issymedia
Communication & Innovation

Jeudi 18 Avril 9h00 à 11h00
"Menace Cyber: Êtes-vous vraiment prêts?"

Hôtel de ville d'Issy-les-Moulineaux, Salle Multimédia
62 rue du Général Leclerc
92130 Issy-les-Moulineaux

Le 18 avril, un panel d'experts est intervenu à Issy-les Moulineaux pour faire un point sur la menace cyber et les bonnes pratiques pour s'en prémunir. Issus d'horizons différents, les intervenants qui traitent quotidiennement de ces problématiques ont dressé un tableau exhaustif et original de cette menace et des techniques permettant aux entreprises et aux collectivités de s'en prémunir.

Modérateur: Christophe Ysewyn, Expert spécialisé en analyse de risque

- **Introduction : Eric Legale ; Directeur Général de Issy Média, ville d'Issy-les-Moulineaux**

La meilleure défense contre les cyber menaces ? Nous mêmes!

Nous le savons tous : les cyber menaces représentent déjà un réel danger. Pour les entreprises comme pour les collectivités locales ou les particuliers. Et ça ne va pas aller en s'arrangeant puisque les spécialistes s'accordent à dire qu'elles vont continuer de croître sous des formes variées. A la question que tout décideur doit se

poser (mon organisation est-elle prête à y faire face ?), la réponse est probablement négative. Car les solutions techniques, logicielles ou matérielles, ne suffisent pas puisque les principaux risques sont liés aux comportements individuels. Il suffit d'un malheureux clic sur un lien malveillant pour mettre son entreprise en danger. Il y a donc une "nécessité de se préparer à la crise", comme l'a rappelé Benoît Fuzeau, responsable sécurité des systèmes d'information de la Casden Banque Populaire, lors d'une Matinale de So Digital consacrée au sujet, le 18 avril dernier.
Mais si chacun d'entre nous représente une menace, nous pouvons aussi jouer efficacement en défense. En étant d'abord bien informés, grâce à des sites web très bien documentés comme ceux de la CNIL (Commission Nationale Informatique et Libertés), de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ou du Clusif (Club de la Sécurité de l'information français).
On peut aussi se rendre sur les pages d'informations dédiées sur le site Gouvernement.fr ou visualiser les nombreuses vidéos sur Youtube qui y sont consacrées, comme celle-ci :
Allez voir aussi la série de clips de la "Hack Academy" que le Cigref, association spécialisée dans le numérique, a réalisé il y a quelques années.
Ces informations devraient être diffusées sur les grands médias aux heures de pointe, tant il est important que le grand public prenne conscience des petits gestes qui peuvent les protéger. C'est encore plus vrai pour ceux qui ne sont pas spécialisés ou à l'aise avec l'informatique. Rendre intelligible ce dont on parle, notamment en direction des générations pré-numériques, n'est pas facile mais indispensable.
La ville d'Issy-les-Moulineaux prend régulièrement des initiatives pour sensibiliser la population sur les risques encourus dans le monde virtuel. Ce fut le cas lorsqu'elle a décidé d'adopter Qwant comme moteur de recherches par défaut pour tous ses postes informatiques, celui-ci garantissant ne pas tracer nos navigations sur Internet. Ou en lançant des campagnes d'affichage sur les bons gestes pour se protéger, comme celles-ci :

Au-delà de ces campagnes de sensibilisation, il faut parfois seulement faire preuve de bon sens, ne pas banaliser (signaler immédiatement la perte ou le vol d'un ordinateur professionnel par exemple) et surtout ne pas être fatalistes. Comme l'a souligné l'un des orateurs avec un peu d'humour, "les hackers sont d'abord de très bons informaticiens et, comme tous les informaticiens, ils sont fainéants et n'attaqueront que les cibles les plus vulnérables".
Au cours de cette conférence, Randy Yaloz, un avocat franco-américain fondateur d'ELC Group mais surtout expert en contentieux en matière de nouvelles

technologies et Alice Pézard, avocate et conseiller honoraire à la Cour de cassation ont insisté sur les risques juridiques touchant notamment les organisations (de la petite association à l'entreprise multinationale), car les risques de fuite de données peuvent venir de prestataires insuffisamment protégés et ne respectant pas le RGPD (Règlement général sur la protection des données). «Le contrat n'intervient que lorsqu'un problème survient. Il faut donc être vigilants sur ce point» et avoir conscience des risques. Or, 90% des PME et une entreprise moyenne sur deux ne sont pas couvertes contre le risque cyber, a souligné Arnaud Gressel, président de RESCO Courtage, qui propose des assurances contre les risques cyber. C'est d'autant plus indispensable que ces assureurs ont des experts pour accompagner et conseiller l'entreprise en cas de crise liée aux cyber attaques, des experts juridiques rodés au RGPD (rappelons qu'une entreprise n'a que 72h pour déclarer à la CNIL une fuite de données).
En fait, comme pour les risques liés aux incendies, il faut prendre des mesures préventives mais aussi mener des exercices de simulation.
Quand on assiste à une conférence sur le sujet, c'est l'angoisse garantie. Les exemples d'attaques informatiques dans n'importe quelle organisation ou de fraudes auprès des particuliers sont tellement nombreux qu'on pourrait être fatalistes et croire que le Pearl Harbor numérique qu'on nous promet depuis une bonne vingtaine d'années est inéluctable. Gardons à l'esprit que «la sécurité est l'affaire de tous mais surtout l'affaire de chacun».

Benoît Fuzeau, Responsable sécurité DSI de la CASDEN

Benoît Fuzeau a mis en évidence la nécessité de se préparer à la crise et d'éduquer l'ensemble des collaborateurs aux risques cyber comme ils le sont au risque incendie au sein des organisations. Cette démarche est en cours mais des marges de progrès existent.

Nicolas Hernandez, CEO Aleph Technologie

Caractérisant les risques en grandes catégories, Nicolas Hernandez, a mis en évidence la première nécessité qui est celle d'être informé du niveau d'exposition de votre organisation et de la survenue ou non d'un sinistre. En effet, au delà du « rançon-giciel » dont les responsables d'entreprises sont par définition informés, le vol de données est une pratique potentiellement extrêmement dommageable et qui contrairement à un vol physique peut passer inaperçu. Il est donc nécessaire de veiller les menaces, failles et données issues de votre organisation susceptibles d'exister au cœur même des environnements où se préparent et se déroulent ces actions que sont les Dark et Deep Web.

Le risque Cyber dépasse le SI
Longtemps le domaine des RSSI en termes de couverture de risque le Cyber est devenu transverse et dépasse le périmètre professionnel. Le monde personnel et professionnel communiquent via le cyber.
Aujourd'hui le risque cyber concerne ;

- Les infrastructures Logiques (SI)
- Les infrastructures Physiques (bâtiments, biens)

- Les personnes (VIP, acteurs du SI)
- Les données au sens large

Les risques associés dépassent donc la seule responsabilité du RSSI. Pour toucher la Direction Générale.

Les surveillances à des fins de couverture de risques à mettre en place sont donc multiformes, et multi périmètres. Dans le cas de la surveillance externe si surveiller le Clear Web et les réseaux sociaux sont devenus des standards, les surveillances des deep et dark web deviennent essentiels afin de maitriser l'entièreté du périmètre de risque.

Alice Pezard, avocat et arbitre, Conseiller honoraire à la Cour de cassation

Alice Pezard a brossé un tableau complet des pratiques à mettre en œuvre pour se préparer à ce type de menace, avant, après et en permanence.
- Pas de panique mais la guerre est asymétrique, mondiale et « terrible »
- La donnée est au cœur de la révolution Cyber : il conviendrait de statuer sur la propriété des data. L'homme a un droit d'usage sur ses data, peut-être pas davantage
- La donnée est essentielle dans la stratégie et la valorisation des entreprises : savoir faire, base de données, actifs immatériels, secrets d'affaires...
- Rendre intelligible le conflit entre les attaquants et la société

Avant et après l'attaque

I Avant:
- Une protection facile: Anti-virus, Pas de mot de passe ou en changer régulièrement
- La sécurité du numérique à la portée du clic : 12 mesures, par exemple ordinateur, tablette, téléphone même « combat »
- 7 règles à suivre avant l'été : par exemple sensibiliser les travailleurs saisonniers temporaires….
- Toutes ces règles sont définies sur les sites web de l'ANSSI
- Sensibiliser les salariés de l'entreprise: télésurveillance ; la proportionnalité avec le respect à la vie privée est requise. Toutefois, la problématique de la techno – surveillance sur le lieu de travail et du droit à l'accès aux données doit tenir compte des enjeux cruciaux de protection pour l'entreprise, notamment sa survie. Le collectif doit parfois primer sur la vie privée.
- Détection d'anomalies : avoir recours au prédictif sur les éventuels bugs informatiques
- Les Militaires utilisent la crypto : ne pas s'en priver
- Bonne mise en conformité avec la réglementation en vigueur : à l'instar des établissements de crédit ; les entreprises doivent veiller à ce que leur programme de lutte contre la cybercriminalité soit développé parallèlement aux autre programme (RGPD, lutte contre la corruption….) et non pas successivement , ce qui affaiblit les protections.
- Enveloppe Soleau, protection de sa Propriété intellectuelle
- **Et surtout: cybermalveillance.gouv.fr**

II Après:
Dénoncer immédiatement aux Autorités compétentes :
- Cybersurveillance.gouv.fr: ANSSI projet ACYMA
- Site du Gouvernement contre les sites frauduleux
- Site des Douanes
- Payer ou non la rançon : on ne récupère pas ses données

III Toujours :
- Règle générale : la naïveté est un grand risque !
- La survie des entreprises et d'une économie saine est en danger
- Une œuvre pédagogique soutenue est nécessaire :
- Il conviendrait d'organiser à l'ENM, chez les magistrats des réunions avec des cyber experts d'entreprises, qui ont la connaissance des nouvelles performances des attaquants.
- La survie nécessite anticipation, réactivité
- La Défense est probablement l'institution la plus sensibilisée à ces questions (voire l'IHEDN et son cycle annuel cyber sécurité)

Randy Yaloz, Avocat franco-américain et associé fondateur d'ELC Group, expert et stratégiste en contentieux en matière de nouvelles technologies et RGPD.

Randy Yaloz, a éclairé l'auditoire sur le risque supplémentaire lié au RGPD qui introduit une faille dans la relation contractuelle. En effet, les contraintes engendrées par ce règlement sont telles qu'ils constituent une potentialité de rupture de contrats par leur nature qui rend ses préconisations quasiment impossibles à respecter de façon exhaustive

Gestion des Risques Contractuels:
La Boîte de Pandore: L'obligation de conformité avec le Règlement Général sur les Données Personnelles (le RGPD) est-elle un piège pour les uns et les autres?
Examinez vos contrats en matière des données personnelles.
Généralement, il est prévu que chaque partie garantit sa conformité avec le RGPD et de le respecter pour la durée de son contrat.

Naturellement, il apparaît que ce genre d'obligation serait, dans la plupart des cas, une condition essentielle dont le non-respect pourrait justifier la résolution du contrat. Quelle entreprise ne se heurterait pas à une difficulté pour se conformer parfaitement au RGPD ?

Lors de la conférence, le silence a rempli l'auditoire au moment où la question a été posée.
Le RGPD et la loi étaient aussi silencieux que l'auditoire…
En effet, nos législateurs ont créé une boîte de pandore en matière de conformité avec le RGPD !

Il est apparu que les contrats traitant des données personnelles auraient tendance à imposer une «obligation de résultat» aux parties contractantes alors que cette qualification juridique est mal adaptée à la réalité contractuelle et technique.
Seulement une évolution jurisprudentielle vers une «obligation de moyen» pourrait créer plus de certitude dans ce domaine et éviter un grand nombre de litiges qui risque de surgir.

Il existe des astuces pour minimiser ces risques.

L'avocat stratégiste aura pour mission de guider et conseiller son client afin de traverser ce terrain miné.

Arnaud Gressel, Président et fondateur de RESCO Courtage

Enfin, Arnaud Gressel, a exposé l'intérêt d'une démarche assurancielle dans la stratégie à mettre en place pour se préparer au risque cyber.

Pourquoi s'assurer contre les risques cyber ?
Alors que toutes les entreprises sont assurées contre le risque incendie, une très forte proportion de PME n'est pas ou mal assurées contre les risques cyber. La situation est un peu meilleure pour les ETI mais la marge de progression est forte.
Surprenant pour le risque perçu comme N°1 des entreprises.
Plusieurs explications à cela :

- C'est bien connu, les risques cyber, cela n'arrive qu'aux autres...
- Beaucoup de dirigeants pensent être assurés par défaut sans savoir véritablement comment et ni pour quels montants
- Une méconnaissance des offres de« cyber assurance »
- Sans doute un manque de sensibilisation de la part des divers conseils, bien que les choses évoluent rapidement et dans le bon sens, ne serait-ce que par rapport à 2018.

Un contrat de « cyber assurance » est la meilleure protection qui soit, et vient compléter le dispositif en place (protection/sensibilisation) au sein de l'organisation via :

- Un volet assistance (experts IT, avocats, conseil en communication de crise)
- Un second volet plus classique qui couvre entre autres la perte d'exploitation subie et la responsabilité civile en cas de perte / vol de données.
- Des garanties spécifiques aux risques cyber, variables selon les polices d'assurance telles que fraude informatique ou téléphonique, remboursement de la rançon, remboursement des amendes administratives, …

A noter que les assureurs associent des dispositifs de prévention pertinents.

Pour conclure, il faut rappeler que le processus de souscription d'un contrat de «cyber assurance» est vertueux car il contribue à augmenter le niveau de résilience. Et que cette démarche peut, et doit, être valorisée pour aider à sécuriser le business et/ou à remporter des appels d'offres par exemple.