Risques de cybercriminalité au cœur des cycles de vie contractuels et de projets

Table ronde dans le cadre de l'intersession du Forum Ouvert du Contract Management - 21 juin 2022 à Paris.

Naoual BERGGOU : « *Quelle est la réalité du risque des attaques informatiques et en quoi le Contract Manager est-il concerné ?* »

Grégory LEVEAU : L'Agence nationale de la sécurité des systèmes d'information, organe gouvernemental donc, a publié le chiffre phénoménal de 255 % de cyberattaques en plus en 2020 par rapport à l'année précédente. Et la tendance reste à la hausse sur 2021. Les entités touchées en premier lieu par les rançongiciels sont les TPE, PME et ETI (34 % des victimes) et sont suivies par les collectivités (19 %) et les entreprises stratégiques (10 %).

Ces attaques à finalité lucrative ne doivent pas occulter les campagnes d'espionnage et de sabotage qui concernent autant les acteurs institutionnels que les acteurs privés.
Le sujet est particulièrement d'actualité depuis le démarrage de la guerre contre l'Ukraine qui n'est évidemment pas que militaire.
La cybercriminalité s'installe durablement partout et est exacerbée en temps de crise.

Ce qui est inquiétant à l'échelle des contrats sur lesquels le Contract Manager intervient découle du constat de la croissance des attaques ciblant la chaine d'approvisionnement par exemple, générant des retards considérables sur les projets qui n'avaient déjà pas été épargnés par la crise sanitaire de la COVID-19.
Les nouveaux usages numériques comme le Cloud sont également exploités par les cyberattaquants et la multiplication des divulgations de données facilite la conduite de nombreuses attaques informatiques puisque les données exfiltrées contiennent souvent des informations d'authentification et fournissent ainsi une porte d'entrée dans les systèmes informatiques.

Grégory Leveau Ouidad Loncelle

Eric Legloahec Naoual Berggou

Le renforcement de la cybersécurité de ces données doit donc être une priorité et le Contract Manager a, ici, un rôle évident à jouer.

Naoual BERGGOU : « *D'un point de vue technique, quelle est la nature de ces attaques et pourquoi se produisent-elles ?* »

Éric LEGLOHAEC : Il faut bien distinguer le vecteur utilisé pour l'attaque et l'objectif de l'attaque.

Le vecteur d'attaque implique dans 85 % des cas un élément humain :

- En premier lieu par le biais du « *phishing* » (ou hameçonnage), qui consiste à recueillir des informations personnelles en utilisant des moyens trompeurs : faux mails, faux sites, etc ;
- Ensuite par le « *social engineering* » (ou ingénierie sociale), qui consiste à abuser psychologiquement d'une victime pour lui soutirer des informations par mail, par téléphone, par les réseaux sociaux, ou par interaction directe.

Les autres vecteurs d'attaque, un peu moins répandus, sont :

- L'exploitation d'applications, notamment web ;
- L'exploitation des vulnérabilités ou des défauts de configuration d'un système informatique ;
- Le piratage de la connexion à distance – plus important depuis la généralisation du télétravail – ;
- Le piratage *via* les données mobiles (piratage du Wifi, installation de logiciels malveillants sur un téléphone mobile) ;
- Enfin l'intrusion physique, plus rare, mais qu'il ne faut pas négliger.

L'objectif de l'attaque, quant à lui, peut se réaliser indifféremment par ces différents vecteurs.

Grégory en a parlé, il peut s'agir :
- D'empêcher l'entreprise d'accéder à ses données en lui demandant une rançon (rançongiciels) ;
- D'exfiltrer des données (espionnage, vente des données, chantage) ;
- D'utiliser des données de connexion pour détourner de l'argent (faux ordre de virements, ...) ;
- De paralyser l'entreprise par un déni de services (DOS) ;
- De porter atteinte à l'image de l'entreprise.

Comme nous l'avons vu, étant donné que la grande majorité de ces attaques se produisent par le biais d'un facteur humain, la cause principale en est une carence de formation des salariés et plus globalement, le manque d'une véritable culture de la sécurité de l'information au sein des organisations.

Ensuite, l'absence de moyens humains et/ou financiers suffisants alloués à la sécurité informatique dans l'entreprise peut être une cause importante du succès d'une cyberattaque. Moins l'entreprise investira dans son infrastructure informatique, plus elle s'exposera à des cyberattaques dévastatrices sur le plan financier.

Vous reprendrez bien un peu de Contract Management ?

Certifié par l'Etat

Certificat Professionnel
C²MPC®
de Contract Management

e²cm
Ecole Européenne de Contract Management

e²cm consulting

01 48 86 05 27 . e2cm.net . contact@e2cm.net

Naoual BERGGOU : « *Comment l'assureur s'est emparé du sujet et quelles ont été les évolutions de votre positionnement ces dernières années au vu du nombre croissant de cas de cyberattaques ?* »

Ouidad LONCELLE : Les grands Groupes sont assurés depuis 20 ans pour ce risque par les compagnies d'assurance (en tout cas Axa) et plus largement dans les pays anglo saxons qui y sont très sensibles.
Si on remonte un peu dans le temps il y a d'abord eu chez Axa un premier mouvement ou plutôt un frémissement en 2014, puis en 2017 un véritable électrochoc avec l'entrée des *malwares*.
En 2018, le RGPD a permis d'éveiller toutes les entreprises, même les plus petites aux risques liés à la cybercriminalité. En tant qu'Agents généraux, nous avons mené de larges campagnes de sensibilisation auprès de nos clients, aussi bien aux risques d'attaques, qu'aux conséquences économiques et réputationnelles des entreprises.
En 2020, la pandémie de Covid 19 s'est accompagné d'une explosion de la cybercriminalité caractérisée par :
- Plus d'attaques ;
- Une augmentation du volume de sinistres ;
- Une prise de conscience généralisée des risques par les entreprises.
Les organisations criminelles ont identifié une véritable opportunité dans ce contexte de crise sanitaire. En effet, il est intéressant de rappeler que le marché représente 1.5 milliard € pour ces cybercriminels qui disposent de moyens accrus, leur permettant d'investir dans tous les domaines :
- Le *fishing* ;
- La recherche sur les systèmes de vulnérabilité ;
- Le piratage.

Ces investissements leur donnent les capacités d'opérer plus d'attaques, d'une puissance croissante. Ces cybercriminels bénéficient d'une protection juridique puisque localisés dans des pays étrangers.

La prévention est de surcroît l'une des protections les plus efficaces. Ainsi, il est indispensable de mettre en place des mesures d'hygiènes informatiques, tout comme on peut le faire pour éviter un vol avec un portail, une alarme, une serrure, etc. L'entreprises doit mettre en place des lignes de défense successives pour se protéger des cybercriminels.

Pour en revenir à l'assurance, dans la mesure où les attaques sont de plus en plus nombreuses, les assureurs sont devenus plus exigeants sur la sélection des risques en prévoyant notamment des prérequis pour pouvoir couvrir un risque. Je reprends mon exemple du vol, si vous laissez les clés sur la porte, ou la porte fermée avec la clé sous le paillasson, le risque est plus fort.

Naoual BERGGOU : « *Et concrètement, quel doit être l'apport du Contract Manager quant à la prévention des risques de cybercriminalité sur les projets et les prestations de services ?* »

Grégory LEVEAU : Dans le cadre de notre processus d'administration des données sensibles, qui couvre la gestion de la propriété intellectuelle, de la confidentialité et des données personnelles, trois sujets éminemment techniques d'un point de vue juridique, nous devons intégrer ce risque cyber de plus en plus prégnant.

Cela passe par différentes catégories d'actions préventives :

- La création des bonnes clauses contractuelles avant tout et, surtout, l'assurance du suivi, par des audits réguliers, de la concrétisation des engagements contenus dans lesdites clauses : protocoles de conservation des données, outils de cryptage, plans d'action anti-intrusion, procédures de sauvegarde et autres garanties de résilience, renvoi à des normes et standards idoines, etc ;
- Vérifier que la police d'assurance de l'organisation est adaptée au niveau de risque identifié sur notre contrat ; les polices à l'échelle de la société étant parfois désuète au regard des nouveaux enjeux contractualisés sur un projet car l'évolution technologique va très vite et le juridique doit rester au diapason ;
- Sensibiliser les acteurs du projet le plus tôt possible dans la phase d'exécution et idéalement dès la signature du contrat. La *Contract Awareness* est un très bon outil pour informer les opérationnels et les responsabiliser sur la mise en œuvre des mesures préventives indispensables ;
- Créer et mettre à jour, main dans la main avec les experts opérationnels, une charte informatique qui sera déclinée sur les projets au gré de leurs spécificités ;
- Évaluer notre niveau de maturité interne, à l'échelle du contrat/projet que nous pilotons ; à ce titre, la mise en place d'un questionnaire de sécurité systématiquement déployé serait une bonne pratique.

Autrement dit, la cybercriminalité est traitée par le Contract Manager comme n'importe quelle autre catégorie de risque, à côte des aléas commerciaux, relationnels, géopolitiques, environnementaux, financiers notamment dans le cadre d'une stratégie globale qui consiste à identifier le risque, l'évaluer et surtout le piloter par le biais de plans d'actions robustes. Un risque cyber qui reste noyé au cœur d'un registre sous format Excel ne sera pas considéré comme étant « géré ».

Naoual BERGGOU : « *Nous avons vu avec Grégory le rôle du Contract Manager sur le sujet. Plus spécifiquement d'un point de vue technique, quels sont les réflexes incontournables et qui est concerné par la mise en place des actions de prévention ?* »

Éric LEGLOHAEC : Comme je le mentionnais précédemment, la première action est de former le personnel de l'entreprise aux bonnes pratiques en matière de cybersécurité. Reconnaître une attaque par hameçonnage, maîtriser ses données confidentielles, identifier les sites à risques, vérifier l'identité de ses interlocuteurs, verrouiller son poste de travail, ranger son bureau tous les soirs, utiliser des mots de passe complexes sont quelques exemples de ces bonnes pratiques à appliquer au quotidien et sur lesquelles il faudra sensibiliser les utilisateurs.

Bien entendu, la DSI (Direction des Systèmes d'Information) est la colonne vertébrale de la cybersécurité dans l'entreprise. C'est à elle, en partenariat avec la Direction de l'entreprise, de mettre en place les mesures nécessaires à la protection des données du SI (Système d'Information). Cela passe par des investissements humains et matériels et bien sûr, par la formation du personnel informaticien, comme non-informaticien. Un point d'attention très important doit être porté à la politique de sauvegarde des données de l'organisation.

Il est aussi possible de faire appel à des société de cybersécurité qui feront effectuer des tests d'intrusion (« *pentests* ») par des hackers éthiques sur le SI de l'entreprise afin d'identifier les failles potentielles et les corriger.

L'entreprise peut aller plus loin dans la démarche de cybersécurité, en obtenant une certification ISO 27001, par exemple. Cette norme, bien que coûteuse, est un investissement important pour l'avenir. Elle permet d'instaurer une véritable culture de la sécurité en mettant en place un système de management de la sécurité de l'information (SMSI) au sein de l'entreprise, comprenant : évaluation des risques, objectifs de sécurité, planification, amélioration des processus, sensibilisation, revues de sécurité, amélioration continue, audits, etc.

La certification ISO 27001 n'est pas une norme purement liée à la cybersécurité, elle aborde également la gestion des documents au format papier, la sécurité physique, la fiabilité des fournisseurs, notamment. C'est un réel atout pour l'entreprise, et c'est un avantage concurrentiel non négligeable !

Naoual BERGGOU : « *Grégory mentionnait l'importance de mettre en place et de vérifier la cohérence des polices d'assurance avec nos besoins au sein des organisations comme des projets, quels sont les conseils de l'assureur en matière de protection ?* »

Ouidad LONCELLE : Éric et Grégory l'ont bien dit, la prévention est un impératif qui passe par un bon suivi des actions mises en place par l'entreprise et par la formation des individus composants l'entreprise.

De notre côté, les assureurs sont de plus en plus exigeants car le risque est très élevé, il ne relève parfois plus de l'aléa. Mais nous ne laissons pas nos clients sans solution.
Lors de la sélection du risque nous avons un questionnaire qui permet de vérifier la nature du risque et les points de fragilité en matière de potentielle faille. En fonction des informations transmises, nous proposons lorsque cela s'avère nécessaire, des conseils de base tel que décrit par Eric mais aussi des audits pour faire un état des lieux, au travers de partenariats avec des entreprises spécialisées.
Quoi qu'il arrive il faut analyser le risque en fonction de l'activité de l'entreprise, on comprend bien qu'une entreprise qui a un site internet marchand sera plus pénalisée par un cyber attaque, qu'une entreprise qui travaille dans le secteur de la construction. La perte d'exploitation sera plus forte dans le premier cas, *a priori*.
L'assurance et la prévention ne peuvent pas être dissociées, il s'agit d'un bloc.

Cela passe par :
- La formation des salariés ;
- La mise en place de mots de passe complexes qui seront modifiés régulièrement ;
- L'accès à distance VPN doivent être sécurisés ;
- La mise à jour des logiciels : il s'agit d'une faille de plus en plus utilisée pour s'introduire dans les systèmes ; appelé Faille Log4j : un cauchemar pour des millions d'applications Java.

Une fois introduit, le passage à l'acte peut être volontairement long, cela permet aux cybercriminels d'analyser le système avant de l'attaquer.

Naoual BERGGOU : « *Tout ceci est un coût additionnel qui vient impacter la marge des contrats. Dans quelle fourchette se situe-t-il ?* »

Ouidad LONCELLE : Le tarif du contrat d'assurance dépend de nombreux critères :
- Chiffre d'affaires ;
- Nombres de salariés ;
- Sites marchands ou non ;
- Sauvegardes ;
- Suivi ;
- Etc.
- Options choisies : perte d'exploitation, cyber fraude, responsabilité civile, cyber rançonnage...

Il est difficile de donner un montant, cela peut varier de 500 € pour une TPE à ...
Le budget audit peut lui aller de 1 500 € à 3 000 € pour des PME, en moyenne, en fonction de la nature des entreprises. Le marché des PME est globalement peu protégé et dynamique.

Naoual BERGGOU : « *Nous avons identifié le rôle du Contract Manager en phase de prévention du risque de cybercriminalité, mais qu'en est-il en cas d'intrusion ?* »

Grégory LEVEAU : Le piège serait d'imaginer que ça n'arrive qu'aux autres. Or, nous devrions plutôt partir du principe que le partenaire est considéré, par défaut, comme non sûr.

L'outil contractuel cohabitera inéluctablement avec l'outil technique dans ce domaine. Il convient alors d'anticiper le problème par l'organisation de règles de gestion des incidents, elles aussi contractualisées dans une annexe technique, un plan qualité ou un plan de continuité, ou tout document adapté et engageant les parties. L'idée ici est de limiter au maximum les dégâts, de réduire la temporalité de l'incident et d'assurer un maintien des activités au cœur du projet.

Le support de la loi doit aussi être envisagé, dans une perspective réparatrice cette fois.

Le code pénal notamment, via son chapitre sur les atteintes aux systèmes de traitement automatisé de données (articles 323-1 à 323-8), vise à sanctionner entre autres les personnes (physiques ou morales) qui cherchent à prendre connaissance d'informations confidentielles ou non présentes dans le système informatique de l'organisation, qui bloquent l'efficacité du système de traitement, qui portent atteinte à l'intégrité des données, et autres réjouissances.
Et, indépendant de ces textes spécifiques et relativement récents qui seront vraisemblablement mis à jour et développés régulièrement dans les prochaines années, nous trouvons dans les règles préexistantes des infractions pénales élargies, *de facto*, aux atteintes aux réseaux numériques, à l'instar de l'escroquerie (qui peut être caractérisée via l'utilisation d'internet), l'atteinte à la réputation qui viserait à annihiler la concurrence ou l'ébranler.

En cas d'attaque, les réponses techniques seront déployées par les opérationnels et le Contract Manager s'assurera, en coordination avec les juristes, que dans l'écosystème de son contrat, une réponse juridique est également préparée. L'attaque sera alors cartographiée, l'huissier saisi en vue de dresser constat et une plainte déposée auprès du procureur de la République compétent territorialement.

Naoual BERGGOU : « *Lorsque malgré tous nos efforts, l'attaque a lieu, comment réagir, quelles sont les clés de l'efficacité technique mentionnée par Grégory ?* »

Éric LEGLOHAEC : La première chose à faire est d'organiser une cellule de crise cyber réunissant les principaux intéressés : Direction, Communication, DSI, etc., qui permettra de prendre des décisions rapides, efficaces, et non précipitées. Agir dans la panique n'est jamais bon.
Ensuite, il faudra déconnecter les machines infectées du réseau pour éviter la propagation de l'attaque à l'ensemble du Système d'Information.
Une fois l'attaque circonscrite, il faudra évaluer les dommages sur le SI, comprendre comment l'attaque est arrivée et remettre en route les services de l'entreprise arrêtés, lorsque tout risque aura été écarté.
Si votre entreprise possède un SI d'Importance Vitale (produits de santé, gestion de l'eau, alimentation, énergie, etc.), vous avez l'obligation de déclarer l'attaque à l'ANSSI.
Si une violation de données personnelles a eu lieu, l'incident doit être déclaré à la CNIL.
Il faudra aussi porter plainte auprès des autorités compétentes contre les auteurs de cette cyberattaque.
Pour toutes ces étapes, il est conseillé de faire appel à une entreprise experte en cybersécurité, qui pourra vous accompagner afin d'être plus serein dans la reprise de vos activités et qui garantira que l'attaque ne va pas recommencer instantanément.

Naoual BERGGOU : « *Quelles sont vos recommandations finales que tous les Contract Managers et les acteurs du projet, plus largement, doivent avoir en tête ?* »

Éric LEGLOHAEC : Aujourd'hui, le pirate informatique n'est plus le jeune à capuche réalisant tranquillement ses activités illégales dans la confidentialité de son appartement. Depuis plusieurs années, les cyberattaquants se sont professionnalisés, ils sont organisés en véritables entreprises avec des directeurs, des chefs de projets, des exécutants et réalisent des « chiffres d'affaires » qui feraient rougir les entreprises classiques. Ils sont donc capables d'être très patients, et ce quel que soit le niveau de sécurité de votre SI. S'ils veulent pénétrer dans votre organisation parce qu'elle représente pour eux un enjeu important, notamment financier, ils réussiront tôt ou tard.

Comme le disait Grégory, ne vous croyez donc jamais à l'abri ! Le risque est réel et doit être pris en compte dans vos contrats. Il est bien entendu possible de minimiser ce risque en réalisant les actions que j'ai décrites précédemment, avec les investissements adéquats.

Naoual BERGGOU « *Dans la vision assurantielle, quelles seraient les préconisations ultimes et, en faisant un peu de prospective, à quoi les assureurs se préparent-ils dans les années à venir ?* »

Ouidad LONCELLE : Le risque cyber évolue très vite. Sur certains risques, il y a de moins en moins d'assureurs car les résultats techniques se dégradent, notamment depuis 2019, principalement en raison d'une pénurie de Réassureurs.
D'ailleurs, même les assureurs se font *hacker* ! On l'a vu chez certains courtiers et même chez des compagnies d'assurance.
Il faut donc accélérer la formation, continuer à s'adapter.
Le risque cyber est un risque systémique. Les *malwares* peuvent être diffusés en une fois et de manière massive dans beaucoup de pays en même temps.
Les grandes entreprises resouscrivent leurs contrats, tous les ans pour évaluer les risques.
On commence à voir apparaitre des outils de comparaison pour évaluer les risques par analogie entre sociétés similaires mais aussi des *cyber rating* qui mesurent les critères de risques presque en temps réel, les protections des entreprises afin de pouvoir ajuster les couvertures d'assurance en conséquence et ainsi, s'adapter aux hackers qui vont de plus en plus vite.
Il est important que la cybersécurité et l'appréhension du risque soient pilotées par la Direction Générale (pas uniquement par la DSI), c'est d'ailleurs le cas dans les grandes entreprises du CAC 40 assurées par AXA.
Des discussions sont aussi en cours avec l'État pour imaginer une couverture conjointe, du type catastrophes naturelles, où les assureurs couvriraient jusqu'à un certain niveau et l'État prendrait le relais.
Néanmoins le potentiel systémique rend la comparaison avec les « *Cat' Nat'* » moins aisée et donc la mise en œuvre plus complexe.

Naoual BERGGOU : « *Nous avons compris que le Contract Manager ne pourrait pas contourner la réalité de la cybercriminalité sur les contrats complexes qu'il pilote. Mais, est-ce le cas pour les Contract Managers de tous les secteurs ?* »

Grégory LEVEAU : Certaines typologies de contrat, projets ou prestations de services, sont plus sujettes à ce risque, bien évidemment. On pense au secteur de l'informatique, des télécoms, de la défense. Mais, la dématérialisation allant croissante, avec une accentuation certaine à la suite de la COVID-19 et la généralisation d'outils distanciels et du travail à la maison, il est difficile d'ignorer ce risque au regard de la nature extrêmement confidentielle, stratégique ou dangereuse de ce qui circule d'un terminal à l'autre sachant à quel point nous sommes toutes et tous hyperconnectés.

Pensons à un projet pharmaceutique de mise au point d'un traitement révolutionnaire ou à la construction d'un nouvel EPR, le risque de cyberattaque est partout ou presque.

Le Contract Manager ne pourra pas se départir de cette nouvelle mission.

Ouidad Loncelle
Agent Général risques entreprises
& Membre du Bureau National de l'union professionnel des agents
AXA, Administratrice de la CNAM

Eric Legloahec
Expert en cybersécurité
Fondateur Numeric Security

Naoual Berggou
Directrice générale adjointe, e²cm Consulting

Grégory Leveau est Contract Manager et Médiateur professionnel, fondateur et président de l'Ecole Européenne de Contract Management (e²cm) et du cabinet e²cm Consulting.
Il est l'auteur de l'ouvrage Pratique du Contract Management, éditions Gualino – Lextenso.
www.e2cm.net