Germanwings : Les enseignements en matière de sécurité

Quel rapport y-a-t-il entre le crash de l'Airbus A320 de la Germanwings et la sécurité informatique ? A priori aucun d'autant que la cause d'origine technique semble définitivement écartée. Il y a cependant beaucoup d'enseignements à retenir lors d'un tel accident que l'on peut appliquer directement à la sécurité de l'information.

J'anime depuis plus de 20 ans des séminaires sur la sécurité informatique et j'utilise bien souvent dans mes exemples des analogies avec la sécurité routière car à y regarder de plus près les principes fondamentaux sont les mêmes : Il y a des risques (accidents), des mesures de sécurité (ceinture de sécurité, ABS, campagne TV de prévention, etc…), des contrôles (gendarmes, radars, alcotest, etc…) mais aussi hélas des impacts potentiels (contraventions, blessures, décès). Dans le domaine de la sécurité aérienne, on retrouve les mêmes concepts et tout comme dans le domaine de la SSI, après chaque catastrophe, on essaie d'en tirer les leçons pour diminuer les accidents sachant que la probabilité d'occurrence est faible mais que les impacts sont très lourds (150 morts dans le cas du drame de la Germanwings). Ainsi, après les attentats du 11 septembre, les autorités aériennes, EASA (Agence de sécurité aérienne européenne) et FAA (agence américaine) ont demandé aux acteurs de l'aérien de travailler ensemble sur un système permettant de verrouiller le cockpit afin que personne de l'extérieur ne puisse ouvrir la porte même sous la contrainte d'une arme. C'est la raison pour laquelle les cockpits disposent aujourd'hui d'une porte blindée et d'une option de verrouillage (Lock). Lorsque la porte est verrouillée, même le code confidentiel connu exclusivement par le personnel habilité (PNC) ne permet pas d'entrer dans le cockpit. Le problème évidemment est que si la menace est à l'intérieur même du cockpit et que le mécanisme de sécurité est enclenché, on court tout droit à la catastrophe. C'est ce que l'on appelle dans le jargon de la SSI : une menace liée à une malveillance interne (malicious insider threat). Cette menace existe partout (dans l'administration, la police, l'armée, les entreprises privées, etc…) et il ne faut jamais la négliger au risque d'en payer le prix fort. Le cas d'Edward Snowden à la NSA l'illustre très bien même si Snowden n'était pas un agent de la NSA mais un simple prestataire externe.
Et qu'en est-il chez un prestataire de Cloud me direz-vous ? Et bien exactement la même chose ! Même si l'on recrute avec la plus grande prudence (enquête de moralité, antécédents judiciaires inscrits au TAJ, etc…) et que l'on rajoute des clauses de confidentialité dans le contrat de travail, le risque existe toujours. Mais ce risque existe aussi bien sûr lorsque nos données sont gérées en interne. J'ai d'ailleurs rencontré récemment une entreprise française qui désirait externaliser des données dans le Cloud car elle estimait que le risque lié à des administrateurs indélicats était supérieur aux risques induits par le Cloud. Les données en question concernaient un projet de plan social et les dirigeants ne souhaitaient pas que des

fuites d'information puissent parvenir aux syndicats de l'entreprise.
Revenons à la sécurité aérienne, on a donc mis en œuvre une mesure de sécurité pour réduire le risque lié à une menace externe (des terroristes en cabine) mais dont les conséquences entrainent une augmentation du risque lié à la malveillance interne. C'est bien toute la difficulté de la sécurité : une mesure de sécurité n'annule pas un risque, elle le diminue et il reste toujours un risque résiduel. Ce risque résiduel sera-t-il acceptable ? Si tel est le cas, la mesure de sécurité sera suffisante. Dans le cas contraire, on devra songer à une autre mesure de sécurité en complément ou en remplacement de la première. D'autre part et on le voit bien dans l'exemple aéronautique, une mesure de sécurité peut entrainer de nouveaux risques. Il convient alors de bien identifier tous les effets de bord d'une mesure de sécurité pour s'assurer qu'un risque nouvellement créé ne soit pas supérieur au risque initialement traité. Dans le contexte actuel où la menace terroriste est particulièrement forte, il est évident que les passagers sont plus en sécurité dans un avion équipé d'un cockpit sécurisé. Pour autant, peut-on accepter qu'un des deux pilotes puisse à lui tout seul décider de la vie ou de la mort de 150 personnes ? Et voilà que les compagnies aériennes se précipitent vers une nouvelle mesure de sécurité : La présence obligatoire d'une hôtesse de l'air ou d'un steward dans le cockpit lorsqu'un pilote s'absente. Première interrogation : la mesure de sécurité est-elle efficace ? Une hôtesse sera-t-elle en mesure d'empêcher le pilote de « crasher » l'appareil ? A priori non, le risque résiduel est donc inacceptable. J'entendais un expert en sécurité aéronautique dire ce matin sur BFMTV : « *Cela n'empêchera sans doute pas le pilote d'agir mais la mesure apportera un réconfort psychologique auprès des passagers* ». En d'autre terme, ce qui compte ce n'est pas d'être sécurisé mais simplement le sentiment d'être sécurisé et il y a de fortes chances que cette mesure soit adoptée par toutes les compagnies aériennes. En effet, si les clients ont peur, ils auront une tendance naturelle à éviter de prendre l'avion. Pour les trajets courts, ils pourront par exemple privilégier le train. Pour les compagnies aériennes comme pour les fournisseurs de Cloud, un client qui a peur est un client qu'il sera difficile de convaincre ou de fidéliser et donc un réel frein au business. Il faut donc rassurer et donner le sentiment de sécurité même si le niveau réel n'a pas vraiment évolué. Mais le fait de faire rentrer une autre personne dans le cockpit n'entraine-t-il pas un nouveau risque ? Sachant qu'il y a, dans le cockpit, une hache (destinée en cas d'accident à arracher une cloison), on peut facilement imaginer un scénario dans lequel un steward terroriste pourrait s'isoler dans le cockpit et se débarrasser facilement du pilote avec cette arme. Ce nouveau risque a-t-il été soigneusement étudié ? Il serait certainement plus sage que tous les acteurs de la navigation aérienne se concertent et définissent ensemble la mesure la plus appropriée. On peut en effet imaginer d'autres réponses comme par exemple un code spécifique pour les pilotes ou un lecteur biométrique (iris) pour déverrouiller la porte même en position lock. Pourquoi ne pas envisager une reprise du contrôle à distance de l'avion par les autorités lorsque les pilotes ne répondent plus et que l'avion part visiblement au crash. On n'imagine bien sûr dans ce cas, un niveau de sécurité comparable au pilotage d'un drône militaire et les actions possibles limitées à faire atterrir l'avion sur l'aéroport le plus proche. Bien sûr aucune mesure n'est infaillible et le risque zéro n'existe pas mais à chaque

incident ou accident, on doit toujours prendre le temps de bien analyser toutes les causes et en tirer les conséquences afin d’améliorer sans cesse la sécurité. Et s’il faut encore se rassurer, il suffit de regarder les chiffres pour constater que le transport aérien reste encore un des moyens de transport le plus sûr au monde.