Les assurances en quête de sécurité

Par Théodore-Michel Vrangos | 15/09/2016, 12:18 | 1183 mots


(Crédits : DR)

Les assureurs sont pris dans une contradiction entre les contraintes règlementaires qui les poussent vers le développement de systèmes ouverts et les nécessités de la sécurité. Par Théodore-Michel Vrangos, cofondateur et président d'I-Tracing

La cybersécurité est un élément essentiel pour toutes les entreprises et le secteur des assurances n'y échappe évidemment pas. Les Systèmes d'Information des assureurs attirent particulièrement les cybercriminels et il faut équilibrer les besoins et les priorités, tout en respectant les spécificités du métier. Le développement de la culture numérique y est récent et les bonnes pratiques ne sont pas toujours inscrites dans les comportements, alors que les contraintes réglementaires poussent au contraire vers un développement rapide de systèmes d'information plus ouverts et plus connectés, avec les exigences de sécurité qui en découlent.

L'assurance, un domaine très particulier

Historiquement, la migration des architectures informatiques dans le secteur de l'assurance et des mutuelles vers les technologies Internet d'aujourd'hui a été plus lente que dans beaucoup d'autres secteurs. L'ouverture du SI a été freinée, contrairement au secteur bancaire "frère", du fait des applications métiers très spécifiques car très sectorielles et souvent peu interconnectées. Le digital y est actuellement en pleine croissance, tant pour les SI métiers internes que pour les applications proposées aux clients, entreprises ou

particuliers. La dynamique numérique au sein des assurances est très forte. La sécurité doit évidemment suivre, et même anticiper.

Une autre particularité du monde de l'assurance son besoin d'outils d'analyse prédictive des risques métiers (risques naturels, risques industriels, etc.), c'est-à-dire d'outils de modélisation IT, de statistiques, de corrélation, etc. Ces modèles sont sensibles car ils concentrent la connaissance métier de l'entreprise, les données et aussi les résultats, bien évidement. Et dans ces métiers, le big data s'impose tout naturellement.

Une digitalisation rapide

I-TRACING travaille avec les leaders mondiaux du domaine comme AXA ou Allianz mais aussi, avec des acteurs de pointe en forte croissance comme Thélème Assurances. Pour tous, la cybersécurité est un sujet déterminant et critique. D'autres acteurs en plein développement comme par exemple les FinTech et InsureTech arrivent. Plus que tout autre secteur économique, après la relative léthargie technologique évoquée plus haut, l'assurance met les bouchées doubles : plateformes de services en ligne, digitalisation des parcours clients, ouverture et interconnexion des SI vers des partenaires FinTech, partage des données marketing, cloud, big data, etc., d'où une multiplication des cyber-risques.

La multiplication des risques

Le métier d'assureur est complexe et très varié. Les risques le sont aussi. Certains sont semblables à ceux de l'ensemble des entreprises comme les attaques par malware ou ransomware. D'autres, très particuliers, sont liés aux données des assurés, aux spécificités de la protection des données médicales, aux vulnérabilités des centres d'assistance et d'appels internes et surtout externalisés, aux données de CRM, etc. Ces risques sont amplifiés par des systèmes d'information de plus en plus ouverts vers les assurés, les partenaires B2B, les partenaires banques, etc.

A ces risques « classiques » s'ajoutent les risques immatériels aujourd'hui couverts par les assurances, et notamment les risques IT de leurs clients. Désormais les assurances, les mutuelles et les courtiers en assurances se transforment en prestataires en sécurité du SI, car pour assurer contre le risque digital, il faut en évaluer le degré... On parle de scoring, de notation de l'entreprise cliente face aux cyber-risques.

Un des aspects critiques, aux yeux des spécialistes d'I-TRACING, est hautement sensible : les sociétés d'assurances comblent actuellement leur retard IT avec, comme c'est souvent les cas dans ce type de situation, un saut technologique important.

Ainsi, le big data, par exemple, très prisé, à juste titre, offre un potentiel métier, de pilotage, de gestion, d'analyse, de projection et de prédiction des risques, etc. gigantesque. Mais, il introduit en même temps, un nouveau risque portant sur des informations de haute importance si la sécurité de ces plateformes, d'une grande complexité, n'est pas correctement prise en compte.

Pour poursuivre avec cet exemple, l'attrait des cybercriminels vient du regroupement en un seul et unique "lieu" des informations métier stratégiques. Ils savent que consulter, aspirer,

casser l'intégrité de ces informations et de ces plateformes métiers big data provoquerait de graves incidents, mettant l'entreprise potentiellement en danger.

Encore et toujours, anticiper

La plupart des RSSI (Responsable de la Sécurité des Systèmes d'Information) et RSO (Responsable Sécurité Opérationnel) des sociétés d'assurances et des mutuelles sont déjà très sensibles au sujet de la sécurité. Ils devraient encore plus se rapprocher des métiers, sensibiliser les CDO (Chief Digital Officer) de leur entreprise, se positionner effectivement sur les solutions et des démarches efficaces de sécurisation et sur le contrôle permanent des applications et des plateformes digitales, accélérer la mise en œuvre de SOC (Security Operations Center) de nouvelle génération, auditer systématiquement et régulièrement les applications mises en production, etc.

La prise en compte et l'implémentation des contraintes légales peuvent être mal appréciées mais elles permettent à l'entreprise de mettre en règle la sécurité de son SI, d'en tirer profit et de capitaliser sur l'effort financier consenti.

La culture numérique, c'est aussi sensibiliser à la sécurité

C'est le rôle croissant du Chief Digital Officer. Dommage que ce rôle ne soit pas tenu par le DSI, mais il est maintenant trop tard. En revanche le RSSI, comme le CESIN (*Club des experts de la sécurité de l'information et du numérique*) l'exprime régulièrement : le potentiel de développement de la sécurité accompagnant la transformation numérique est énorme et crucial.

Dans une vision stratégique, certains assureurs s'associent à des acteurs *pure-players* de la cyber-sécurité pour mieux évaluer et prévenir les cyber-risques ; ils améliorent ainsi l'assurabilité du marché, même si la couverture assurantielle de ces risques reste faible en Europe. Pourtant les nouveaux risques, par exemple ceux liés à la digitalisation du parcours client, à l'ouverture de l'écosystème financier, déplacent et disséminent le risque. Faut-il rappeler qu'en 2015, les pertes liées à la cyber criminalité étaient en hausse de 22% et estimés à 220 milliards d'euros (source : Les Echos Etudes) ?

Le monde de l'assurance (InsurTech, FinTechn, courtiers, mutuelles, etc.) est un écosystème clé de la sécurité IT. Sur son marché il devra autant gérer ses propres cyber-risques que ceux de ses clients. La sécurité du SI des assurances dans l'avenir sera indéniablement centrée sur la protection et la traçabilité des accès à l'information et des opérations, la surveillance constante des plateformes de services, les signaux faibles à travers des SOC orientés vers la prévention et la prédictibilité des attaques. Elle sera également centrée sur le Big Data Sécurité.

Les assureurs le savent, il faut prévenir, car guérir coûte toujours beaucoup plus cher.

Théodore-Michel VRANGOS