Le coût des cyberattaques

Aucune entreprise, aucune administration n'est à l'abri d'une cyberattaque

En 2017, la Russie lançait une cyberattaque, surnommée **NotPetya**, par un logiciel malveillant, contre l'Estonie, avec pour but de détruire les systèmes d'Information de ce petit pays, tout en simulant un ransomware. Mais NotPetya ne s'est pas arrêté aux frontières de l'Estonie. Les entreprises qui avaient des filiales dans ce pays, par exemple St Gobain en France ont subi également des dégâts considérables.

Les dégâts économiques engendrés par NotPetya sont estimés globalement à **10 milliards de dollars**.

Aujourd'hui, les cyberattaques se multiplient. Votre entreprise est connectée à l'Internet où se trouvent vos clients, vos partenaires, où se trouvent vos employés, la question n'est plus : « *allez-vous subir une cyberattaque ?* » mais *quand serez-vous attaqué ?* Et la question sera : combien ça va vous coûter ? Pertes

financières, perte de réputation, perte de clients… Comment estimer ce coût qui justifiera aussi vos investissements pour sécuriser votre information et les systèmes qui la soutiennent.

Ce sera le thème du « Lundi de la Cybersécurité du mois d'octobre, et pour le traiter, nous avons fait appel à un expert …

Je donne la plume à cet expert, Julien CHAMONAL

Le coût des cyberattaques ne se limite pas aux pertes financières directes. Derrière chaque incident se cachent des impacts multiples — financiers, organisationnels, business et réputationnels — qui peuvent profondément affecter la trajectoire d'une entreprise.

Lors de ce Lundi de la Cybersécurité, je vous proposerai une immersion dans la démarche de **quantification du risque cyber**, qui permet de traduire les menaces cyber en scénarios économiques concrets. Cette approche repose sur des calculs probabilistes et une analyse rigoureuse de la menace : fréquence des attaques, vulnérabilités spécifiques, modes opératoires d'attaque observés. Elle permet de modéliser des risques réalistes et chiffrés, utiles pour la prise de décision.

Nous explorerons ensemble les différents types d'impacts sur la base de cas concrets liés à des attaques récentes :

- **Financiers** : interruption d'activité, coûts de remédiation, frais juridiques, pénalités réglementaires.
- **Organisationnels** : désorganisation des équipes, surcharge opérationnelle, perte de confiance interne.
- **Business** : ralentissement des ventes, rupture de partenariats, perte de compétitivité.
- **Réputationnels** : crise de communication, défiance des clients et investisseurs, atteinte à l'image de marque.

Enfin, nous évoquerons les différents cas d'usage que la quantification du risque cyber permet de couvrir :

- **justifier les budgets cybersécurité** auprès du COMEX avec des données chiffrées plutôt que des scénarios hypothétiques,
- **prioriser les investissements** en fonction de leur impact réel sur la réduction du risque financier,
- **calculer le ROI des mesures de sécurité**, en comparant leur coût à la réduction de risque qu'elles apportent,
- **communiquer des rapports adaptés au langage du comex**, facilitant les arbitrages budgétaires et les décisions stratégiques.

- En somme, vous découvrirez que quantifier le risque cyber, c'est passer d'une posture défensive à une stratégie proactive, fondée sur des données, des scénarios concrets et des décisions éclairées.

Qui est Julien CHAMONAL ?

Julien CHAMONAL est le Chief Revenue Officer (CRO) chez Citalid, une entreprise de cybersécurité basée à Paris. Il a construit sa carrière à l'intersection de la cybersécurité, de la gestion des risques et de la conformité.

Julien a commencé son parcours professionnel en 1999 chez Orange Business Services à Rennes, en France, où il a travaillé comme ingénieur sécurité, se concentrant sur des projets de sécurité avancés tels que la détection d'intrusion pour des plateformes Internet haut débit.

Au fil des années, il a dirigé de nombreuses initiatives liées à la sécurité des données, des infrastructures et a développé une expertise approfondie dans le déploiement de solutions de gouvernance et de gestion des risques dans divers secteurs.

Demande d'inscription au lundi 20 octobre, par visio-conférence à partir de 18 h 00.

Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos évènements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 20 octobre, dès 18 h 00** ou mieux, un peu avant. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. C'est toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec Anne SOUVIRA - https://www.pointdecontact.net/

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 15, nous donnons pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Cette séquence des quelques minutes avec une association sera animée par **Anne SOUVIRA**, Commissaire Divisionnaire Honoraire et ancienne Cheffe de la Mission « Cyber » de la Préfecture de Police de Paris. Elle est depuis le mois de juin, la présidente de l'association « **Point de contact** ». Cette association travaille en étroite collaboration avec le Ministère de l'Intérieur dans la lutte contre les contenus illicites sur Internet tels que les violences et exploitations sexuelles de mineurs, la provocation à la haine ou encore les contenus à caractère terroriste.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez, sur le web de l'ARCSI en **https://www.arcsi.fr/evt_passes.php** tous les détails, slides, parfois aussi les enregistrements et des comptes rendus écrits par Clarisse Véron, qui a terminé le master2 « Cybersécurité et e-Santé » de l'Université Paris Cité.

Le coin des « Lundi de la cybersécurité » suivants.

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?
Prompt posé à Gemini (l'IA Générative de Google) :

Combien coûte une cyberattaque ?

Le coût d'une cyberattaque varie considérablement, mais il est souvent très élevé et peut même entraîner la faillite d'une entreprise. Pour les organisations en France, le coût total des cyberattaques réussies a été estimé à 2 milliards d'euros en 2022. Les coûts ne se limitent pas seulement à la rançon, ils incluent aussi de nombreux frais directs et indirects.

Le coût moyen selon la taille de l'entreprise

Le coût d'une cyberattaque dépend grandement de la taille de l'entreprise ciblée. Plus l'entreprise est grande, plus l'impact financier est important.

- **PME/TPE :** Selon une étude de l'ANSSI, le coût moyen d'une cyberattaque pour une TPE ou PME peut atteindre **466 000 euros**.
- **Grandes entreprises :** Pour les grandes entreprises, ce coût peut s'élever à **135 millions d'euros**, d'après la même étude.

Ces chiffres mettent en lumière la vulnérabilité des PME, souvent moins préparées et moins solides financièrement pour se relever d'un tel incident. On estime que près de **60% des entreprises victimes d'une cyberattaque font faillite dans les 18 mois**.

Les différents types de coûts

Le coût d'une cyberattaque est complexe et se compose de plusieurs éléments, visibles et cachés.

Coûts directs

- **Rançon :** La rançon demandée par les cybercriminels, notamment dans les attaques par rançongiciel (ransomware), qui peut se chiffrer en milliers, voire en millions d'euros. Le montant moyen d'une rançon est estimé à **25 700€** par cyberattaque réussie.
- **Remédiation IT :** Les frais de restauration des systèmes informatiques, de renforcement de la sécurité, et de mise à jour des logiciels.
- **Frais d'experts :** Le coût des prestataires externes, comme les experts en cybersécurité, les avocats et les agences de communication de crise.
- **Sanctions et amendes :** Les amendes réglementaires, en particulier en cas de violation du RGPD (Règlement général sur la protection des données), peuvent être très lourdes.
- **Frais juridiques :** Les frais liés aux éventuelles poursuites judiciaires intentées par des clients ou des partenaires.

Coûts indirects

- **Pertes d'exploitation :** L'interruption de l'activité, qui peut durer plusieurs jours ou semaines, et qui génère une perte de chiffre d'affaires. C'est souvent le poste de coût le plus important.
- **Perte de données :** Le coût de la récupération ou de la reconstitution des informations perdues, qu'il s'agisse de données clients, de propriété intellectuelle ou de documents internes.

- **Atteinte à la réputation :** La dégradation de l'image de l'entreprise et la perte de confiance des clients, des fournisseurs et des investisseurs, qui peut entraîner une érosion du chiffre d'affaires sur le long terme.
- **Augmentation des primes d'assurance :** Après une attaque, les primes des assurances cyber augmentent considérablement.

Nous écouterons **Julien CHAMONAL** nous dire ce qu'il en pense. Je trouve que les dates de cette réponse de Gemini remontent à plusieurs années. Aujourd'hui, les chiffres sont en hausse. Pour 2024, j'ai le chiffre de 129 milliards de dollars.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com)

Gérard