

LE LIVRE BLANC CYBERDAY2020

CYBER-DAY.INFO

2020

by veillemag en partenariat avec EGE

Paris, 11 mars 2020

ORGANISÉ PAR VEILLE MAGAZINE
EN PARTENARIAT AVEC EGE/AEGE
CLUB CYBERSÉCURITE

3^{ème} édition
Ecole de Guerre Economique

>> cyber-day.info

11 mars 2020

196, rue de Grenelle, 75007 PARIS

CONFÉRENCES DÉBATS WORKSHOPS RENCONTRES

DE LA SÉCURITÉ
DE L'INFORMATION À UNE
CYBER-GOUVERNANCE MÉTIERS

EGE Ecole de Guerre Economique

Veille mag.com



Cybers-sécurité · Cyber-gouvernance · Cyber-résilience
Ce livre blanc s'enrichira régulièrement de nouveaux articles.
Nous vous tiendrons informés
Continuez à nous donner vos avis, à nous poser vos questions ...
www.cyber-day.info · #cyberday

LE CYBER DAY 2020 A DE NOUVEAU TENU SES PROMESSES : ÉTAT DES LIEUX ET TOUR D'HORIZON



The image shows a promotional poster for Cyber Day 2020 on the left and a summary box on the right. The poster features a dark background with a network of blue and red nodes and lines. Text on the poster includes: "3^{ème} édition Ecole de Guerre Economique", "cyber-day.info", "11 mars 2020", "196, rue de Grenelle, 75007 PARIS", "CONFÉRENCES DÉBATS WORKSHOPS RENCONTRES", "DE LA SÉCURITÉ DE L'INFORMATION À UNE CYBER-GOUVERNANCE MÉTIERS", and logos for EGE (Ecole de Guerre Economique) and Veille (veille.org.com). The summary box on the right has a large quote icon at the top, followed by the text "Au fil d'une journée". Below this, in a dark blue section, it lists "Quelques focus rencontres débats workshops ***".

par Laurence Dubrovin, Analyste Conseil, Expert
BI/Analytics/IA, CRM/CxM & MDM

#cyberday. Ils nous font confiance. Nos partenaires

EGE Ecole de Guerre Economique



Veillemag.com

CESIN

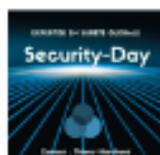


onepoint.
beyond the obvious

CYBER CERCLE

GAC GROUP

ISSA
Information Systems Security Association
France Chapter



I.E.S.A.S

AQUILA

Lawint

ELYSIUM SECURITY



CGI

m8

oic
Observatoire International des Crises
OIC

Cyberologue

SOMMAIRE

- Conférence d'ouverture.
- Conférence sur la psychologie et l'iA au service de la sécurité de votre entreprise par Cleverm8
- Conférence Innovation x Humain x Cyber sécurité : comment vous assurer de protéger la valeur de ce que vous créez ? Gac Group
- Conférence Nouveaux défis. La cyber résilience face au Covid-19. Gestion de crise et plan de continuité. Cabinet Heiderich
- Conférence CESIN - 5ème édition du baromètre annuel. De l'urgence de nommer des Directeurs de la Cyber sécurité ?
- Conférence sur l'évolution des politiques de sécurité avec l'émergence du Cloud
- Conférence Sécuriser les usages, un rempart à la déstabilisation économique, politique et sociétale. ISSA FRANCE

www.cyber-day.info - suivez-nous

www.cyber-day.info - Programme

MERCREDI 11 MARS - 197 RUE DE GRENELLE 75017 PARIS

CONFERENCES

- Défis 2020. Invités : Catherine MORIN-DESAILLY, Sénatrice. Philippe LAVAULT, Chef des Ressources extérieures ANSSI.

9h00/9h45.

- Assurance cyber : sécuriser son business et limiter les impacts

9h45/10h30

- Innovation x Humain X Cybersécurité : Comment vous assurer de protéger correctement la valeur que vous créez ?

10h45/11h30

- Nouveaux défis. La Cyber-Résilience face au Covid19. Gestion de crise et Plan de continuité

11h45/12h30

- CESIN - 1/ 5ème édition du baromètre annuel - 2/ De l'urgence de nommer des Directeurs Cybersécurité ?

14h00/14h45

- L'évolution des politiques de sécurité avec l'émergence du cloud

15h00/15h45

- Sécuriser les usages : Un rempart à la déstabilisation économique, politique et sociétale.

16h00/16h45

- Table ronde de clôture : Principaux enseignements 2020. Nos invités nous rejoignent

17h00/17h45

WORKSHOPS

La psychologie et l'IA au service de la sécurité de votre entreprise. CleverM8.

Cyber résilience et retour d'expérience. One point

Pourquoi la cybersécurité est aujourd'hui une obligation légale ? Lawint

Stratégie technologique, financière et marketing de l'innovation Cyber et IT. Gac Group

Security-Day.com. Ensemble, demain sera plus sûr. Matinale #1 Rendez-vous 18 juin 2020

Infrastructures numériques, une filière industrielle à haut risque

 On se retrouve Mercredi 11 mars 2020. On compte sur vous !

LE CYBER DAY 2020 A DE NOUVEAU TENU SES PROMESSES : ÉTAT DES LIEUX ET TOUR D'HORIZON

Par Laurence Dubrovin



Le Cyber day organisé chaque année par Veille Magazine s'est déroulé le 11 mars dernier à l'EGE (Ecole de Guerre Economique) peu avant les mesures de confinement demandées par les autorités gouvernementales. Plus de 350 participants étaient réunis : des intervenants issus de tous horizons - fournisseurs et utilisateurs de solutions - et de nombreux auditeurs avaient répondu à l'appel. Pas moins de 8 conférences et 5 workshops se déroulaient tout au cours de la journée. Des sujets passionnants étaient abordés sous différents angles : stratégie, métier et technique. Retour sur cette journée par Laurence Dubrovin Analyste Conseil, Expert BI/Analytics/IA, CRM/CxM & MDM.

Conférence d'ouverture

La conférence d'ouverture sur les défis 2020 de la cyber sécurité réunissait Mme Morin Desailly, sénatrice et M. Philippe Lavault, chef des ressources externes de l'ANSSI. Des plans de formation sont nécessaires pour monter en compétences en France. Les entreprises du CAC 40 sont prêtes, en revanche pas les PME-PMI. Il faut aussi organiser notre cyber défense par des systèmes à la fois défensifs et offensifs.

Enfin, il convient d'investir en R&D sur nos propres technologies, de mener une politique industrielle puissante et enfin de se positionner sur un Web durable et éthique.

Les points à retenir :

- Stimuler les initiatives publiques en France
- De l'importance de construire une cyber sécurité européenne
- Accompagner la cyber civilisation, en particulier avec l'IoT

Conférence sur la psychologie et l'iA au service de la sécurité de votre entreprise par Cleverm8

La plateforme Sensefact basée sur les APIs de Cleverm8 couvre les domaines suivants : management et RH, ventes et marketing, cyber sécurité.

De quels risques parle-t-on ?

Monter une clé USB sur son PC, avoir des discussions à caractère privé en public, divulguer des informations de façon involontaire, spontanée ou provoquée, se faire passer pour une entité avec un lien à cliquer ou une pièce jointe à télécharger (Phishing ou hameçonnage), hacker un forum de discussion en le branchant sur un autre, faire payer une fausse application sur smartphone sont autant de risques à prévenir dans un cyber espace.

Alors comment prévenir ces situations ?

Sensefact travaille sur la détection des comportements face aux menaces : selon les personnes l'attitude diffère et peut être risquée, méfiante ou bien défensive. Ceci est aussi lié à la multiplicité des lieux, des moyens et des sujets à traiter.

organise by veilemag en partenariat avec l'EGE



Ces attitudes sont aussi à corréliser avec la protection et la conscience qu'en a l'utilisateur à tous les niveaux (données, supports, cloud, accès, virus). Elles sont également à regarder sous l'angle de la collaboration et du niveau d'exposition (plateforme, recherches, documents, outils, espaces, réseaux).

La plateforme analyse les connaissances, les risques et détecte les failles humaines chez les personnes et leurs attitudes face aux crises.

Pour anticiper ces failles humaines, il convient de mettre en place une stratégie adaptée aux personnes de l'entreprise, d'améliorer les outils de sécurité, enfin de proposer des formations personnalisées.



Sensefact qui s'appuie sur Cleverm8, brique d'intelligence artificielle différenciatrice, est une application destinée à résoudre ces questions de psychologie au service de la cyber sécurité. Cette technique d'IA est en mesure de détecter les exceptions, repérer les cas rares et donc individuels, contrairement aux autres techniques d'IA (système expert basé sur des règles pour automatiser des processus relativement simples, et machine learning pour catégoriser et trouver des similitudes pour automatiser des tâches générales répétitives).

Conférence Innovation x Humain x Cyber sécurité : comment vous assurer de protéger la valeur de ce que vous créez ?

St Gobain en 2017 a subi une cyber attaque qui a détruit ses données, l'hôpital de Rouen ne pouvait plus accepter de nouveaux patients suite à une cyber attaque, une agence matrimoniale a vu publier ses données personnelles par ceux qui n'appréciaient pas son activité ce qui a engendré des catastrophes humaines, le logo Orange a été utilisé pour une publicité mensongère sur la 6G, etc.

Nombreux sont les exemples de cyber-attaques qui ont des conséquences lourdes pour les entreprises ou organismes touchés.

Il convient en particulier de faire évoluer le savoir-être des collaborateurs au sein des entreprises et d'être vigilant sur les aspects suivants :

- Les cyberliens et les sites sur lesquels ils pointent
- Les logiciels à charger (shadow IT)
- Les réseaux sociaux et ce que l'on partage dessus
- Les échanges privés dans les lieux publics
- L'intégration de la sécurité de la conception (« secure by design ») jusqu'au développement et à la maintenance (« secure by default »)
- La capacité de résilience du SI : être en mesure de se reconstruire après une attaque, à l'image d'un système auto-immun.



CYBER-DAY 2020
11/03/20 - EGE - PARIS

**CYBERSECURITE
INNOVATION**

COMMENT PROTÉGER
LA VALEUR QUE VOUS CRÉEZ ?

Veille mag.com GAC GROUP EGE Ecole de Guerre Economique TRUS



Les points à retenir :

- Instaurer une politique de sécurité descendante, insufflée par la Direction Générale
- Sensibiliser le plus grand nombre aux risques de cyber attaque
- Former des experts en cyber sécurité
- Investir en trouvant un équilibre entre coûts de prévention et coûts en cas de cyber attaque

Nouveaux défis. La cyber résilience face au Covid-19. Gestion de crise et plan de continuité. Cabinet Heiderich

Il est intéressant d'établir un parallèle entre un virus informatique et un virus biologique. En effet, dans les 2 cas :

- Le virus a besoin d'un hôte (programme hôte vs cellule hôte)
- Il se propage (réseau informatique vs réseau humain)
- Il crée des dommages (destruction totale ou partielle de l'hôte)
- Son analyse passe par les datas car des mutations sont possibles
- -Il nécessite d'être isolé pour réduire la menace (segmentation des réseaux vs confinement)
- Dans le cas du virus biologique, il convient d'examiner les risques pour l'entreprise et son organisation :
 - -Contamination interne
 - -Absentéisme
 - -Personnes clés malades
 - -Défaillances du côté fournisseur
 - -Pertes de marché
 - -Continuité d'activité

Coronavirus Covid-19



Et les autres risques associés :

- RGPD
- Réglementation
- Règles de gestion et RH
- Contamination d'un client, fournisseur ou prestataire
- Protection juridique

Il convient d'identifier les lieux possibles de contamination : Open space, matériel en partage, lieux de passage, salles de réunion, cantine, transports en commun. Des incertitudes existent sur l'étendue du phénomène, la durabilité et les mutations possibles. Des questions se posent sur le stade de propagation, les personnes infectées, les retours de mission de zones infectées, le droit de retrait, les doutes sur les prestataires etc.

COVID-19

Les recommandations sont les suivantes :

- Doter la DSI de masques de protection
 - Scinder les équipes pour éviter la propagation
 - Faire un point régulier avec les prestataires critiques
 - Vérifier la capacité matérielle et technique pour supporter un grand nombre de télétravailleurs
 - Vérifier la capacité de chaque service à assurer ses missions en télétravail
 - Etablir des règles pour la maintenance du matériel des collaborateurs
- Il est nécessaire que la DSI accompagne cette période par des mesures spécifiques :
- Télétravail
 - Gestion des accès
 - Réservation des salles
 - Informations sur Intranet
 - Modification des règles d'utilisation du matériel informatique
 - -Mémoire des présences et liens inter- personnes en cas de personne malade
 - Organisation d'une cellule de crise pour fonctionner à distance
 - Gestion du retour à la normale et reprise des activités
 - Il convient d'observer la prudence en matière de collecte des données :
 - -Travailler de concert avec le DPO (Délégué à la Protection des Données)
 - -Les employeurs ne peuvent pas prendre des mesures susceptibles de porter atteinte au respect de la vie privée, notamment la collecte des données de santé (CNIL)
 - L'employeur doit suivre les préconisations du médecin du travail en cas de signalement (CNIL)



Il est nécessaire que la DSI accompagne cette période par des mesures spécifiques :

- Télétravail
- Gestion des accès
- Réservation des salles
- Informations sur Intranet
- Modification des règles d'utilisation du matériel informatique
- Mémoire des présences et liens inter- personnes en cas de personne malade
- Organisation d'une cellule de crise pour fonctionner à distance
- Gestion du retour à la normale et reprise des activités



**Enfin, il ne faut pas attendre qu'un phénomène viral se produise pour s'y préparer, il faut l'anticiper.
Il faut donc se préparer à l'imprévisible.**

Il convient d'observer la prudence en matière de collecte des données :

- Travailler de concert avec le DPO (Délégué à la Protection des Données)
- Les employeurs ne peuvent pas prendre des mesures susceptibles de porter atteinte au respect de la vie privée, notamment la collecte des données de santé (CNIL)
- L'employeur doit suivre les préconisations du médecin du travail en cas de signalement (CNIL)

Enfin, il ne faut pas attendre qu'un phénomène viral se produise pour s'y préparer, il faut l'anticiper. Il faut donc se préparer à l'imprévisible.



14h00/14h45.

CESIN

1/ 5ème édition du
baromètre annuel

2/ RSSI : vers un Directeur
Cyber Sécurité ?

Alain Bouillé (Délégué Général at CESIN - Club des Experts de la Sécurité de l'Information et du Numérique répond aux questions de
Jérôme Fréani (Cybersecurity consultant / Head of Cyber club @AEGE / Founder @Cyberologue)

Conférence CESIN - 5ème édition du baromètre annuel. De l'urgence de nommer des Directeurs de la Cyber sécurité ?

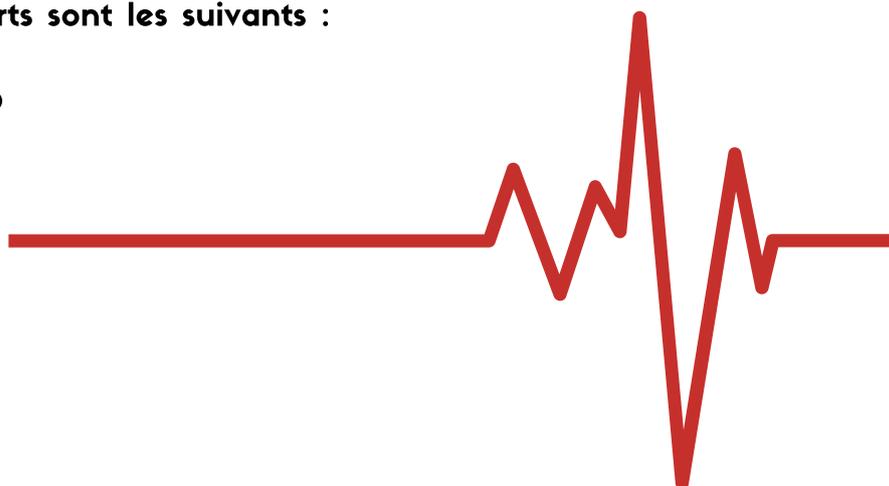
Le CESIN (Club des Experts de la Sécurité de l'Information) est francophone et compte 600 membres. Son dernier baromètre analyse 253 réponses sur 634 contacts. Alain

Le panel des entreprises qui ont répondu est le suivant :

- 22% ont plus de 50 000 salariés**
- 25% ont entre 1000 et 4999 salariés**
- 8% ont moins de 250 salariés**

Les secteurs d'activités couverts sont les suivants :

- 47% pour le service**
- 21% pour l'industrie et le BTP**
- 17% pour les services publics**
- 13% pour le commerce**



Voici les principaux résultats de l'enquête :

- 39% des entreprises disent être préparées à une cyber attaque de grande ampleur (soit seulement 4 entreprises sur 10)
- Parmi les principales solutions mises en place, 85% des entreprises mettent en oeuvre une passerelle de sécurisation pour les mails et également une passerelle VPN/SSL, 83% un proxy et un filtrage des URL.
- Les offres innovantes en cybersécurité issues des startups séduisent 4 entreprises sur 10
- La majorité des entreprises considèrent que les solutions de cyber sécurité proposées sont adaptées
- 91% des entreprises ont mis en place un programme de cyber résilience ou envisagent de le faire
- Il existe une grande défiance vis-à-vis du programme ZeroTrust (qui consiste à ne faire confiance à personne), même si un peu plus d'une entreprise sur 10 a commencé à le mettre en oeuvre
- 60% des entreprises ont souscrit à une cyber assurance
- 65% des entreprises déclarent avoir eu une cyber attaque (soit plus de 2 entreprises sur 3)
- En moyenne, les entreprises subissent plus de 15 cyber attaques par an (soit plus d'une par mois)
- Les cyber attaques impactent en premier lieu la production dans 27% des cas
- Le phishing (hameçonnage) reste en tête des vecteurs d'attaque constatés (79%), suivi de l'arnaque du président (47%)
- L'usurpation d'identité et l'infection par malware sont les conséquences les plus fréquentes des attaques
- En lien avec la cyber sécurité, la négligence des salariés est souvent la cause
- 89% des entreprises stockent au moins une partie de leurs données dans le Cloud.

Conférence sur l'évolution des politiques de sécurité avec l'émergence du Cloud. One Point



Le cloud prend de jour en jour une place de plus en plus importante dans les entreprises. Il offre la promesse d'une plus grande agilité et d'un Time To Market sensiblement raccourci.

Avec l'émergence du Cloud, voici deux nouveaux risques en termes de stratégie diamétralement opposés :

- ne pas avoir de politique de sécurité
- ou au contraire vouloir tout maîtriser avant de se lancer.

La première nécessité pour construire sa stratégie Cloud est de d'acculturer le sujet.

En effet, passer en mode Cloud est un changement de culture pour toutes les fonctions IT (développement, production, sécurité).

L'entreprise est aussi exposée à des risques différents par l'ouverture de son SI sur l'extérieur, ce qui prend du temps et nécessite éducation et sensibilisation.

Pour relever les défis de la cyber sécurité dans le Cloud, il convient de rencontrer plusieurs fournisseurs, de suivre des formations, de passer des certifications, de s'appuyer sur les frameworks du marché, de solliciter aussi l'expertise technique externe.

Dans tous les cas, il faut adopter une approche par les risques car elle sera identique quelles que soient les techniques retenues. Le Cloud vient juste changer la façon d'implémenter les préconisations, c'est en cela qu'il apporte des gains.

Quels sont les acteurs du Cloud ?

On distingue 2 catégories d'acteurs de Cloud :

- **Les high providers** : leurs offres sont orientées « security by design » ce qui requiert de tout déclarer. Un ensemble de services de sécurité sont fournis. Enfin, ces solutions sont très sécurisées : les données sont dupliquées sur x serveurs et chiffrées.

- **Les autres providers Cloud** : ils sont moins complets et nécessitent une approche plus dirigiste en termes de sécurité.

Il est important de vérifier que ces fournisseurs sont certifiés (Soc2, etc.)

Quelle stratégie sécurité adopter ?

- La fonction sécurité doit être impliquée dans les processus de décision de l'entreprise
- La fonction sécurité doit avoir une posture de veilleur et non de suiveur vis-à-vis du Cloud et anticiper les évolutions technologiques
- La fonction sécurité doit structurer et décliner sa stratégie
- La stratégie sécurité doit se définir par une approche par les risques (voir plus haut)

Quels sont les nouveaux risques liés au Cloud ?

A titre d'exemple comment se protéger du data breach (violation des données), l'un des principaux risques associés au Cloud computing ?

- Chiffrer ses données (un expert en sécurité conseille de le faire en local et pas sur le Cloud, le Cloud devenant essentiellement un espace de stockage et de calcul des données déjà chiffrées)
- Mettre en place un mécanisme de clé privée (jeton privé) pour éviter qu'un concurrent ne pénètre dans le système par user id, nom et prénom
- Construire des environnements et une infrastructure de manière à surveiller le trafic
- Vérifier que les autorisations d'accès des administrateurs de la solution soient conformes c'est-à-dire mises en oeuvre à l'aide d'un protocole de type « need-to-know, need-to-access protocol »
- Passer par un CASB (Cloud Access Security Broker) qui agit comme une sentinelle et garantit les entreprises que leurs données sont sécurisées de bout en bout, du cloud au périphérique et vice versa, pour les appareils, les emplacements et les utilisateurs autorisés.
- Travailler avec une approche par les risques, chaque risque nécessite la mise en place de mesure de sécurité, et chaque mesure de sécurité doit être déclinée en fonction du fournisseur Cloud.



Comment accompagner efficacement les initiatives associées au Cloud ?

Quand les initiatives Cloud se multiplient, l'émergence de multiples environnements Cloud impose la mise en place d'une gouvernance,

- d'une part dans la répartition des responsabilités entre les équipes de développement et les métiers,
- d'autre part dans l'organisation des environnements de développement, de tests et de production de façon à bien cloisonner les environnements de chaque projet.

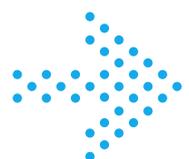
Comment le Cloud permet-il de mieux gérer la crise ?

Les apports du Cloud résident dans les services de résilience qu'il propose :

- **Le DRaaS (Disaster Recovery as a service)** : la récupération en tant que service est une catégorie de Cloud utilisée pour protéger une application ou des données d'une catastrophe.
- **Le RaaS** : Resilience as a Service : la résilience en tant que service est une catégorie de Cloud utilisée pour reconstruire un système après une attaque.
- **Le BaaS (Back-up as a Service)** : la sauvegarde en tant que service à la demande n'est pas réalisée sur site mais via un Cloud privé, public ou hybride géré par un prestataire.

Il existe plusieurs niveaux de maturité dans l'adoption du Cloud :

- Niveau 1 : le Cloud vu comme une menace
- Niveau 2 : le Cloud vu comme une opportunité
- Niveau 3 : le Cloud non considéré comme un partenaire de confiance
- Niveau 4 : le Cloud considéré comme un partenaire de confiance





Sécuriser les usages, un rempart à la déstabilisation économique, politique et sociétale. Issa France

**Sécuriser les usages :
Un rempart à la
déstabilisation économique,
politique
et sociétale.**

ISSA
Information Systems Security Association
France Chapter

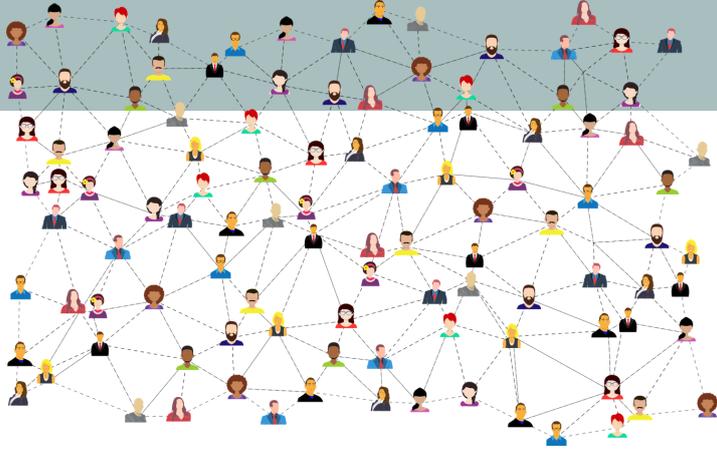
#cyberdayinfo
CYBER-DAY.INFO
L'effort de protection des ISE
Paris, 11 Mars 2020
11 MARS 2020

L'humain
Clé de voute
de la cybersécurité

Diane Rambaldini. Entrepreneur - Fondatrice Crossing Skills | Sécurité numérique
Hadi El-Khoury. co-fondateur du chapitre français de l'Information Systems Security Association (ISSA)
Anne-Charlotte Brou, division communication, responsable du bureau presse. pilote du mois de la cyber

L'obligation de sécuriser les données dans notre société est liée au respect de la vie privée.

Les exemples en la matière sont légion :
le projet Safari dans les années 70 qui a donné lieu à la loi de de 1978 informatique et libertés,
l'affaire plus récente de Benjamin Grivaux qui suite à une maladresse personnelle le conduit à une catastrophe politique.
Le manque de culture autour de la sécurité a souvent des conséquences désastreuses pour les individus.



La sensibilisation dans les faits ne se voit pas beaucoup au niveau des entreprises, de l'État et des associations.

Cependant, les droits européens de la cyber sécurité se construisent peu à peu. Une agence de cyber sécurité a été lancée en 2013. Elle permet de relayer des messages autour de la sécurité numérique que chaque pays organise selon ses moyens et ses ressources. Des actions gouvernementales sont engagées en ce sens depuis 4 ans. Chaque ministère sensibilise au sujet son personnel en interne.

Les organisations professionnelles se mobilisent également pour relayer les messages communs à tenir et à partager. Mais les moyens engagés ne sont pas encore suffisants pour toucher le grand public. C'est pourquoi relayer les messages auprès de la société civile devient une priorité.

Dans ce cadre, une plateforme d'information a été créée en 2020 pour rendre les messages plus intelligibles au grand public. Il convient de mettre en valeur les nouvelles ressources créées et mises à disposition : documents pédagogiques, kit sur les attaques et les bonnes pratiques à observer. L'enjeu est de taille car il s'agit de travailler sur les éléments de langage et de vulgariser ces notions pour le grand public.

Ainsi, l'État met en place des moyens coercitifs (radars) pour informer les personnes, par exemple en touchant leur affect. Mais comme souvent les moyens coercitifs sont insuffisants, l'État diffuse des chiffres (ex : dans le secteur de la santé, les chiffres sur le sida ou encore le coronavirus).

Concernant, les bonnes pratiques à respecter, un vaste chantier de formation/sensibilisation est à lancer comme par exemple l'usage des mots de passe qui souvent est le même au travail et à domicile.

Mais comment vérifier ces mauvais usages et les prévenir ?

Pour marquer les esprits, l'expérience montre qu'il faut toucher l'affect des personnes. De nombreux exemples ont montré leur efficacité. Le Titanic a voulu aller plus vite pour atteindre New York. Mais comment ne pas avoir anticipé les chocs possibles du navire sur la banquise et ce malgré les alertes reçues ? C'est en voyant la souffrance des gens qui sombrent en mer que cet accident mortel est resté gravé dans les mémoires. Autre exemple : au Canada, des gens du bâtiment portent en souvenir d'un pont qui s'est effondré une bague au doigt de la matière du pont.



Plusieurs décisions s'imposent face aux multiples dérives du digital

- Faire signer un serment aux personnes qui travaillent dans le secteur de la cyber sécurité, à l'image de celui d'Hippocrate pour les médecins
- Ne pas faire confiance aveuglément aux plateformes
- Limiter les risques d'exposition, en particulier les enfants en exerçant notre droit de parentalité numérique (la moitié des enfants héritent très tôt du téléphone portable de leurs parents qu'ils n'ont même pas demandé...)

Quid de l'éducation numérique à destination des enfants ?

Les parents sont les premiers à devoir enseigner les bonnes pratiques du numérique à leurs enfants telles que :

- Ne pas exposer trop jeunes les enfants au numérique
- Les inciter quand ils sont adolescents à ne pas diffuser aux amis leur mot de passe
- Les sensibiliser aux enjeux et risques du numérique (voir les cahiers de vacances à télécharger depuis le site : www.security.com)
- Les accompagner dans leurs débuts de vie numérique

voir interviews postés sur Youtube
depuis le portail www.portail-ie.fr



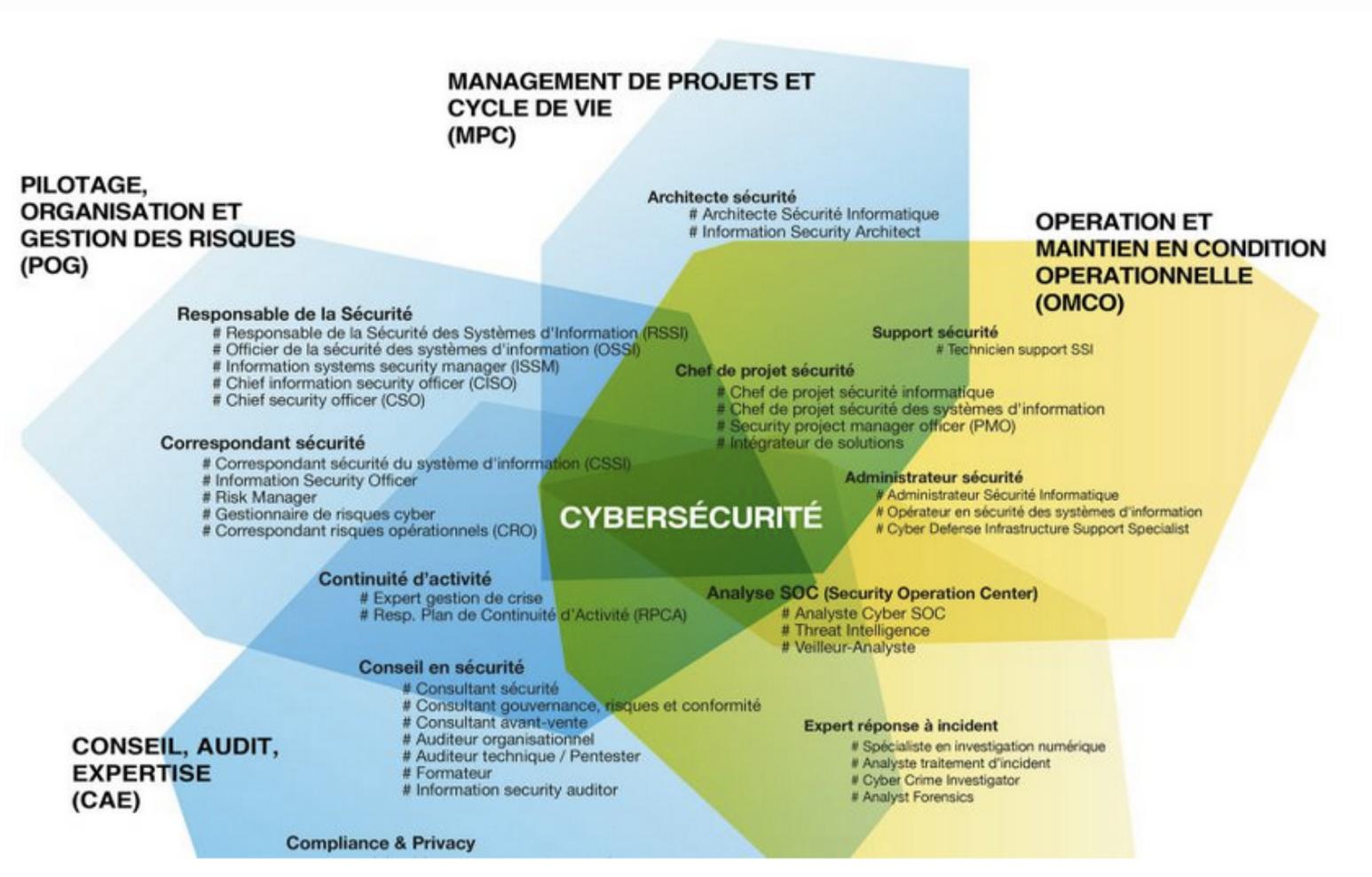
Par ailleurs, nous avons eu la chance de pouvoir réaliser le Cyberday avant la crise. Il a rassemblé, une fois de plus cette année, plusieurs centaines de participants pour assister aux ateliers et conférences. Pour la première fois, l'intégralité des présentations ont été filmées. Plusieurs sont déjà disponibles sur YouTube. Profitez du confinement pour développer vos connaissances et revivre ensemble cette journée passionnante.

CONFÉRENCE DE CLÔTURE : QUELS ENSEIGNEMENTS POUR 2020 ?

Les principaux enseignements et points de vigilance pour 2020 en matière de cyber sécurité à retenir :

- Eduquer les enfants sur l'ergonomie et les risques du numérique car il immerge désormais toutes les facettes de notre vie : ils savent tous cliquer mais ne savent pas du tout ce qui est derrière un clic.
- Former l'humain à s'organiser et à avoir conscience des enjeux de la sécurité
- sensibiliser les individus et les entreprises à la cyber sécurité pour prévenir les attaques et organiser la cyberésilience pour réparer les attaques.

S'appuyant sur le retour "terrain" des diplômés de l'Ecole de Guerre Economique, le club Cyber de l'AEGE et l'Ecole de Guerre Economique publient la "Cartographie des métiers de la Cybersécurité", afin de mettre en exergue les évolutions de la Cybersécurité.



JULY 2020 | ISSUE 7

CYBERDAY C'EST AUSSI ...

Des Avis d'experts
Des news
des rendez-vous
des personnalités
à découvrir
toute l'année

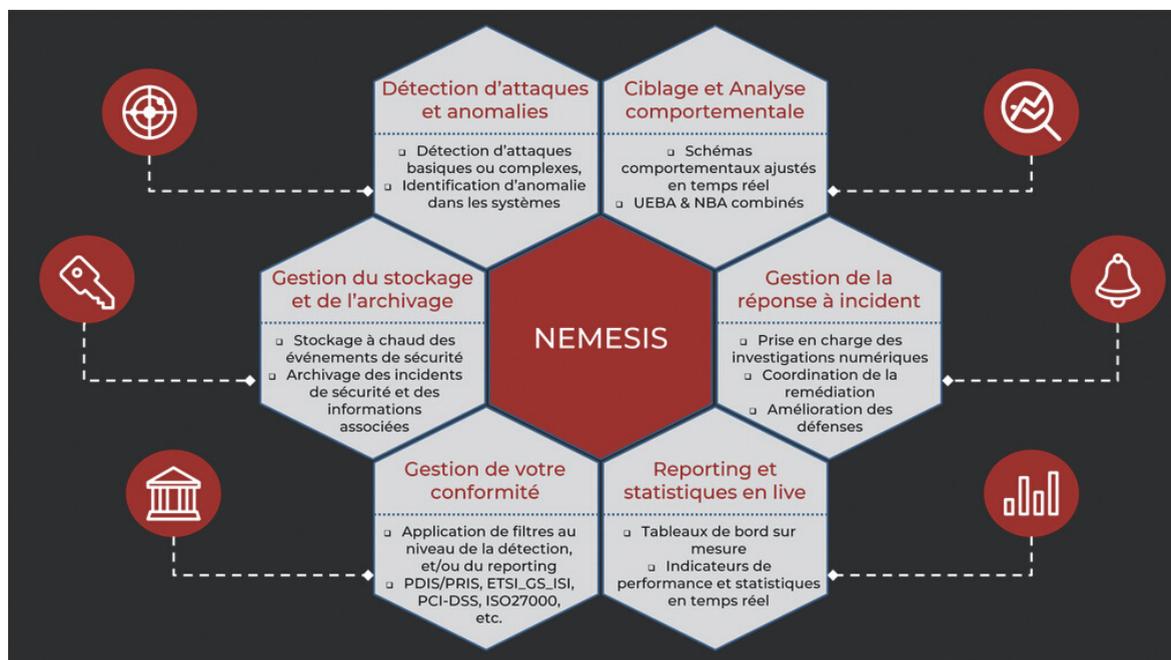
Cybers-sécurité
Cyber-gouvernance
Cyber-résilience

Ce livre blanc s'enrichira
régulièrement de
nouveaux articles.
Nous vous tiendrons
informés ...
jsala@veillemag.com



ELYSIUM SECURITY AU-DELÀ DE LA NÉCESSAIRE MAÎTRISE DE LA CYBERSÉCURITÉ, LA CYBERGOUVERNANCE EST UNE OPPORTUNITÉ

Par Cynthia Glock



Fournisseur français de services et de solutions de sécurité informatique, Elysium Security est l'un des partenaires de Cyber-Day 2020. La crise du Coronavirus ne nous a pas permis d'ouvrir le workshop prévu pour lancer la nouvelle version de sa solution logicielle de sécurité NEMESIS. Mais qu'à cela ne tienne, nous prenons dans cet article le relais pour vous en dire plus sur cette nouvelle version.

L'un de ses trois co-fondateurs, qui en est aussi le président, Sébastien Dartigalongue s'est également intéressé très particulièrement, en partenariat avec Olivier Queval-Bourgeois (Aquila-Eyes) à la "la Performance financière par la Maîtrise des informations" que nous vous révélerons bientôt.

FOCUS : NEMESIS PAR ELYSIUM SECURITY

Douvez-vous nous expliquer la genèse de NEMESIS, et nous dire ce qui en fait une solution de sécurité accessible à tous types d'entreprises ?

Lorsque nous avons lancé Elysium en 2016, le constat initial était que très peu d'entreprises étaient réellement bien équipées en solutions de sécurité informatique. Encore aujourd'hui elles ne sont que 5 % et 10%, majoritairement de grands groupes, car le coût est très important. Par ailleurs, la complexité de ce type de dispositifs nécessite des compétences techniques spécifiques. Enfin, les solutions du marché sont vieillissantes. Elles sont donc à la fois chères, complexes et moyennement fiables.

NEMESIS est une suite de sécurité 100 % française qui permet d'assurer et d'orchestrer la sécurité d'un système d'information. Elle fournit des capacités avancées et intelligentes de collecte d'informations, d'analyse comportementale, de détection d'intrusions complexes et de gestion des incidents de sécurité. Également dotée de capacités de réaction rapide, Nemesis peut mener en temps réel des actions automatiques permettant de suivre, endiguer ou isoler une menace identifiée.

Parce que nous considérons que disposer d'un système d'alarme ne devrait pas être un luxe et grâce à la maîtrise que nous avons sur chaque composant, la solution NEMESIS est accessible à tout type d'entreprise : grands groupes, PME, TPE.

Qu'il s'agisse de phishing basique via des ransomwares ou d'attaques complexes ciblées conduites par des professionnels, chaque entreprise se fait attaquer au moins une fois par an. Notre solution permet ainsi de réduire la probabilité que ça arrive, et d'augmenter la réactivité en cas d'alerte de sécurité avérée.

NEMESIS nouvelle génération, en bêta-test depuis 2018, aurait dû être officiellement lancée pendant Cyber-Day 2020.



Maîtriser la sécurité de son système informatique ne suffit pas, encore faut-il maîtriser ses données. En quoi consiste selon vous une bonne cybergouvernance ?

De nombreuses entreprises se font pirater car la donnée (cartes bancaires, RIB, données d'identité, fichiers clients, brevets industriels...) a une valeur, qui se monnaie sur le darknet. Les problèmes surviennent lors de certains mouvements, tels qu'une fusion ou une acquisition d'entreprise, qui impliquent des transferts de données.



Un investissement sur deux échoue après l'opération, à cause d'un incident de sécurité sur des données ou de mauvaise estimation du degré de « propreté » de ces données.

Par exemple, lors d'une fusion entre deux structures, le système de l'une se fait contaminer par le système corrompu de l'autre. Autre exemple : une entreprise rachète une petite structure à forte valeur d'innovation. Or, un concurrent a récupéré frauduleusement des données R&D de cette structure et développe déjà un brevet.

Autre exemple encore : une entreprise, dont la franchise d'assurance s'élève à 1000 euros par mois, se fait pirater. Or les pertes en matériel, réputation etc. sont évaluées à 120 millions d'euros... que l'assurance se voit contrainte de rembourser !



Le risque financier lié à la mauvaise gouvernance de la donnée est aujourd'hui bien identifié par les investisseurs comme par les assureurs. Des audits multi-expertises, techniques et juridiques, permettent de chiffrer la valeur des données et fournir une estimation de risques, donc du niveau de protection et du montant de franchise d'assurance requis. La finalité étant qu'une fois la donnée maîtrisée, protégée donc gouvernée, elle peut être valorisée. Ce levier de financement de premier ordre constitue tout l'enjeu d'une bonne cybergouvernance.

Merci Sébastien Dartigalongue.



9h00/9h45. Défis 2020. Invités : Catherine MORIN-DESAILLY, Sénatrice. Guillaume POUPARD, Directeur Général ANSSI.

9h45/10h30. Assurance cyber : sécuriser son business et limiter les impacts

10h45/11h30. Innovation x Humain X Cybersécurité : Comment vous assurer de protéger correctement la valeur que vous créez ?

11h45/12H30. Cybergouvernance : la Performance financière par la Maîtrise des informations

14h00/14h45. CESIN - 1/ 5ème édition du baromètre annuel - 2/ De l'urgence de nommer des Directeurs Cybersécurité ?

15h00/15h45. « L'évolution des politiques de sécurité avec l'émergence du cloud »

16h00/16h45. Sécuriser les usages : Un rempart à la déstabilisation économique, politique et sociétale.

17h00/17h45. Table ronde de clotûre : Principaux enseignements de cyberday2020. Nos invités nous rejoignent

Rendez-vous l'année prochaine

WWW.CYBER-DAY.INFO



3^{ème} édition
Ecole de Guerre Economique

cyber-day.info
11 mars 2020
196, rue de Grenelle, 75007 PARIS

CONFÉRENCES DÉBATS WORKSHOPS RENCONTRES

DE LA SÉCURITÉ
DE L'INFORMATION À UNE
CYBER-GOUVERNANCE MÉTIERS

EGE
Veille
Economie

”

Au fil d'une journée

Quelques focus
rencontres
débat
workshops

#cyberday.