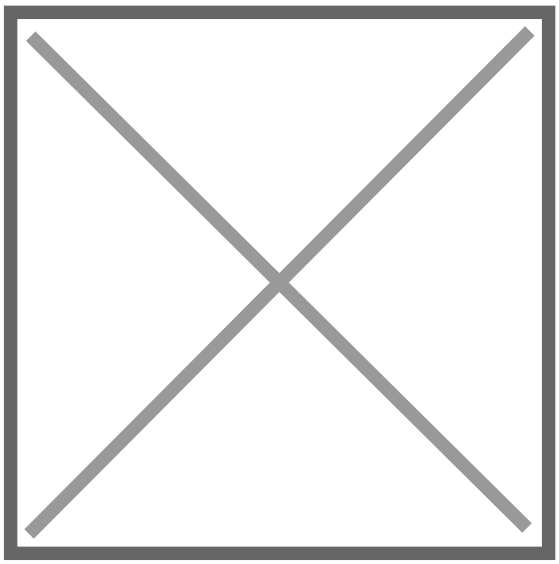
Virustotal

- Verdächtige Datei oder Link mit Virustotal überprüfen

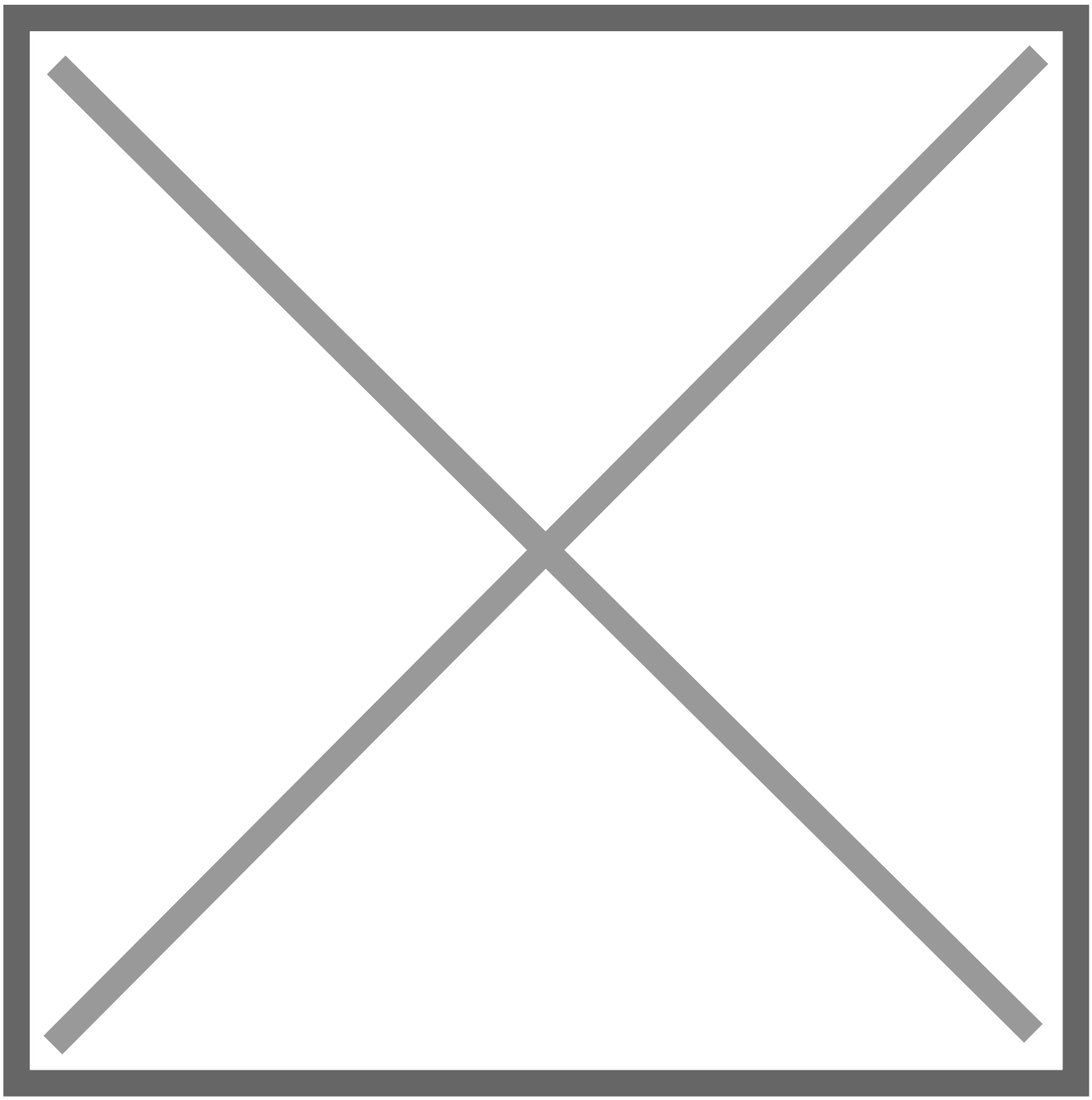
Verdächtige Datei oder Link mit Virustotal überprüfen

1 In Ihrem Postfach finden Sie eine verdächtige Email mit einem Anhang. Sie wollen überprüfen ob der Anhang Schadsoftware enthält und ob Sie den Anhang gefahrlos öffnen dürfen. Die folgenden Schritte zeigen wie Sie relativ einfach diesen Anhang überprüfen können.

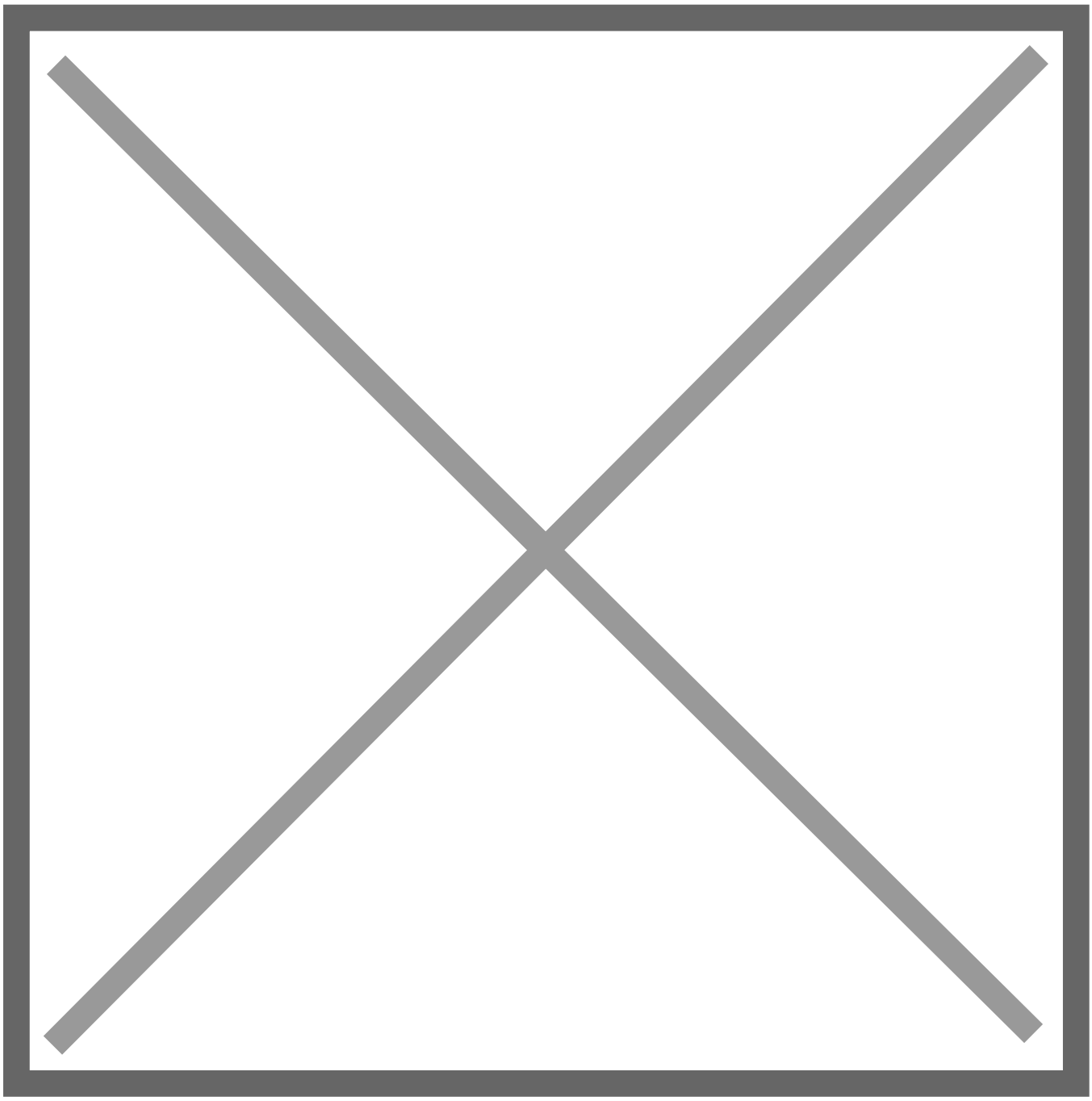


Damit wird sichergestellt dass eine potentiell gefährliche Datei aus dem Emailanhang immer im gleichen Ordner abgespeichert wird und nicht unkontrolliert irgendwo auf dem Rechner.

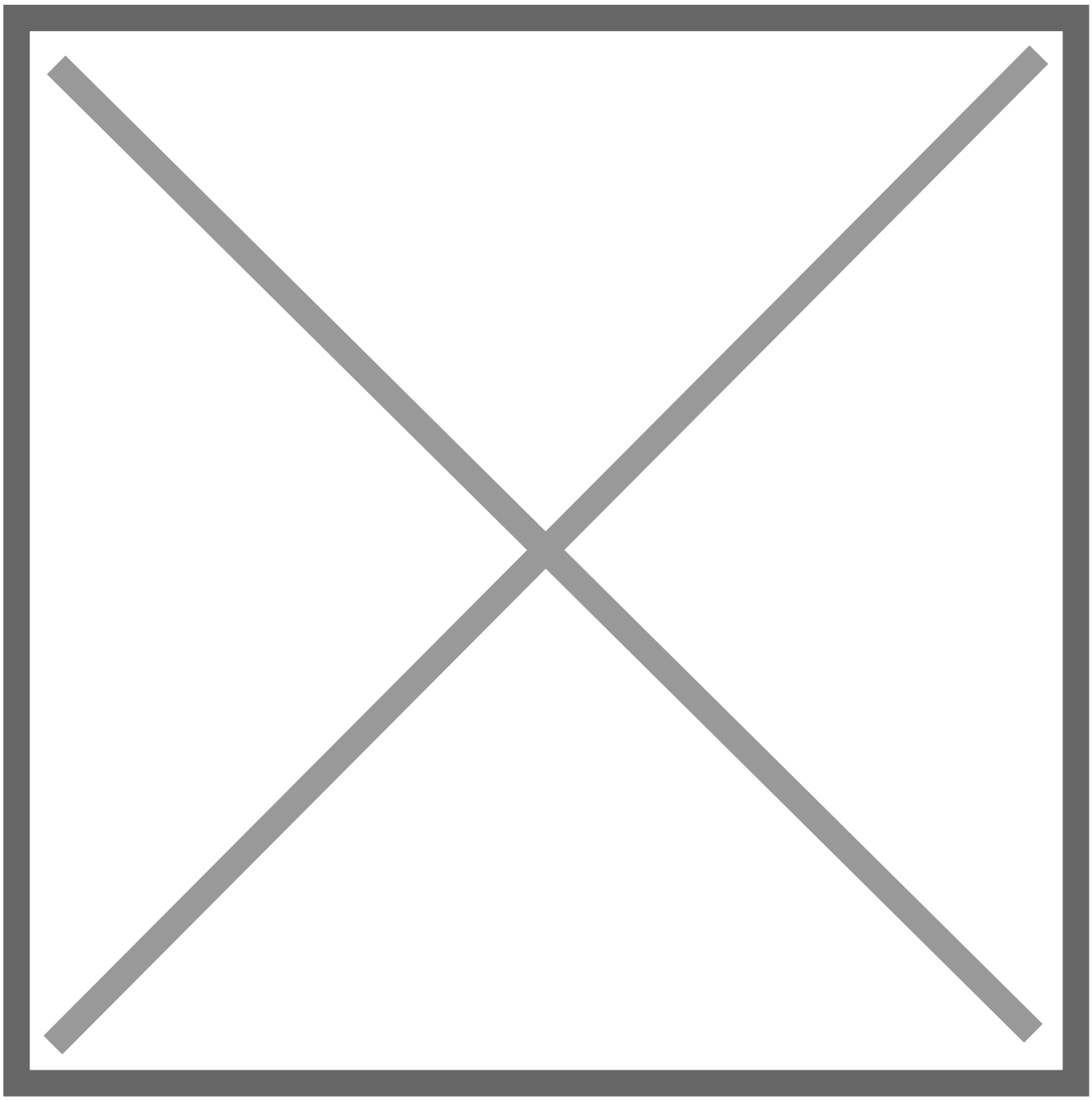
2 Markieren Sie die Email sodass diese im rechten Fenster im Outlook angezeigt wird



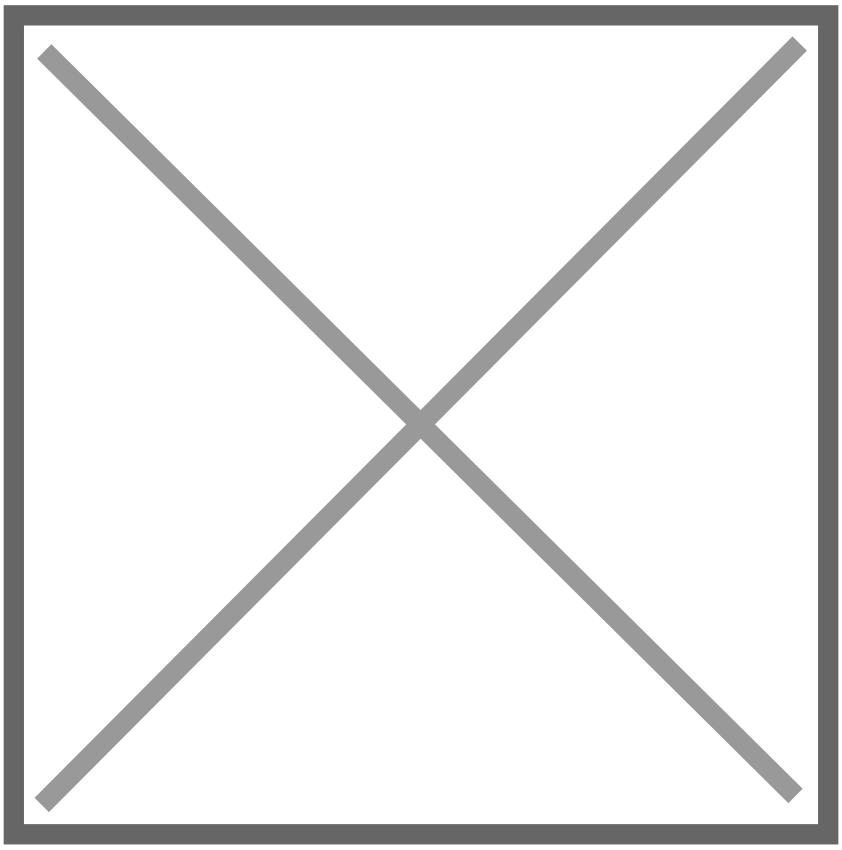
3 Speichern Sie den Anhang, hier die pdf-Datei Antrag.pdf, auf Ihrem Rechner. Dazu markieren Sie den Anhang nur 1 Mal mit der rechten Maustaste (ACHTUNG: Den Anhang **NIEMALS** doppelklicken ansonsten öffnen Sie die Datei was wir ja unbedingt verhindern wollen) und wählen im Kontextmenü «Speichern unter» an:



und als Speicherort wählen Sie den Ordner «VIRUS» den Sie unter Punkt 1 erstellt haben und klicken auf «Speichern»



Wenn Sie den Ordner «VIRUS» öffnen dann sehen Sie die von Ihnen abgespeicherte Datei. Auch hier gilt wieder dass Sie diese Datei unter keinen Umständen öffnen!



4 Öffnen Sie nun einen Browser (Internet Explorer, Firefox oder Chrome) und geben Sie ein:

www.virustotal.com

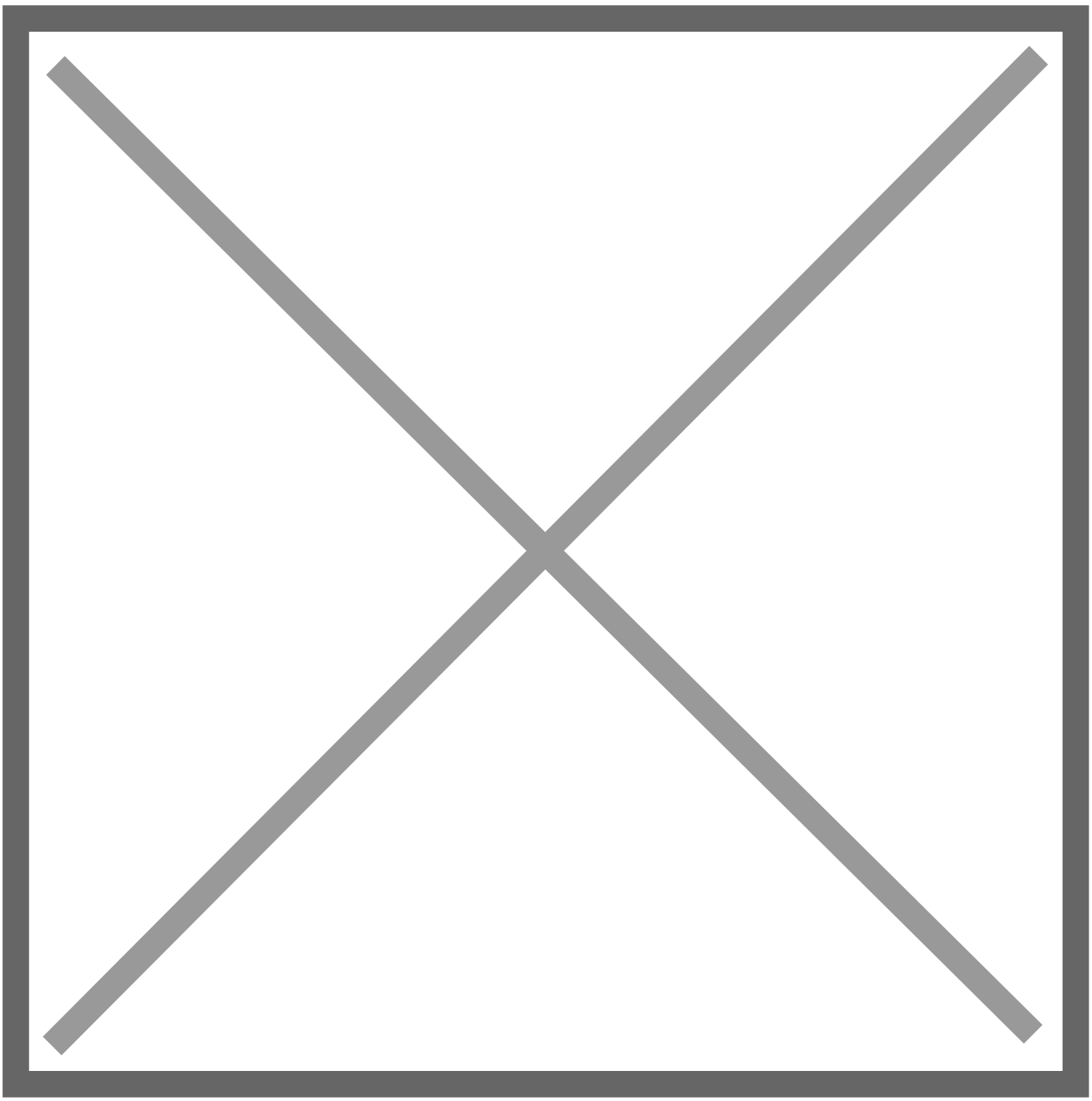
Sie gelangen auf die Webseite von Virustotal. Diese stellt verschiedene Dienste zur Verfügung:

a) Sie können eine verdächtige Datei raufladen welche von ca. 60 verschiedenen Antiviren-Scannern auf Schad-Software überprüft wird

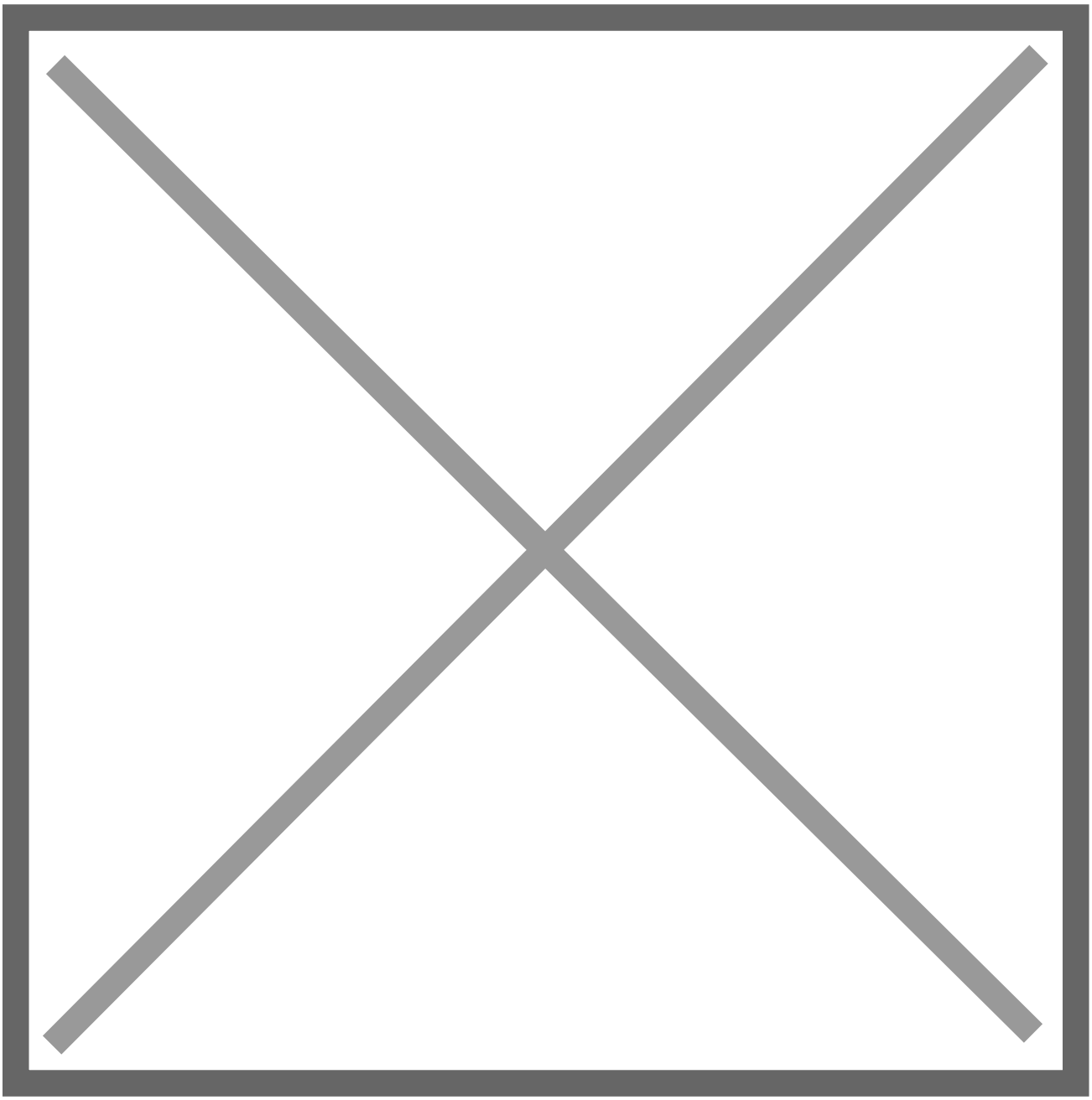
b) Sie können einen verdächtigen Link, welcher hauptsächlich in verdächtigen Emails eingebettet ist (z.B. UPS oder DHL Sendungen), zur Analyse raufladen (URL). Virustotal untersucht die von diesem Link

aufrufbare Webseite auf Virus-Risiken

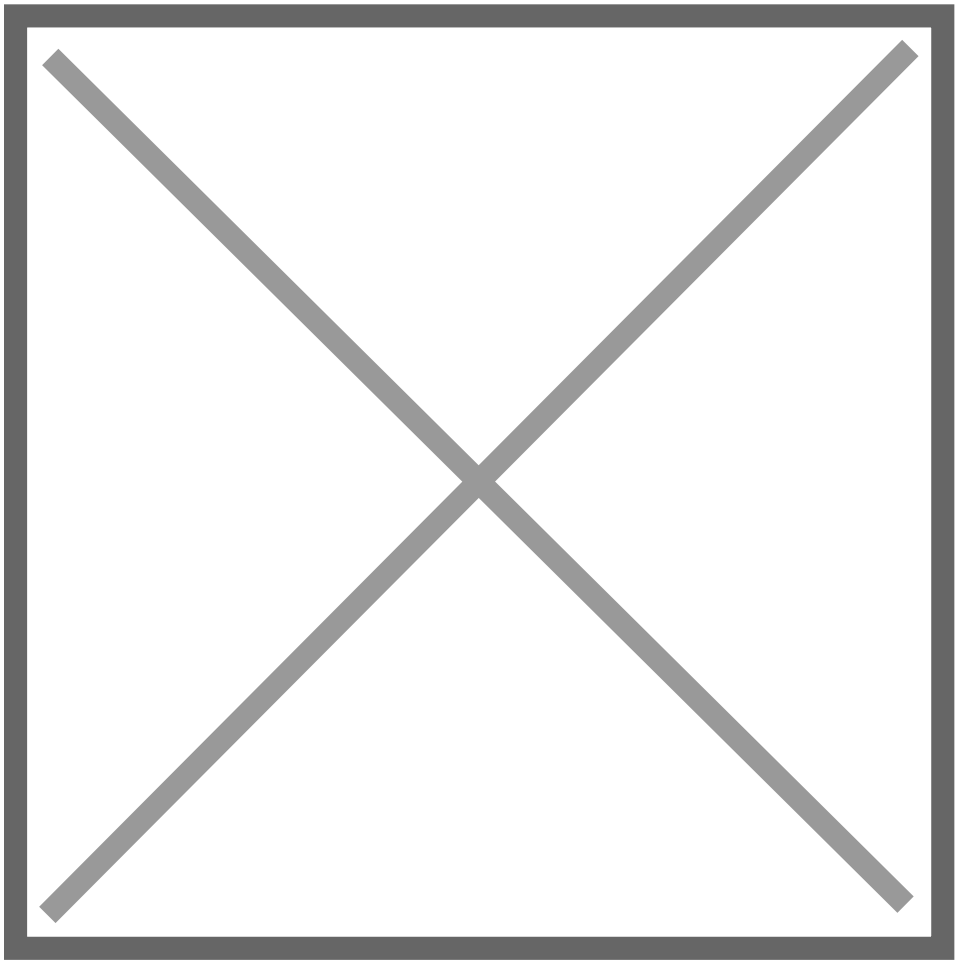
Wir wollen jetzt nur a) die verdächtige Datei «Antrag.pdf» mit virustotal.com überprüfen. Dazu klicken Sie auf File (rot markiert) und klicken danach auf «Choose file»



und markieren im Ordner «VIRUS» die Datei «Antrag.pdf» aus und bestätigen durch «Öffnen». Der Ausdruck «Öffnen» im unteren Bild bezieht sich nur darauf, dass die markierte Datei zum Upload auf virustotal.com ausgewählt wird. Damit wird die Datei aber nicht ausgeführt – was wir ja auch nicht wollen



Bevor die Datei nun auf virustotal.com raufgeladen wird erscheint eventuell noch ein Bestätigungs-fenster. Hier klicken Sie auf «OK»:



5 Analyse der Datei auf Schadsoftware

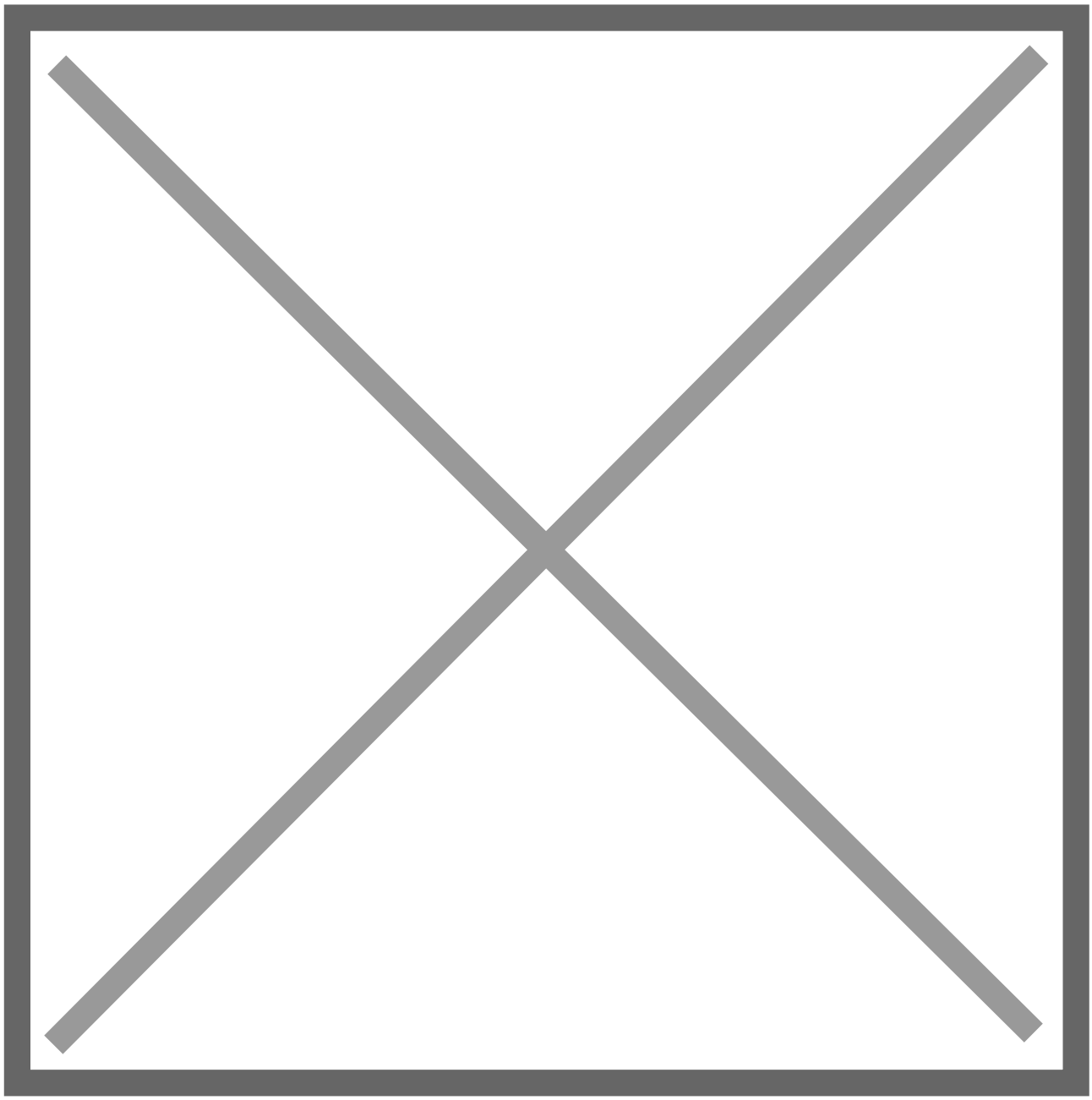
Die Datei wird nun von mehr als 50 verschiedenen Antiviren-Scannern überprüft. Dabei gibt es zwei mögliche Resultate:

- die Datei ist höchstwahrscheinlich sauber

- die Datei ist «verseucht»

5.1 Die Datei ist höchstwahrscheinlich sauber:

Alle Antiviren-Scanner zeigen überall grüne Häkchen. Das bedeutet dass kein Scanner eine Bedrohung in dieser Datei gefunden hat. Man kann somit mit grosser Wahrscheinlichkeit davon ausgehen dass die Datei virenfrei ist:



WICHTIG:

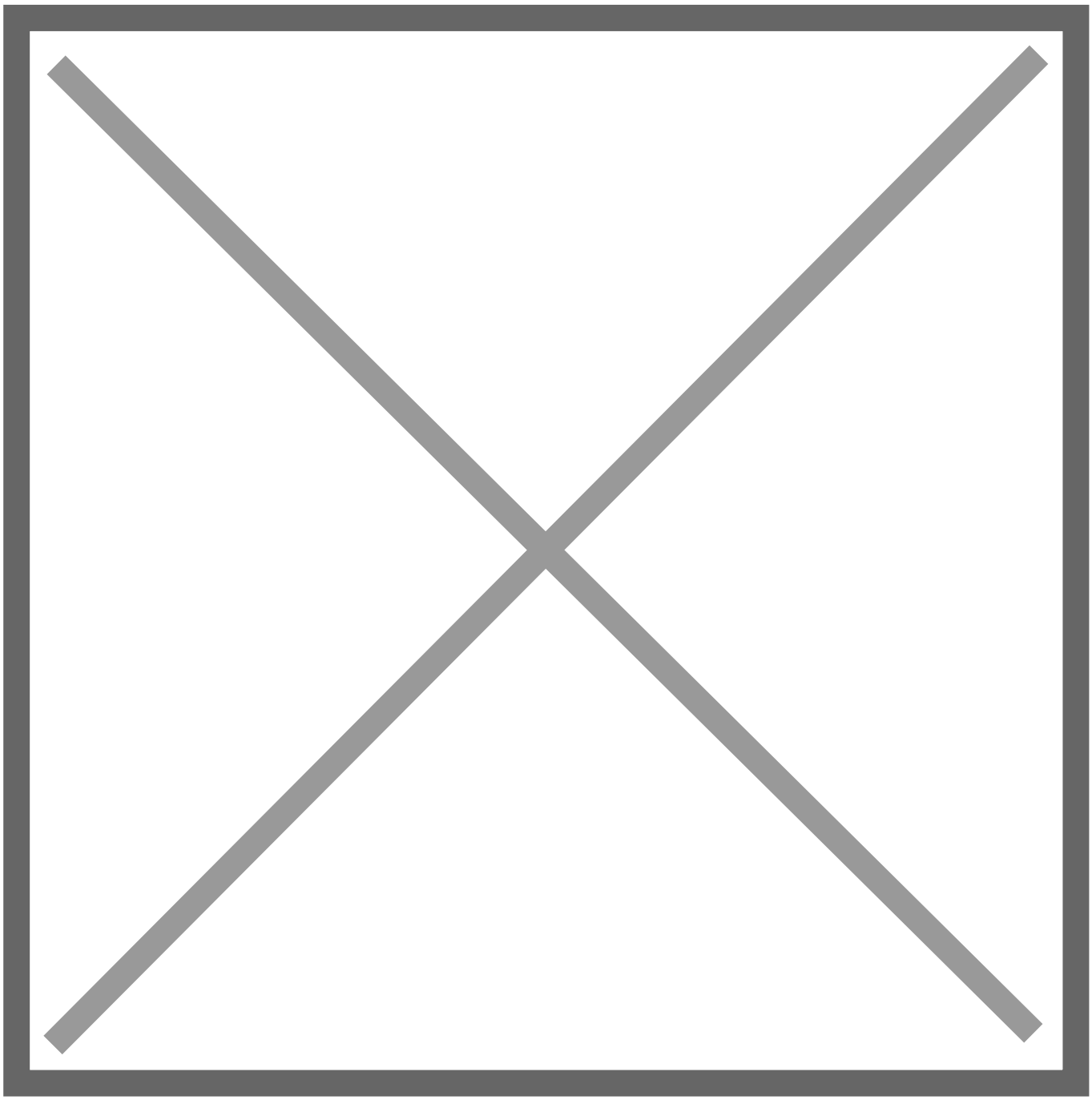
Eine absolute Garantie dass die Datei virenfrei ist gibt es jedoch nicht: Da täglich Tausende von neuen Viren und Trojanern in Umlauf gebracht werden ist es möglich dass die Antiviren-Scanner diese zum jetzigen Zeitpunkt noch nicht erkennen und die Datei fälschlicherweise als virenfrei bezeichnen.

Deshalb empfehlen wir grundsätzlich mindestens noch einen oder zwei Tage abzuwarten und den Analyse-Vorgang unter Punkt 4 nochmals zu wiederholen. Nach dieser Zeit haben die Antiviren-Scanner ihre Erkennungs-Datenbank aktualisiert und das Analyse-Resultat der Datei ist dann sehr zuverlässig.

Wird die Datei nach einer Analyse nach zwei Tagen immer noch als virenfrei bezeichnet können Sie die Datei öffnen. Die Datei im Ordner «VIRUS» kann danach gelöscht werden.

5.2 Die Datei ist «verseucht»:

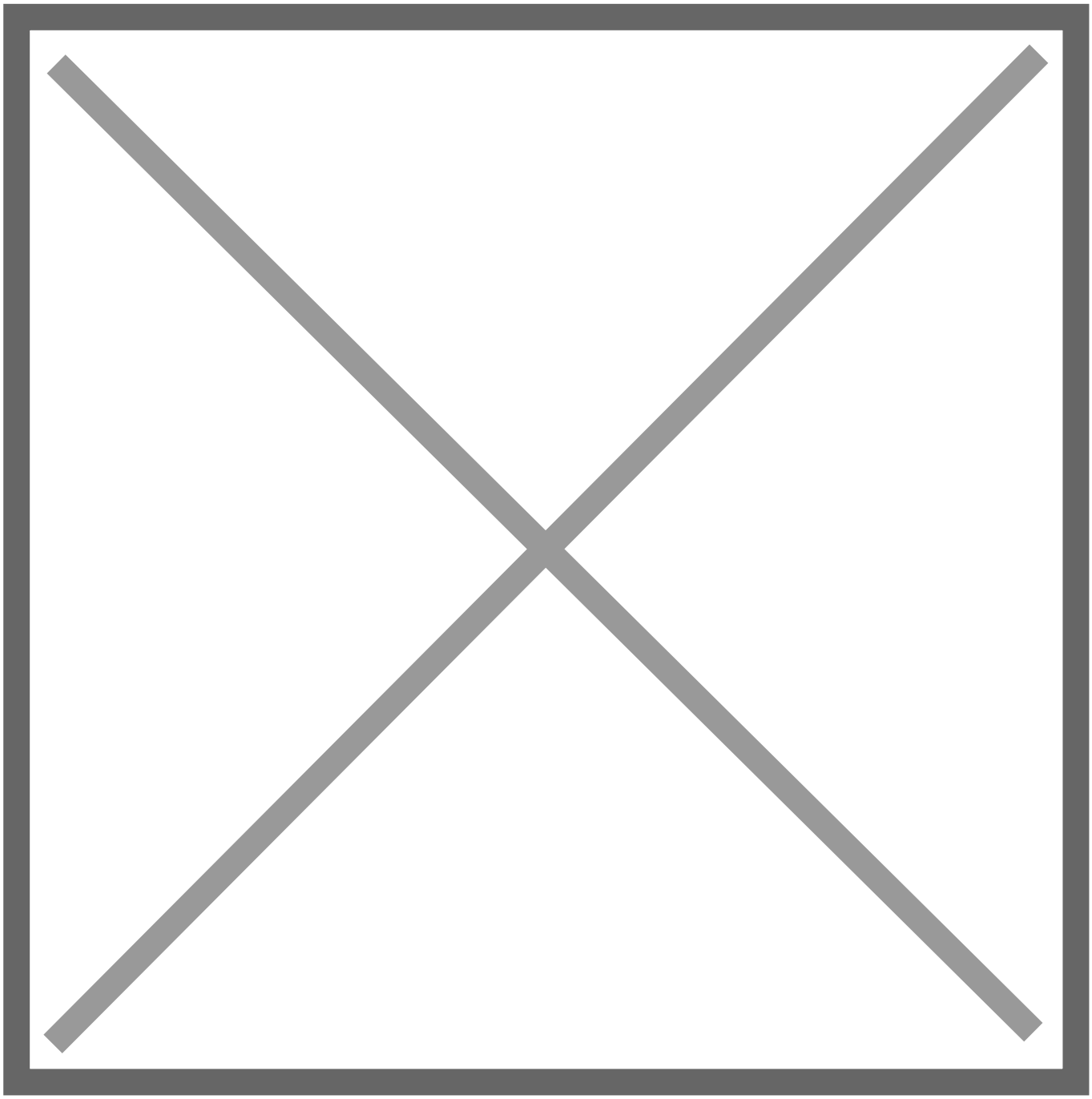
Einer oder mehrere der Antiviren-Scanner zeigen eine Bedrohung durch diese Datei an:



In diesem Fall muss das Email und die Datei im Ordner «VIRUS» sofort gelöscht werden oder rufen Sie uns an unter 071 929 29 59

Löschen Sie dieses Emails im Postfach => Das Email wird in den Ordner «Gelöschte Elemente» verschoben

Klicken Sie mit der rechten Maustaste auf «Gelöschte Elemente» und dann auf «Ordner leeren»



Löschen Sie die Datei im Ordner «VIRUS». Die Datei wandert dann in den Papierkorb

Leeren Sie den Inhalt des Papierkorbs auf dem Desktop: