

Tribune Libre

Cybersécurité Tous concernés

Member : Emma HENRY

VTK

VERY TECH KNOW





CEO & FOUNDER



**"La cybersécurité ne consiste pas
seulement à protéger les données, mais
aussi à protéger les personnes et les
processus qui les utilisent."**

James Comey, ancien directeur du FBI.

Quelques exemples

YAHOO 2013 : compromissions de 3 milliards de comptes d'utilisateurs = 350 millions de dollars.

EQUIFAX 2017 : violation de données personnelles pour 147 millions de personnes = 1,7 milliard de dollars

TARGET 2013 : violation de données sur les informations de carte de crédit de 41 millions de clients = 200 millions de dollars

MARRIOTT INTERNATIONAL 2018 : violation de données sur 500 millions de clients = 200 millions de dollars

COLONIAL PIPELINE 2021 : attaque de ransomware qui a interrompu l'approvisionnement en carburant sur la côte est des États-Unis = 50 millions de dollars dont rançon de 5 millions de dollars aux pirates



Un avant... et un après

III

PIXELS • SÉCURITÉ INFORMATIQUE

En Allemagne, une attaque informatique contre une clinique provoque une mort

Une patiente en situation critique n'a pas pu être opérée, en raison d'une attaque au rançongiciel qui a paralysé la clinique universitaire de Düsseldorf.

Le Monde avec AP

Publié le 17 septembre 2020 à 20h29, modifié le 12 novembre 2020 à 17h30 · 🔊 Lecture 1 min.

Autour de nous...

SERETRAM 2008

Fraude au président
17 millions d'euros
2 licenciements
Rachat par General Mills

Mairie de Morcenx-la-Nouvelle (2023)

Blocage par un rançongiciel

Hôpital de Dax (2021)

Cyberattaque de type rançongiciel
Paralysie des systèmes informatiques
Report d'opérations

Communauté de communes Chalosse Tursan (2023)

Effacement complet des données sur son serveur

Société d'ambulances des Trois Cantons à Peyrehorade (2022)

Cyberattaque avec demande de rançon

Département des Landes (2024)

Attaques du site internet revendiquées par un groupe de hackers pro-russes



Emma Henry

VTK

Les compétences



Compréhension business

Approche métier et compréhension des objectifs
Appréhension des risques métier (contrôle interne)
Gestion relationnelle et sensibilisation des acteurs



Compréhension technique

Compréhension exhaustive des infrastructures techniques qui pourraient mettre en risque



Compréhension légale

Appréhension pertinente du cadre légal relatif à l'entité concernée

Cadre légal

- **Loi n° 2018-133 du 26 février 2018** (transposition de NIS 1 - 2016) vise à renforcer la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels (OSE) et des fournisseurs de services numériques (FSN). Elle définit les obligations de ces acteurs en matière de sécurité et de notification des incidents.
- **Loi n° 78-17 du 6 janvier 1978** (Loi Informatique et Libertés) encadre la collecte et le traitement des données personnelles. Elle impose aux organisations de mettre en œuvre des mesures de sécurité appropriées pour protéger ces données contre les accès non autorisés, la perte ou la destruction.
- **RGPD** (25 mai 2018) renforce les droits des personnes en matière de protection de leurs données personnelles. Il impose aux organisations de mettre en place des mesures de sécurité techniques et organisationnelles pour garantir la confidentialité, l'intégrité et la disponibilité des données.
- **Ordonnance n° 2005-1516 du 8 décembre 2005** relative aux échanges électroniques entre les usagers et les autorités administratives :
- **Référentiel général de sécurité (RGS)** édicté par l'ANSSI, le RGS est un ensemble de règles et de recommandations visant à garantir la sécurité des systèmes d'information de l'État et des organismes qui lui sont liés. Il définit les exigences de sécurité applicables aux différents niveaux de sensibilité des informations traitées.
- **Loi de programmation militaire (LPM)** : Les différentes lois de programmation militaire successives contiennent des dispositions relatives à la cybersécurité, notamment en matière de lutte contre la cybercriminalité et de protection des infrastructures critiques.

NIS 2

Quand

- JOUE 16/01/2023
- Projet de loi sur la sécurisation et la régulation de l'espace numérique en France

Quoi

- Elargissement des secteurs concernés
- Exigences plus strictes avec mise en place de politiques et procédures de cybersécurité complètes et adaptées
- Elargissement du signalement des incidents
- Harmonisation européenne

Comment

- 10 000 000 € ou 2 % du chiffre d'affaires mondial total de l'année précédente
- COMEX tenu responsables du non-respect des exigences de cybersécurité

NIS 2 : presque tous concernés

CA : 10 M€ / 50 employés ou plus

- Énergie (électricité, pétrole, gaz, chauffage urbain, hydrogène)
- Transports (aérien, ferroviaire, maritime, transport routier urbain et interurbain)
- Secteur bancaire
- Infrastructure des marchés financiers
- Santé (fournisseurs de soins de santé, laboratoires de référence et recherche et développement pharmaceutique)
- Eau potable
- Eaux usées
- Infrastructure numérique (IXP, DNS, TLD, fournisseurs de services cloud, centres de données, réseaux de diffusion de contenu, fournisseurs de services de confiance, fournisseurs de réseaux de communications électroniques publics)
- Administration publique (au niveau central et régional)
- Espace
- Services postaux et de messagerie
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution de denrées alimentaires
- Fabrication (dispositifs médicaux, ordinateurs, machines, équipements électriques, véhicules)
- Fournisseurs numériques (places de marché en ligne, moteurs de recherche en ligne, plateformes de réseaux sociaux)
- Recherche
- **Seul fournisseur d'un service essentiel**

Pour vous aider

Audit préliminaire

Points forts
Points faibles
Recommandations préliminaires

Audit et Évaluation des Risques

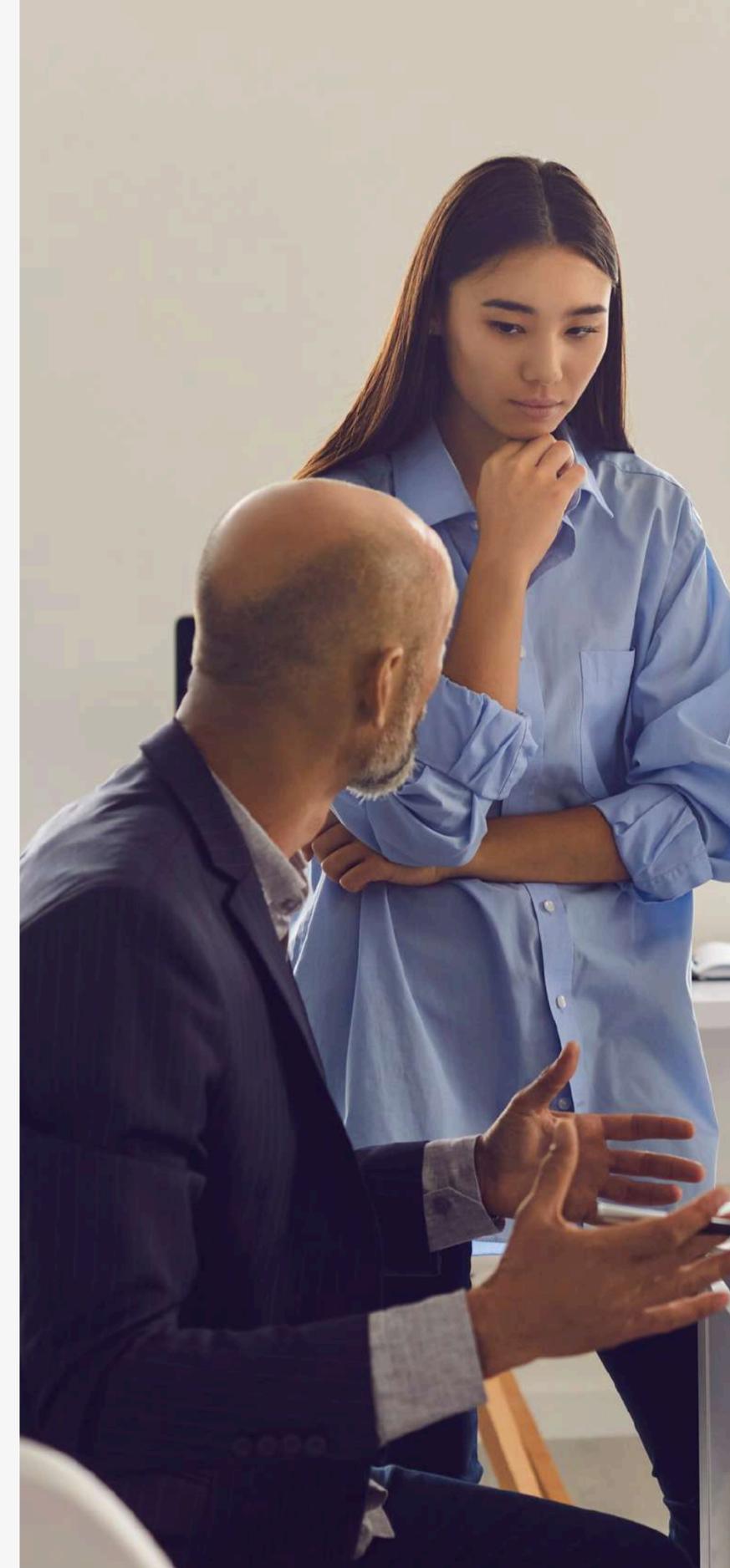
Analyse approfondie de votre infrastructure, de vos applications et de vos processus.
Identification des vulnérabilités et évaluation des risques associés.
Rapport détaillé avec des recommandations personnalisées.

Conformité Réglementaire

Accompagnement pour la mise en conformité avec le RGPD, NIS 2 et autres réglementations applicables

Formation et sensibilisation

Sessions de formation pour vous et vos employés sur les meilleures pratiques en matière de cybersécurité.



Emma Henry

Contact Me



Phone Number

+33687301614

Email Address

emma.henry@verytechknow.com

Social Networks

