nach, was es mit der Mail auf sich hat.

Möchten Sie Ihr Wissen über und Ihre Widerstandskraft gegen Spam-Mails testen? Dann können Sie dies mit einem kostenlosen Test bei der SoSafe GmbH in Köln über das Internet machen: https://phish-test.de/. Sie erhalten dann drei so genannte Phishing-Mails, jedoch ohne gefährlichen Inhalt. Verhalten Sie sich bei diesen Mails falsch, indem Sie z.B. den Link öffnen, so kommen Sie auf eine Lernseite, auf der Ihnen Ihr Fehler erklärt wird.

Und so sieht hoffentlich auch Ihr Ergebnis nach dem Test aus:

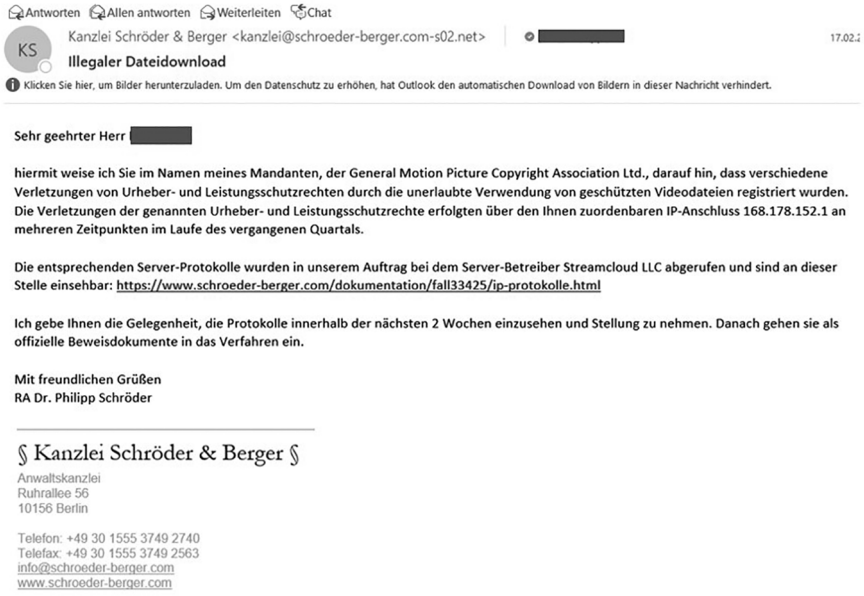
Haben Sie die Mails alle erkannt? Oder sind Sie uns auch einmal "ins Netz gegangen"? So haben Sie abgeschnitten:

Versendete E-Mails:	Schwierigkeitslevel:	Ergebnis:
Anwalt illegaler Download	Leicht	Nicht geklickt
Neues TAN Verfahren	Mittel	Nicht geklickt
Schenkung	Schwer	Nicht geklickt

Haben Sie vielen Dank für Ihre Teilnahme an dieser Aktion.

Sie wollen auch Ihre Freunde, Familie oder Kollegen auf unsere Aktion aufmerksam machen? Dann teilen Sie den Link zu www.phish-test.de doch sehr gerne in den von Ihnen genutzten sozialen Netzwerken - und helfen Sie uns dabei, alle zum Thema Phishing aufzuklären!

Da es sich bei Mails mit einem schädlichen Link um ein für Betrüger besonders interessantes Thema zu handeln scheint, bringen wir ein weiteres Beispiel:



Antworten Allen antworten Weiterleiten Chat

KS Kanzlei Schröder & Berger <kanzlei@schroeder-berger.com-s02.net> [redacted] 17.02.

Illegaler Dateidownload

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Sehr geehrter Herr [redacted]

hiermit weise ich Sie im Namen meines Mandanten, der General Motion Picture Copyright Association Ltd., darauf hin, dass verschiedene Verletzungen von Urheber- und Leistungsschutzrechten durch die unerlaubte Verwendung von geschützten Videodateien registriert wurden. Die Verletzungen der genannten Urheber- und Leistungsschutzrechte erfolgten über den Ihnen zuordenbaren IP-Anschluss 168.178.152.1 an mehreren Zeitpunkten im Laufe des vergangenen Quartals.

Die entsprechenden Server-Protokolle wurden in unserem Auftrag bei dem Server-Betreiber Streamcloud LLC abgerufen und sind an dieser Stelle einsehbar: https://www.schroeder-berger.com/dokumentation/fall33425/ip-protokolle.html

Ich gebe Ihnen die Gelegenheit, die Protokolle innerhalb der nächsten 2 Wochen einzusehen und Stellung zu nehmen. Danach gehen sie als offizielle Beweisdokumente in das Verfahren ein.

Mit freundlichen Grüßen
RA Dr. Philipp Schröder

§ Kanzlei Schröder & Berger §
Anwaltskanzlei
Ruhrallee 56
10156 Berlin

Telefon: +49 30 1555 3749 2740
Telefax: +49 30 1555 3749 2563
info@schroeder-berger.com
www.schroeder-berger.com

Sie werden also von einem Anwalt aus Berlin angeschrieben, der Ihnen illegalen Video-Download vorwirft. Nun, wer hat sich in youtube.com nicht schon einmal Videos angesehen? Aber diese sollen illegal sein? Noch unter Schock stehend wollen Sie sich die Beweise des Anwalts ansehen.

TIPP

Nun, das sollten Sie nicht so schnell tun! Denn es könnte sich auch um eine geschickte Falle handeln:

- ➜ Anwälte versenden ihre Mahnschreiben per Post und nicht per E-Mail!
- ➜ Die Rechtsanwaltskanzlei muss nicht echt sein:
  - Geben Sie die Homepage der Kanzlei in Ihren Browser ein (nicht kopieren). In diesem Fall wird die Homepage nicht gefunden.
  - Geben Sie den Namen der Kanzlei bei der zuständigen Rechtsanwaltskammer ein, in diesem Fall bei der Rechtsanwaltskammer Berlin (www.rak-berlin.de). Auch hier wird die Kanzlei nicht gefunden!
- ➜ Fahren Sie mit dem Cursor leicht (nicht anklicken!) über den angegebenen Link. Sie sehen hier eine andere Adresse, die mit der Klarschrift nichts zu tun hat.

Ergebnis: Dies ist eine Fälschung (Fake-Mail) mit einem Link, der Sie mit hoher Wahrscheinlichkeit zu einer schädlichen Seite führt. Finger weg!

Die zweitgrößte Gefahr neben den Mails mit versautem Anhang, sich ein Schadprogramm einzufangen, besteht beim Surfen im Netz. Allein durch den Besuch einer manipulierten Webseite kann Ihr Computer mit einem Schadprogramm infiziert werden (Fachbegriff: „Drive-By-Infektion"). Dabei kann es sich durchaus auch um seriöse und vielbesuchte Seiten handeln, die unbemerkt für betrügerische Zwecke missbraucht werden.

Wie kann das passieren? Der Computernutzer ruft eine Internetseite auf. Für Betroffene ist nicht erkennbar, dass die Seite manipuliert ist. Heimlich wird ein Programm auf den Opfer-Computer geladen, das den Rechner auf Schwachstellen untersucht. Die gesammelten Daten werden genutzt, um