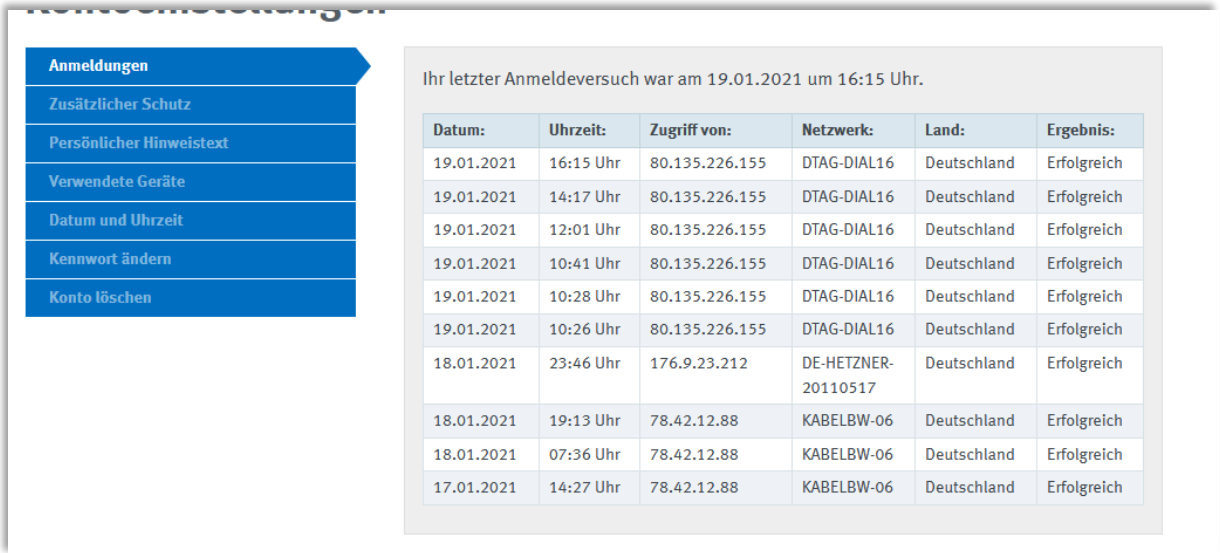
Polizeipräsidium Mannheim
Kriminalpolizeidirektion Heidelberg
z.Hd. Thomas Wacker
Kriminalinspektion 5 / Dezernat 5.1 – Ermittlungen Cybercrime
Römerstraße 2 – 4, 69091 Heidelberg

Neckargemünd, 05.02.2021

Anzeige wegen Angriffen auf Fritzboxen unserer Kunden in unserem MyFritz Konto.

Am 18.1.2021 habe ich abends noch einige Kundenaufträge von zu Hause aus abgearbeitet. Hierzu habe ich mich mit meinem Tablett bei MyFritz eingeloggt. Mir ist aufgefallen, dass der Login beim ersten Mal nicht funktioniert hat. Ich bin jedoch davon ausgegangen, dass ich mein Passwort falsch eingegeben habe. Daraufhin habe ich die Passworteingabe wiederholt und kam so auf die Übersicht der Kundengeräte in unserem MyFritz Konto. Das Einloggen auf der Kunden FRITZ!Box hat dann wiederum ohne Probleme geklappt.
Später habe ich das Login bei MyFritz überprüft und festgestellt, dass es am selben Abend einen weiteren erfolgreichen Zugriff auf unser MyFritz Konto von einer mir nicht bekannten IP-Adresse gab. Hierbei handelt es sich um eine IP-Adresse von Hetzer (176.9.23.212 am 18. Januar 2021 um 23:46).



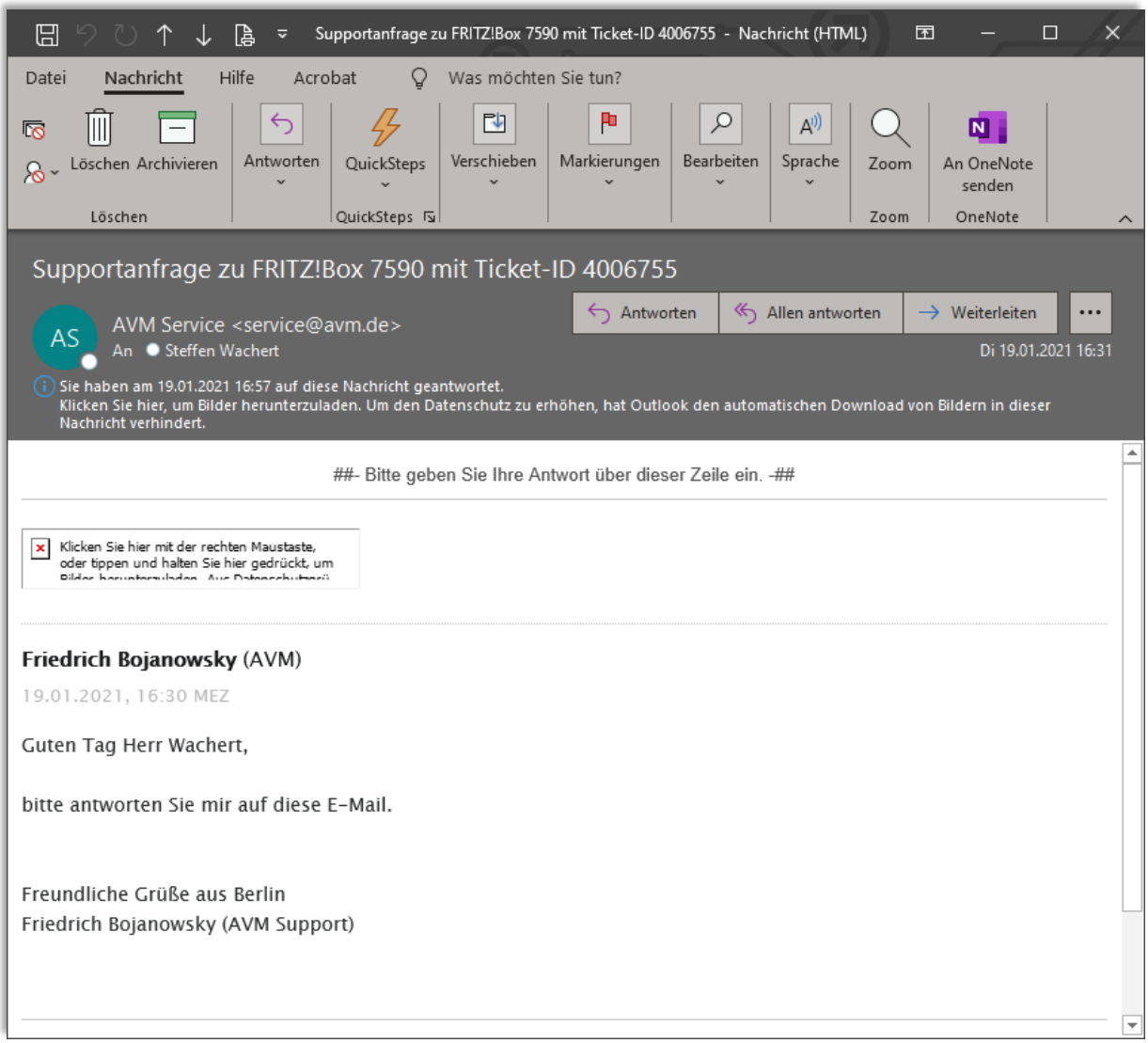
Datum:	Uhrzeit:	Zugriff von:	Netzwerk:	Land:	Ergebnis:
19.01.2021	16:15 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
19.01.2021	14:17 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
19.01.2021	12:01 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
19.01.2021	10:41 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
19.01.2021	10:28 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
19.01.2021	10:26 Uhr	80.135.226.155	DTAG-DIAL16	Deutschland	Erfolgreich
18.01.2021	23:46 Uhr	176.9.23.212	DE-HETZNER-20110517	Deutschland	Erfolgreich
18.01.2021	19:13 Uhr	78.42.12.88	KABELBW-06	Deutschland	Erfolgreich
18.01.2021	07:36 Uhr	78.42.12.88	KABELBW-06	Deutschland	Erfolgreich
17.01.2021	14:27 Uhr	78.42.12.88	KABELBW-06	Deutschland	Erfolgreich

Daraufhin habe ich direkt das Passwort zu unserem MyFritz Zugang geändert.

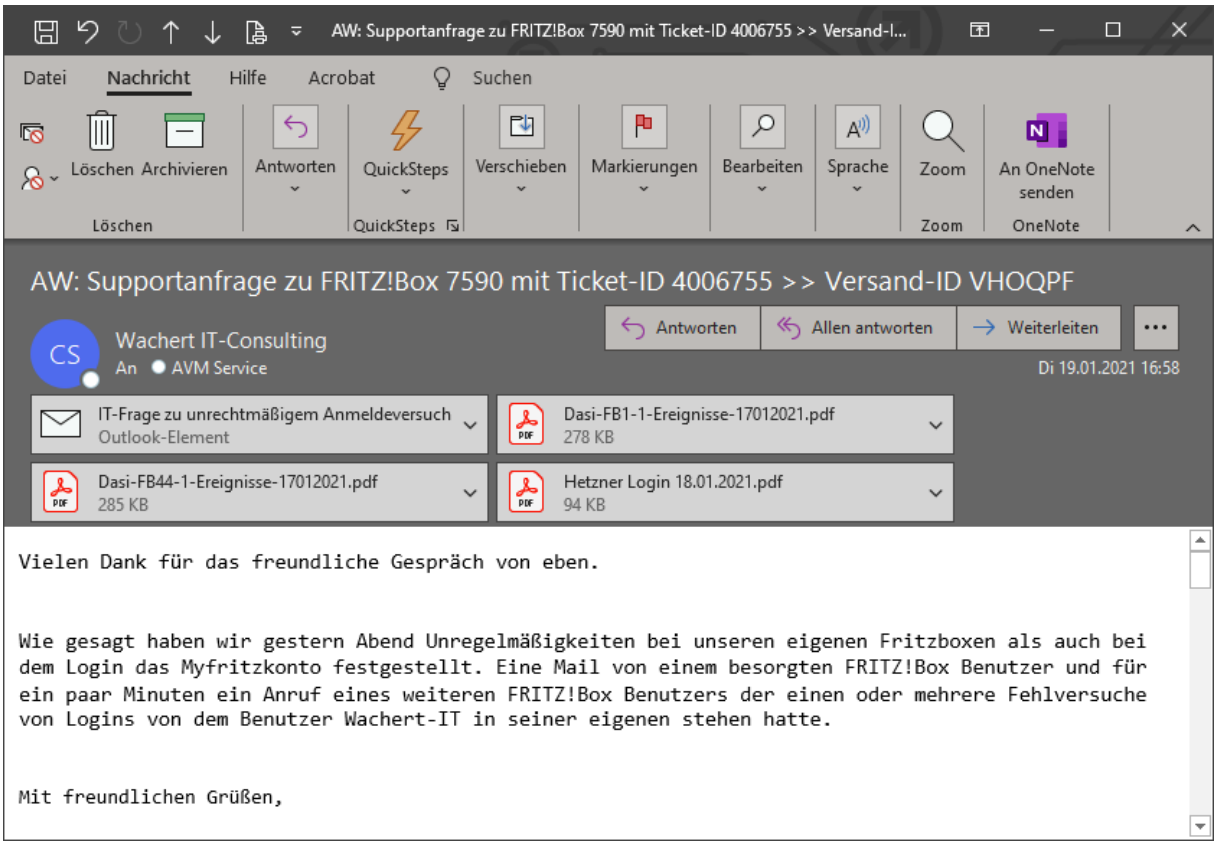
Über diesen Vorgang habe ich AVM direkt am nächsten Tag informiert. Am Telefon wurde mir versichert, dass keine Unregelmäßigkeiten vorliegen würden. Ich hatte dem Kollegen jedoch gesagt, dass ich zu dem Zeitpunkt (18.01.2021 23:46 Uhr) nicht eingeloggt war.

Wir gehen davon aus, dass zu dem Zeitpunkt meines ersten Logins am 18.01.2021 ein Redirect Hack auf die myfritz.net Seite erfolgte.

Von AVM habe ich daraufhin und 16:31 Uhr folgende Mail bekommen:



die ich sogleich mit den gewünschten Daten und Screenshots und 16:58 Uhr beantwortet.

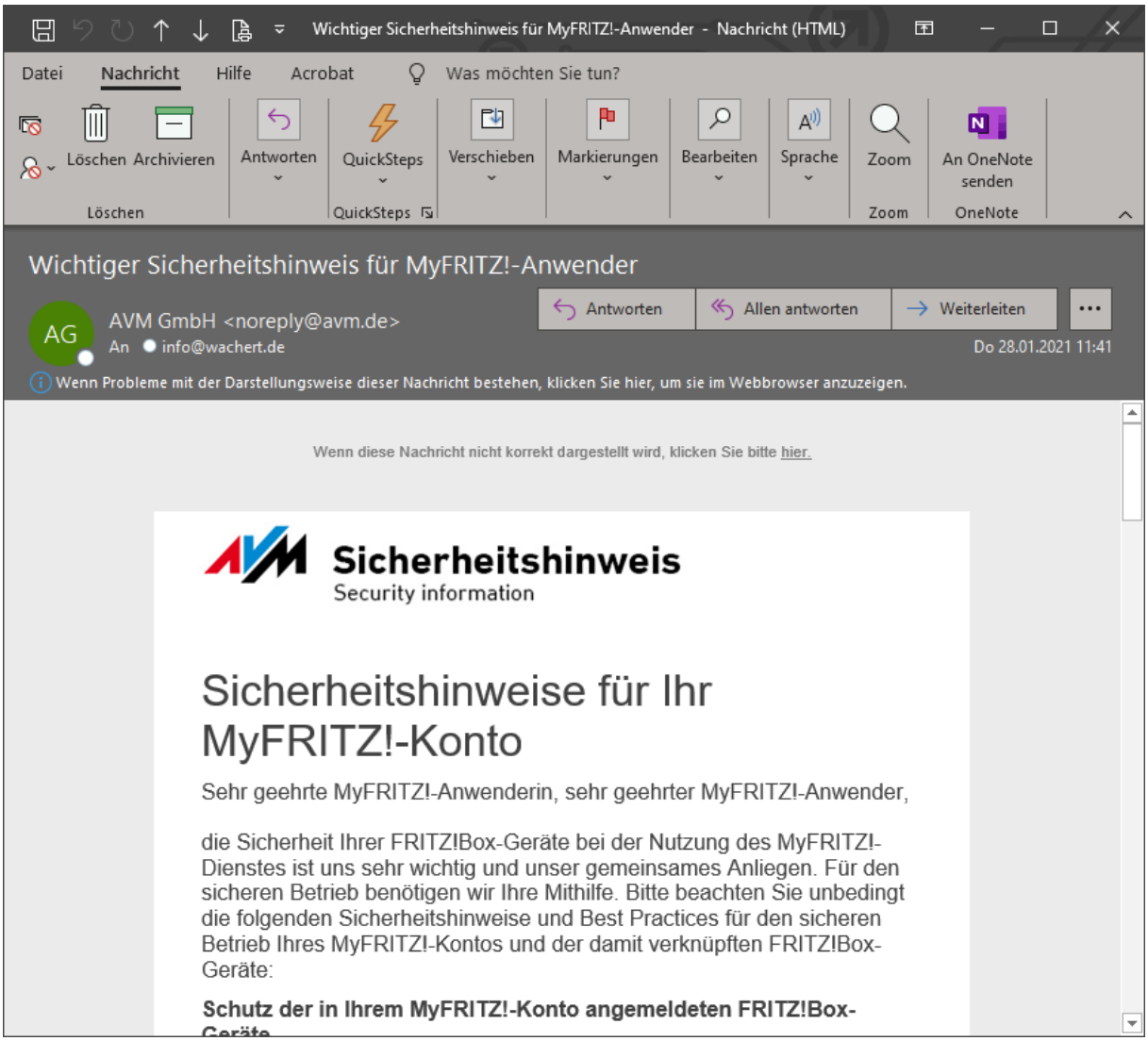


Da unser Login in das MyFritz **Konto** ein anderes ist als unser Standardlogin in die Kunden Fritzboxen, wollte ich zunächst die Reaktion von AVM auf meine E-Mail vom 19. Januar um 16:58 Uhr abwarten.

Es folgten einige weitere Telefonate mit dem AVM Support. Man bat mich Geduld zu haben und die Auswertung abzuwarten.

Nun bekam ich in dieser Woche zwischen dem 28.01.21 und dem 29.01.2021 zwei Telefonate von FRITZ!Box Benutzern die nicht bei uns Kunde sind. Sie wollten wissen warum wir versucht hätten uns bei Ihnen in die FRITZ!Box einzuwählen. Der Benutzer wäre hier Wachert IT gewesen. Ich habe den Anrufern mitgeteilt, dass wir natürlich nicht versucht hatten uns in Ihre FRITZ!Box einzuloggen.

Am 28. Januar um 11:41 Uhr bekam ich nun eine sehr allgemein gehaltene und nicht auf das Ticket 4006755 bezogene E-Mail von AVM die mir allerdings erst am 29.01.2021 aufgefallen ist. Diese Mail enthielt einige Sicherheitshinweise zum MyFritz **Konto.**



Nachdem mich am 29.01.2021 noch dazu unser Kunde [redacted] anrief um mir mitzuteilen, dass die Telekom seine Auslands Gespräche gesperrt hat, war mir klar, dass ich die Reaktion von AVM nicht abwarten konnte. AVM habe ich darüber informiert.

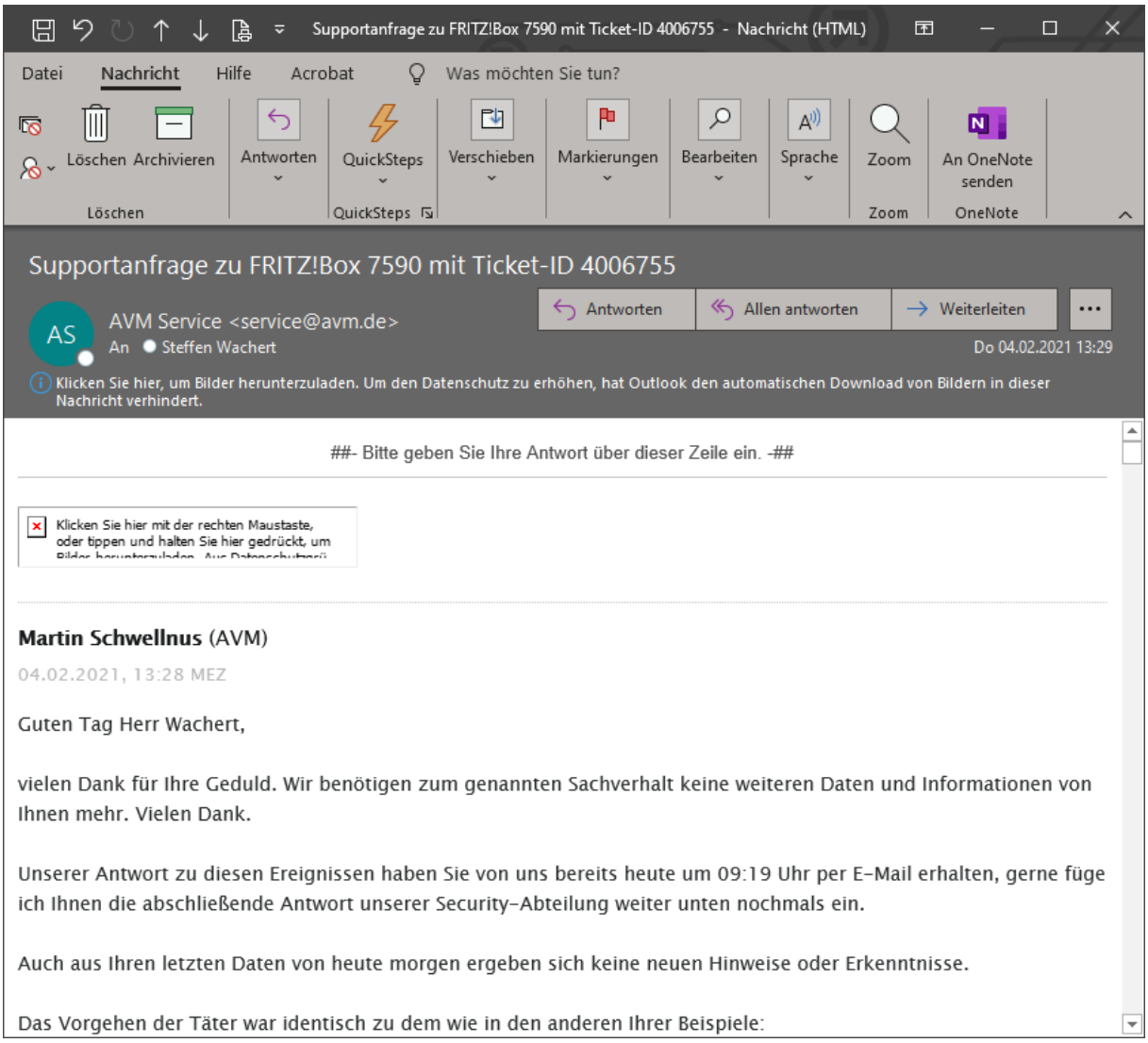
Am Samstag den 30.01.21 habe ich dann direkt damit angefangen mich nach Alphabet bei allen Kunden Fritzboxen, auf die wir Zugriff haben, einzuloggen und ein neues individuelles Passwort zu vergeben. Ebenfalls habe ich geprüft ob die Gesprächsliste gelöscht wurde und ob es eventuelle verdächtige IP Telefone gibt, die der Kunde nicht selbst angelegt hat. Diese habe ich gelöscht. Ebenso habe ich die Gesprächsdatenliste, sofern diese erkennbare Anrufe ins Ausland hatte gesichert. Ebenso habe ich die Systemmeldungen durchgesehen um festzustellen, ob es hier verdächtige Logins oder Loginversuche gab.
Eine entsprechend Liste der Betroffenen Fritzboxkunden füge ich dieser Anzeige an.

Ich habe nun durchgängig von Samstag bis Sonntagnacht um ca. 3 Uhr alle Boxen von unseren Kunden entsprechend ändern können.

Direkt am darauffolgenden Dienstag den 02.02.2021 haben wir angefangen allen entsprechenden Kunden die Veränderungen an ihrer FRITZ!Box per Mail oder per Post mitzuteilen. Es handelt sich um insgesamt 228 Fritzboxen die jedoch vermutlich nur zu ca. 20-30 % kontaminiert waren. Wir haben vorsichtshalber alle 228 Boxen entsprechend durchgeschaut und die Passwörter geändert.

Es folgten weitere Telefonate mit besorgten Kunden. Ebenso folgten mehrere Telefonate mit AVM wie weiter vorgegangen werden soll. Vor allem im Hinblick darauf, wie das MyFritz Passwort von uns abgegriffen worden sein könnte.

Die Reaktion von AVM kam am Donnerstag den 4. Februar um 13:29 Uhr per E-Mail:



Direkt nach dem Lesen dieser E-Mail habe ich bei der Kripo in Mannheim angerufen und den Vorfall gemeldet. Seitdem stehen wir in Kontakt.

Sollte diese Anzeige nicht ausführlich genug sein, werde ich natürlich gerne die eventuell fehlenden Informationen nachliefern.

Mit freundlichen Grüßen,

Steffen Wachert