Lettre des "Lundi de la cybersécurité" n° 84

DORA : Un précurseur pour le règlement qui succèdera à NIS2 ?

La résilience, maître mot aujourd'hui de la cybersécurité

Face aux cyberattaques qui se multiplient et qui visent tous les Systèmes d'Information et tous celles et ceux qui sont connectés, en particulier dans les secteurs de la santé et de la finance, un mot est souvent prononcé quand on parle de cyberdéfense : **la résilience**.

Quand la cyberattaque a volé, détruit, chiffré les données sensibles et dont la disponibilité est indispensable pour continuer à mener ses affaires, comment minimiser les effets de l'attaque ? Et en cas de perte de ses données indispensables, comment continuer de façon dégradée, qui appeler à son secours, à quelles autorités faut-il déclarer le sinistre ? Et comment rétablir rapidement, si c'est possible, un fonctionnement normal ? Et surtout avant l'attaque, comment minimiser le risque ?

Pour guider les entreprises de l'Union européenne à accroitre leurs capacités de résilience, la directive NIS2 donne des directions qui, après avoir été transposées dans la loi française, seront obligatoires pour les entités

concernées. Ces dispositions seront précisées pour chaque pays de l'Union européenne, et deviendront alors une loi du pays.

Dans le secteur de la finance et des assurances, le règlement DORA impose des contraintes qui pourront s'avérer salutaires. Les exigences du règlement DORA imposent que les entités financières, quel que soit leur modèle de service, mettent en œuvre des cadres efficaces de gestion des risques liés aux Technologies de l'Information et de la Communication. Ce règlement s'applique aussi aux fournisseurs de services TIC de ces entités financières.

Quels sont les rapports entre la Directive NIS2 et le Règlement DORA ?

DORA est considéré comme une « lex specialis » de la directive NIS2 pour le secteur financier. S'il y a conflit entre le règlement DORA et la directive NIS2 en droit international, la priorité devrait être donnée à la norme la plus spécifique.,

Un expert de la cybersécurité, très impliqué dans la mise en conformité d'une grande banque avec le Règlement DORA nous l'expliquera au cours de notre Lundi de la Cybersécurité du mois de septembre, le lundi 22 septembre 18h-20h, par webinaire. **Les inscriptions sont ouvertes**.

Je donne la plume à cet expert, Christophe ROUBERTIE

Le secteur financier est essentiel au fonctionnement des sociétés non autarciques, c'est à dire dont les chaines d'approvisionnement s'étendent au-delà du périmètre d'un village.

Le fonctionnement d'un système financier nécessite la confiance des parties prenantes, notamment des clients. Celle-ci repose, en plus de garanties solides sur la solvabilité des établissements, sur l'assurance que l'ensemble des opérations effectuées par les acteurs du secteur le soient avec le niveau d'intégrité des données et des transactions, de confidentialité et de continuité de service les plus élevées.

Dans un contexte où le traitement informatique a remplacé le papier et où les systèmes sont interconnectés, entre autres via Internet, la cybersécurité est cruciale pour apporter ces garanties.

Le règlement sectoriel européen DORA (Digital Operational Resilience Act), qui s'applique depuis le 17 janvier 2025, cadre la démarche de cybersécurité pour le secteur financier, les assurances, les organismes de retraite supplémentaire.

Il repose sur 5 piliers qui sont le cadre de gestion des risques, la notification des incidents aux autorités de contrôle, les tests de résilience, le partage d'informations avec les pairs, et la gestion des risques liés aux fournisseurs IT.

Quelles sont les obligations en termes de formalisation du cadre de gestion des risques, de notification des incidents, de tests de résilience ?

Quelles sont les obligations en matière d'identification des risques dans la chaîne de sous-traitance informatique, de sécurisation contractuelle et opérationnelle ? Quel est l'impact sur la structure de la chaine de sous-traitance, le choix des sous-traitants, les coûts ?

Quels enseignements à en tirer pour les autres secteurs, dont les organisations seront soumises à la directive NIS2 une fois celle-ci transposée ?

Qui est Christophe ROUBERTIE ?

Christophe ROUBERTIE est titulaire des DESS Réseaux et Applications Distribuées de l'Université Paris-VI et Administration des Entreprises de l'IAE de Paris.

Après un début de carrière en ESN, il a intégré PSA Peugeot-Citroën à l'informatique (DTII), puis a rejoint la Direction du Contrôle de Gestion où il a contribué à la refonte du programme gestion puis a contrôlé plusieurs divisions, dont Banque PSA-Finance.

Depuis 2010, il agit pour BNP Paribas Personal Finance sur différents sujets Finance / Conformité, en lien avec les problématiques réglementaires, de maîtrise des processus, et de pilotage du risque et de la performance, sur le périmètre mondial couvert par le Groupe.

Il termine actuellement le MBA Management de la Cybersécurité de DeVinci Executive Education. Sa thèse professionnelle porte sur le respect des exigences DORA dans un environnement Cloud.

Demande d'inscription au lundi 22 septembre, 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 vers 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 22 septembre, 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 Murielle THIBIERGE-BATUDE

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 du « Lundi de la Cybersécurité » de septembre sera animée par **Murielle Thibierge-Batude, présidente de l'association #IWAS** qui réinjecte nos savoirs cyber pour la défense des petits enfants.

#IWAS La lutte contre la malveillance pédo-criminelle n'est pas radicalement différente de la lutte contre les cybercriminels en ce sens qu'il s'agit bien d'un hack aussi : le hack des protecteurs des enfants qui se laissent berner et des enfants qui sont souvent manipulés.

L'approche de l'intelligence adverse est double : draguer l'adulte pour in fine avoir l'enfant le plus longtemps et discrètement possible. Sans oublier la mise en œuvre de soumission chimique...

La malveillance interne existe aussi : des personnes ayant acquis pour l'enfant une élévation de privilèges se trouvent en fait être les pires des prédateurs (multiples affaires). Enfin certains parents même français utilisent leurs enfants en streaming et là seul le voisinage, vous les citoyens, citoyennes, vous devez faire preuve d'un esprit averti que ce n'est pas juste à l'étranger dans les pays pauvres etc ... mais bien chez nous, avec nos enfants, et sous nos yeux.

Rien n'empêche de remettre en œuvre la méthode d'analyse des risques, le système de management de la sécurité, tout notre corpus de termes de la cyber pour déjouer les plans pédo-criminels, on a juste besoin de vous !

Murielle interviendra avec Simon BAILEY, voir qui est ce responsable anglais de la lutte contre la pédo-criminalité en :
https://policing.tv/videos/former-simon-bailey-discusses-child-exploitation-and-child-protection-part-1

Vous voyez le poing fermé de Murielle sur la photo : Elle défend fermement les pré-verbaux ! Il y aura des annonces concrètes ! Et elle assurera la traduction en français des propos de Simon Bailey.

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 termine le master2 « Cybersécurité et e-Santé » de l'Université Paris Cité.

Mais attention, pour des questions de confidentialité société, Christophe ROUBERTIE ne souhaite pas que son intervention soit enregistrée, donc il est conseillé d'être connectés pour le suivre par Zoom et pour lui poser des questions ainsi qu'à Murielle.

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) :

Le règlement Dora succèdera-t-il à la directive NIS2 ?

Non, le règlement DORA ne succédera pas à la directive NIS2. Ils sont **complémentaires** et coexisteront, mais avec des champs d'application différents et des priorités spécifiques.

Voici les points clés pour comprendre leur relation :

- **DORA (Digital Operational Resilience Act)** : C'est un **règlement** européen. Cela signifie qu'il est directement applicable dans tous les États membres de l'UE à partir du 17 janvier 2025, sans nécessiter de transposition dans les lois nationales. Il se concentre **spécifiquement sur le secteur financier** (banques, assurances, prestataires de services de paiement, etc.) et leurs prestataires de services TIC critiques. L'objectif est de renforcer la résilience opérationnelle numérique de ces entités face aux cybermenaces et aux perturbations informatiques. DORA est considéré comme une "lex specialis" (loi spéciale) par rapport à NIS2 pour le secteur financier.
- **NIS2 (Network and Information Security 2)** : C'est une **directive** européenne qui a renforcé la première directive NIS. Elle doit être transposée dans les lois nationales des États membres (date limite : 17 octobre 2024). NIS2 a un champ d'application beaucoup plus large, couvrant une grande variété de **secteurs critiques** (énergie, transports, santé, infrastructures numériques, eau, administration publique, etc.). Son objectif est d'améliorer le niveau global de cybersécurité et de résilience des réseaux et systèmes d'information dans l'UE.

En résumé :

- **DORA** est une loi spécifique et plus exigeante pour le **secteur financier**.
- **NIS2** est une loi plus générale couvrant un large éventail d'autres **secteurs critiques et importants**.

Pour les entités du secteur financier, c'est principalement DORA qui s'appliquera, et les exigences de NIS2 continueront de s'appliquer pour les aspects non couverts par DORA ou si l'entité opère également des services critiques relevant de NIS2. Il y a une volonté d'harmonisation entre les régulateurs pour limiter les doublons et assurer une approche cohérente.

Nous écouterons Christophe ROUBERTIE nous dire ce qu'il en pense. Je trouve cette réponse de Gemini très juste, sauf pour NIS2, la date limite du 17 octobre 2024 qui n'a pas été tenue.

Gérard