Sécurisation du SI : la passion de l'échec

Cédric CARTAU
RSSI et DPO
CHU de Nantes et GHT44

Réussir un projet, c'est bien. Réussir un projet en tenant compte de la sécurité du SI, c'est très bien, tout comme réussir un projet strict de sécurité. Mais si l'on nous enseigne à longueur de séminaires (souvent animés par des jeunes et fringants consultants en costume serré et cravate impeccable) comment réussir un projet, jamais ô grand jamais on ne vous dit comment planter un projet. Et c'est une erreur, la méthode gagne à être connue.

Comment donc ? Planter un projet ? Mais qu'est-ce donc que ce sujet qui frise le niveau 7 sur l'échelle de la Richter-stupidité ? Votre serviteur a-t-il fumé ses tests PCR ? Ou prévu d'aller faire pousser des chèvres et du tabac qui fait rire dans le Larzac ? Rien de tout cela en fait.

Les motivations inavouables

La vie professionnelle étant ce qu'elle est, il ne faut jurer de rien, et en particulier ne pas croire que l'on aura toujours intérêt à voir réussir tous les projets. Sur la fin de carrière, poussés que nous serons tous par des jeunes diplômés à l'ambition aussi mordante que les bouts pointus de leurs chaussures (ou quelle que soit la mode vestimentaire à ce moment), il n'est pas inutile de connaître quelques rudiments destinés à planter en beauté le projet de Kevin, le jeune exalté qui vous pourrit vos réunions et votre moral. Il faut en revenir aux fondamentaux, là encore.

Le plus simple est de torpiller le paramètre délai : en suggérant un délai impossible à tenir, vous avez une bonne chance de passer des week-ends sereins (ce qui ne sera pas le cas pour Kevin). Malheureusement, d'une part les délais ne sont presque jamais tenus, d'autre part il subsiste toujours le risque que Kevin réussisse malgré tout à tenir ses dates.

Il faut alors passer à la vitesse supérieure et lui sabrer ses budgets, le nerf de la guerre sans lequel rien ne se passe. Déjà que tous les projets informatiques ou presque dépassent les montants initiaux, si en plus de cela vous réussissez à lui retirer des ressources humaines (facile à dire, pas trop difficile à faire), vous mettez toutes les chances de votre côté.

En cas de poisse, suggérez que le périmètre initial ne comprend peut-être pas tout ce qu'il aurait fallu prendre en compte. Ce serait bien le drame si Kevin arrive à s'en sortir. Faire constamment varier le périmètre d'un projet est l'assurance presque parfaite qu'il n'aboutira jamais. Un jour on ajoute deux points qui nécessitent de tout reconcevoir, le lendemain on en retire un des deux, et ainsi de suite. Kevin vous haïra (pas grave), mais surtout son projet ne s'en remettra pas (une bonne nouvelle n'arrive jamais seule).

Si enfin, comble de malchance, Kevin et son malheureux projet arrivent à survivre à cela, il reste l'arme ultime : torpiller la gouvernance. Changer la MOA, son directeur et son chef de projet, puis y revenir, puis inclure une autre direction dans le projet pour au final la retirer.
La méthode est garantie sans échec connu.

Les motivations carrément immorales

L'ennui est racine du mal et il faut bien occuper ses journées, surtout quand le RSSI croule sous les injonctions contradictoires (tout protéger, tout le temps et partout, sans aucune thune - bon en même temps cela n'arrive jamais, hein ?). Pourquoi ne pas, à votre tour, faire tourner la MOA en bourrique ? Dois-je vous rappeler que le directeur marketing est forcément payé une blinde, tout cela pour produire des flyers en couleur et des goodies qui font *coin coin*[1] : aucune raison de ne pas lui rendre la monnaie. Un bon truc est d'expliquer à vos MOA que « ben non les procédures dégradées ça ne sert à rien, c'est un truc dont les consultants nous bassinent rien que pour nous fourguer des journées homme », voire, s'ils en ont, leur suggérer que « les tester est inutile, on fait confiance ce sont des pro ». A titre personnel j'aime bien le « ne vous inquiétez pas, tous les bugs sont corrigés dans la prochaine version ». Ou encore « la disponibilité de notre informatique est au niveau des 5-9 » : au mieux ils pensent que c'est un code ésotérique uniquement connu des initiés de la planète Zorglub, au pire ils comprendront que cela veut dire moins de 5 minutes d'arrêt par an et seront admiratifs, pour briller dans les dîners en ville c'est top moumoute.
J'ai remarqué également que l'utilisation du mot « automatique » provoquait un état de quasi transe CBD chez certains métiers : automatique, répétez après moi, au-to-ma-tique, en séparant bien les syllabes : le logiciel bascule sur le serveur de secours de manière au-to-ma-tique (cela ne marche jamais, mais ce n'est pas grave, l'important n'est pas le flacon mais l'ivresse), la clim est redondée de manière au-to-ma-tique, le provisionning des comptes est au-to-ma-tique, on respecte le RGPD de manière au-to-ma-tique. C'est magique, j'adoooore. Evidemment, le jour où le pet se produit, il faut utiliser les excuses classiques des DSI (20 ans d'expérience, j'ai testé) : oui mais ce cas d'usage n'était pas listé dans la matrice des risques pris en charge, oui mais on a un bug d'un sous-traitant qui n'a pas respecté la norme ISO 20 000, oui mais etc. etc. etc.
Je vous garantis que cela serait bien la poisse si, à la prochaine panne, tout ne partait pas en vrille : et vlan, et les salaires des RSSI qui prennent 10 %.

Les motivations tout à fait avouables - les seules valables en fait

Comme dit le célèbre proverbe Shadok et comme le rapportait souvent le Professeur Piéplu : « Ce n'est qu'en essayant continuellement que l'on finit par réussir. Autrement dit : plus ça rate, plus on a de chances que ça marche. »
Etudier les erreurs, c'est le meilleur moyen de ne pas tomber dedans. Pendant la seconde Guerre Mondiale, le commandement des forces aéronavales américaines dans le pacifique voulait savoir comment renforcer la sécurité des Corsair (les avions de chasse que l'on voit dans la série « Les têtes brulées ») en désossant ceux qui rentraient tant bien que mal de mission - les bestioles étaient solides au point de pouvoir continuer de voler avec plusieurs balles dans le moteur. L'idée était de renforcer les parties de la carlingue qui avaient des impacts de balle, mais un mathématicien (Abraham Wald) leur fit remarquer qu'il fallait faire exactement l'inverse. Peut-être

[1] Humour du 18ème degré, on précise tout de même…

que la raison pour laquelle certaines zones des avions n'étaient pas couvertes d'impacts de balle était que les avions qui avaient été abattus dans ces zones ne sont pas revenus. Cette idée a conduit au renforcement du blindage sur les parties de l'avion où il n'y avait justement pas d'impacts de balle.

Depuis quelques années, cette discipline foisonne : depuis l'excellent « Les décisions absurdes » de Christian Morel (trois tomes en tout, un ultra-classique) on a vu arriver le non-moins excellent « Super Fail », podcast de France Inter animé par Guillaume Herner, « Les stratégies absurdes » de Maya Beauvallet, « Vous allez commettre une terrible erreur » d'Olivier Sibony (qui intervient d'ailleurs régulièrement sur la chaîne Xerfi Canal) et le désopilant « Les lois fondamentales de la stupidité humaine » de Carlo M Cipolla, sans parler bien entendu de l'inénarrable « Les grands Z'héros de l'histoire » de Clémentine Portier-Kaltenbach.

Etudier les erreurs est dans l'ADN de certains secteurs tel l'aéronautique, qui diligente une enquête systématique du BEA après chaque crash, même d'un avion de tourisme, qui oblige à signaler les incidents, qui diffuse les FEI (Fiches d'Evénement Indésirable) sur tout le territoire et où chaque pilote considère que son erreur, bien analysée et communiquée, peut servir à sauver des vies (voir à ce sujet la vidéo sur l'atterrissage raté d'un TB10 à Courchevel, qui est connue absolument de tous les pilotes de France et de Navarre). La SSI a clairement des progrès à faire et des enseignements à retirer des 70 ans de pratiques de l'aéronautique.

Conclusion

Au-delà de l'humour de ce début d'article, il faut bien reconnaître que la culture de l'échec - analyse, étude, REX, etc. - est quasi absente des SI et par transition de la sécurisation des SI, tout du moins si on la compare à celle susnommée du secteur aérien. Cette époque est en train de changer : les CERT, les observatoires sectoriels, les groupes d'experts nationaux ou locaux, les échanges dans les club ou les associations, les Think Tank tels le CyberCercle, tout cet écosystème participe selon sa mission à l'évolution des mentalités.

Il y a quelques jours, je participais à une réunion qui consistait à mettre en place un processus inter établissement pour cadrer l'homologation de projets SI sensibles : pendant 45 minutes il a été question de notes, de fiches de services, de réunions périodiques de bilan, etc. C'est bien, c'est nécessaire, mais ce n'est pas ce qui m'intéresse : moi je ne m'intéresse qu'aux projets qui justement allaient échapper à ce processus, soit par manque de connaissance institutionnelle, soit par volonté de masquer (plus rare). Comment les identifier, les pister, les ramener dans le troupeau.

Faites ce simple test : demandez à votre DSI si le parc de PC est protégé par un antivirus : il va vous montrer la console centralisée de supervision de l'AV. Demandez-lui ensuite s'il a mesuré les PC qui, justement, n'avaient pas d'AV et donc n'étaient pas listés dans la console. Gros blanc.

Je ne m'intéresse qu'à l'erreur, l'échec, la liste des trains qui arrivent en retard.

On n'apprend que de l'échec.

Bibliographie

« Les décisions absurdes », Christian Morel, trois tomes

« Un brève histoire du futur », Michio Kaku

« La mort de la mort », Dr Laurent Alexandre

« Le Big Data, penser l'homme et le monde autrement », Gilles Babinet

« Culturama », Aiden Erez

« La sécurité du système d'information des établissements de santé », Cédric Cartau