Conference FSTD / DGAC
16 décembre 2015

Risque viral dans les logiciels de simulation.
Description d'un cas réel

présenté par
Laurent COMBES
FSTD CMM – Airbus S.A.S

AIRBUS

Description de l'évènement

- Samedi 20 Octobre 2012: Sur un simulateur FFS CAE Convertible A330/A340 opéré dans le centre d'entraînement de Toulouse, de gros problèmes sur les FMS sont détectés.
- La maintenance simulateur détecte un blocage du PC simulation FMGEC
- Le Simulateur est stoppé et s'avère inutilisable après de nombreuses tentatives de relance.

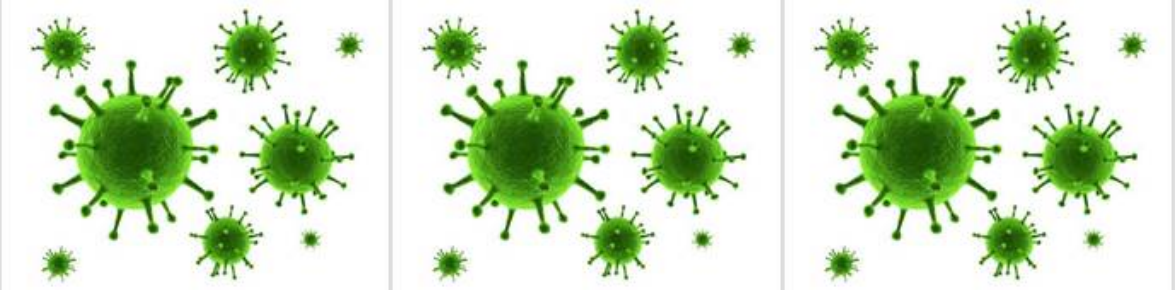
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Description de l'évènement

- Une longue analyse permet finalement de comprendre qu'un virus infecte un ou plusieurs PCs du réseau interne du simulateur.

Evénement totalement inédit dans l'histoire du centre.

- Le nettoyage et la remise en état de la simulation s'avère très long et complexe, le virus ré-infectant la machine après chaque relance.



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Conséquences

- L'Autorité Compétente est informée de l'arrêt du simulateur comme le prévoit le Manuel de Surveillance de Conformité FSTD.
- De nombreuses ressources sont nécessaires pour s'assurer de l'éradication du virus à la fois sur les machines mais aussi sur le réseau interne Airbus.
- 20 sessions de FFS sont annulées.
- Perte financière conséquente pour le centre.
- Impact client.

- Le retour à la normale n'intervient que le 23 Octobre 2012, l'information est transmise à l'Autorité Compétente.
- Des actions sont lancées auprès des fabricants de simulateur ainsi qu'en interne pour éviter la ré-occurrence ou tout du moins, diminuer le risque.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Analyse du problème

- Nous avons été victimes en fait d'un virus sur le Réseau informatique interne d'Airbus (Intranet).

Ce type de virus *("Confiker")*, se propage sur internet et sur les réseaux intranet afin de s'installer sur le plus de PCs possible dans le but de créer un réseau de PCs *"zombies"* , permettant par la suite des attaques à distance pour récupérer des données.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Analyse du problème

- Les simulateurs de vol sont reliés au réseau interne Airbus dans le but de pouvoir faire de la maintenance à distance et de procurer un accès depuis le bureau à notre service d'ingénierie.
- Les pannes simulateurs sont en fait, provoquées par des surcharges du traffic sur le réseau simulateur, dues à la duplication du virus lui-même afin d'infecter un maximum de PCs connectés au réseau.
- L'attaque virale n'était pas ciblée.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

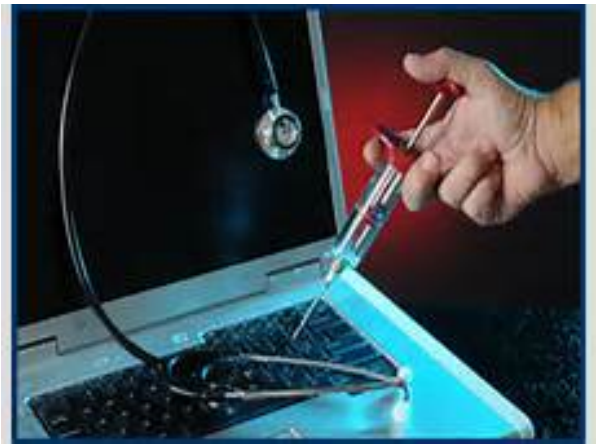
Analyse du problème

- En plus de notre FFS A330/A340, des FFS A320 (Thales) ont été également touchés par l'attaque.
- Impact moins grand sur ces machines A320 de type *Reality 7* qui s'avéraient utilisables une fois lancées. La configuration n'étant pas la même que sur le simulateur A330/A340: Utilisation d'un réseau à fibre optique dédié. La faille se trouvait seulement dans le fait que la *"Debriefing Station"* de ces machines A320 avait été reliée au réseau interne Airbus pour dialoguer avec le simulateur.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Correction du problème

- Les FFS ont été totalement déconnectés du réseau interne Airbus
- Nettoyage du réseau
- Nettoyage de tous les PCs simulateurs
- Vérification des Back-ups
- Sessions de test FFS réalisées avant la remise en service des simulateurs pour l'entraînement.



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

Diminution du risque

- Simulateurs A320: Modification de cablage des *“Debriefing Stations”*
- Simulateur A330/A340: Installation d’un Routeur additionnel avec un *Pare-Feu* intégré
- Action d’envergure lancée par les services informatique Réseau Airbus

- Mise en place de procédures de sécurité:
  - Clefs USB dédiées pour la maintenance (Chargement de données, téléchargement de Tests QTG, etc.). Passage à l’antivirus systématique.
  - Passage à l’antivirus des PCs simulation au besoin (suspicion quelconque)
  - Mise en place d’un outil de vérification du traffic réseau simulateur.
  - Respect strict des procédures de *Back-up* des logiciels de simulation.

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS

Prise en compte dans le SGS Airbus

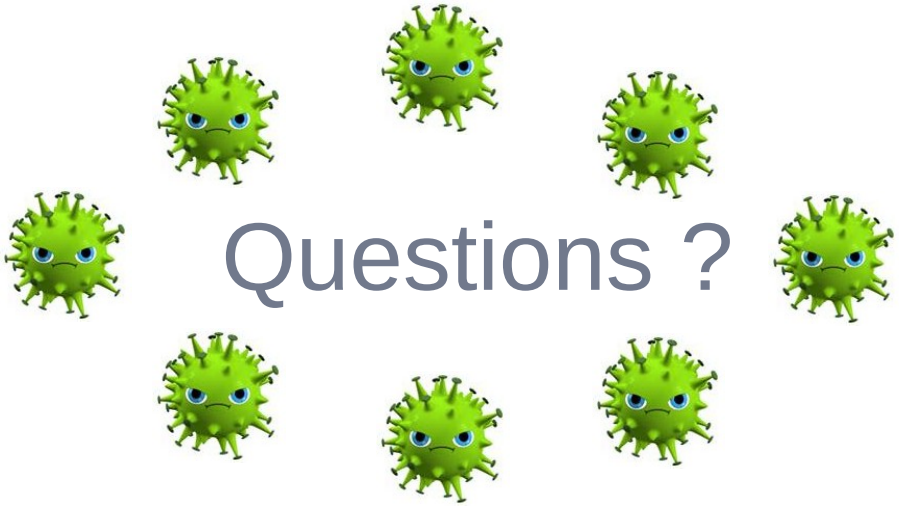
- Dans le cadre du SGS (Système de Gestion de la Sécurité), ce danger a été ajouté dans le cadre de l'analyse de risques:

- Sévérité
- Probabilité d'occurrence
- Conséquences potentielles
- Mesures déjà en place
- Proposition de mesures additionelles pour diminuer le risque

- Une réévaluation du risque régulière est nécessaire, notamment en cas d'installation d'un nouveau simulateur (nouvelle architecture)

© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

© Airbus S.A.S. All rights reserved. Confidential and proprietary document. This document and all information contained herein is the sole property of AIRBUS. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of AIRBUS S.A.S. This document and its content shall not be used for any purpose other than that for which it is supplied. The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, AIRBUS S.A.S. will be pleased to explain the basis thereof. AIRBUS, its logo, A300, A310, A318, A319, A320, A321, A330, A340, A350, A380, A400M are registered trademarks.



© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

AIRBUS