Hallo Herr Beisecker und KollegenInnen,

unser Notebook (Windows 7) haben wir mit Ihrem PC-Sicherheits-Berater, Special-Edition 2017 überprüft. Aktueller Anlass für diese Prüfung war ein uns eigenartig vorkommendes Verhalten des Notebooks:

- Nach dem Hochfahren (Starten) des Notebooks waren auf dem Desktop, entgegen der vorherigen Anordnung, 2 komplette Spalten Icons leer. Die Icons, die vorher in diesen Spalten waren, befanden sich nun verteilt an anderen Stellen des Desktops. (Es kam auch früher schon mal vor, dass einige Icons anders angeordnet wurden, aber nicht, dass ungefähr in der Mitte des Desktops 2 Spalten ohne Icons sind, also vollständig leer wurden.)

- Ohne, dass bei G DATA von mir eine Aktion gestartet war, „blitzte“ es in zwei Fällen (kurz) rot auf, mit „sinngemäßen Meldungen: Rechner gefährdet“. Diese Meldungen verschwanden aber sofort wieder – und kamen auch nicht noch einmal vor.

- Auf dem Notebook ist eine Mini-Anwendung zur Anzeige der Auslastung des Rechners installiert. Diese zeigte (ohne besondere Aktivitäten von mir) plötzlich 100% an, was ich bisher in dieser Höhe noch nie beobachtet habe!

Wir haben also die Überprüfung des Notebooks mit Ihrem „Ihr PC-Sicherheits-Berater, Special-Edition 2017“ begonnen. Bisher haben wir die Kontrollschritte 1 bis 4 durchgeführt, siehe die folgende Zusammenfassung mit Ergebnissen und Fragen dazu:

- **Kontrollschritt 1:** Notebook im abgesicherten Modus starten

- **Kontrollschritt 2:** Entfernen potentieller Schadprogramme in Windows, Scan mit dem Tool Kaspersky **TDSSKiller**, Ergebnis: no threads found

- **Kontrollschritt 3:** Stoppen verdächtiger Schadprogramm-Prozesse, Scann mit **Rkill**
  *Bemerkung: Das Tool Rkill habe ich auf Ihrer DVD nicht gefunden (wahrscheinlich wg. der Vielzahl der Tools dort übersehen). Deshalb habe ich danach „gegoogelt“ und das bei CHIP gefundene **Rkill** benutzt. In dieser Version fehlt im* **Meldungs-Check** *– entgegen zum* **Meldungs-Check** *in Ihrer Anleitung „***Checking Windows Service Integrity” (!), so dass dieses hier nicht überprüft werden kann!**
  Das Ergebnis der von uns durchgeführten Prüfung - mit dem Dateinamen **Rkill** - siehe im **Attachment**.

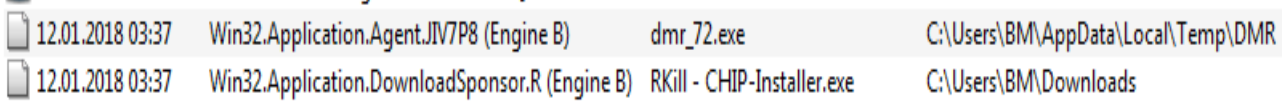
  Das Ergebnis bei **Checking for processes to terminate**: hat abweichend von Ihrem „Muster-Ergebnis für ***keine*** *Gefahr*“, bei uns die Meldung: **1 proccess terminated**
  Nach meinem Verständnis deutet das auf eine Gefahr hin. Deshalb hierzu meine Fragen:
  I. a) Wie bewerten Sie diese Meldung?

I. b) Deutet diese Meldung auf ein Leck in der Sicherheit hin? Welche Maßnahmen sind erforderlich?

II. Können Sie mir einen Link zu *Ihrer* Quelle für das Tool **Rkill** senden, bei dem auch **Checking Windows Service Integrity** enthalten ist, damit wir auch dafür die Prüfung durchführen können?

- **Kontrollschritt 4:** Den Rechner mit G DATA scannen
  Dabei wurden 2 Dateien als Bedrohung festgestellt und wie vorgeschlagen desinfiziert und in Quarantäne genommen. Hierzu das Bildschirm-Foto:

In Quarantäne:



- III. Wie kann man klären, ob es sich dabei tatsächlich um **schädliche** Dateien – oder *nur* um nicht erkannte **harmlose** Dateien handelt?

Wir sind jetzt schon sehr beunruhigt. Bisher haben wir die ersten vier Kontrollschritte durchgeführt und warten jetzt auf Ihre Beurteilung.

- IV. Ist ein „Weitermachen“ mit den Kontrollschritten 5, ... angebracht – oder müssen andere Schritte erfolgen?

Freundliche Grüße von BenutzerIin