RÉUSSIR
CLUB D'ENTREPRISES

26 Novembre 2021

NEWSLETTER SPÉCIAL CYBERSÉCURITÉ

PETIT-DÉJEUNER CYBERSÉCURITÉ

COMMENT APPORTER UNE SOLUTION FINANCIÈRE POUR QUE LES TPE - PME - PMI PUISSENT INVESTIR :

- en solution digitale ?
- pour la mise en place de cette organisation : formation ?
- pour l'assurance cyber ?

ASSURANCE CYBER : QUELS RISQUENT POUR QUELLES GARANTIES ?

Mélanie SPECHT

GROUPAMA D'OC

COMMENT SE PRÉMUNIR CONTRE LA OU LES FRAUDES ?

Stéphane REVEL
Daniel LEGROS

BANQUE POPULAIRE

Jalil BENABDILLAH	Caroline DE RUBIANA	Mélanie SPECHT	Stéphane REVEL	Daniel LEGROS	Guillaume GAILLARD
Vice-Président	Chargée de mission CyberSécurité	Responsable Technique Pôle ACPS, Entreprises, Collectivités, Associations et Assurance collective	Expert en solutions techniques	Expert en solutions techniques	Enseignant chercheur
Économie, Emploi, Innovation et Réindustrialisation	AD'OCC / CYBER'OCC	GROUPAMA D'OC	BANQUE POPULAIRE OCCITANE	BANQUE POPULAIRE OCCITANE	IUT BLAGNAC UNIVERSITÉ TOULOUSE JEAN JAURÈS
RÉGION OCCITANIE					

Jalil BENABDILLAH
Vice-Président
Économie, Emploi, Innovation et Réindustrialisation
04 67 22 68 28

DES FORMATIONS GRATUITES GRÂCE AU PLAN RÉGIONAL DE FORMATION

Dans le cadre de son **Plan Régional de Formation** (ou Programme Régional de Formation), la Région Occitanie finance **30 000 places** de formations professionnelles à saisir **avant le 31 décembre 2021**.

Ces formations sont gratuites, réservées aux demandeurs d'emploi, elles concernent tous les secteurs d'activité et sont réparties sur l'ensemble de la Région.

Plus d'info sur :
https://www.meformerenregion.fr/le-programme-regional-de-la-formation

Caroline DE RUBIANA
Chargée de mission Cybersécurité
www.cyberocc.com
05 32 02 79 97

AD'OCC | Direction de l'innovation - Filière du futur
Agence Régionale de Développement Economique
Région Occitanie / Pyrénées-Méditérannée
www.agence-adocc.com

PRÉSENTATION DU PROJET POUR LA FILIÈRE CYBERSÉCURITÉ D'OCCITANIE

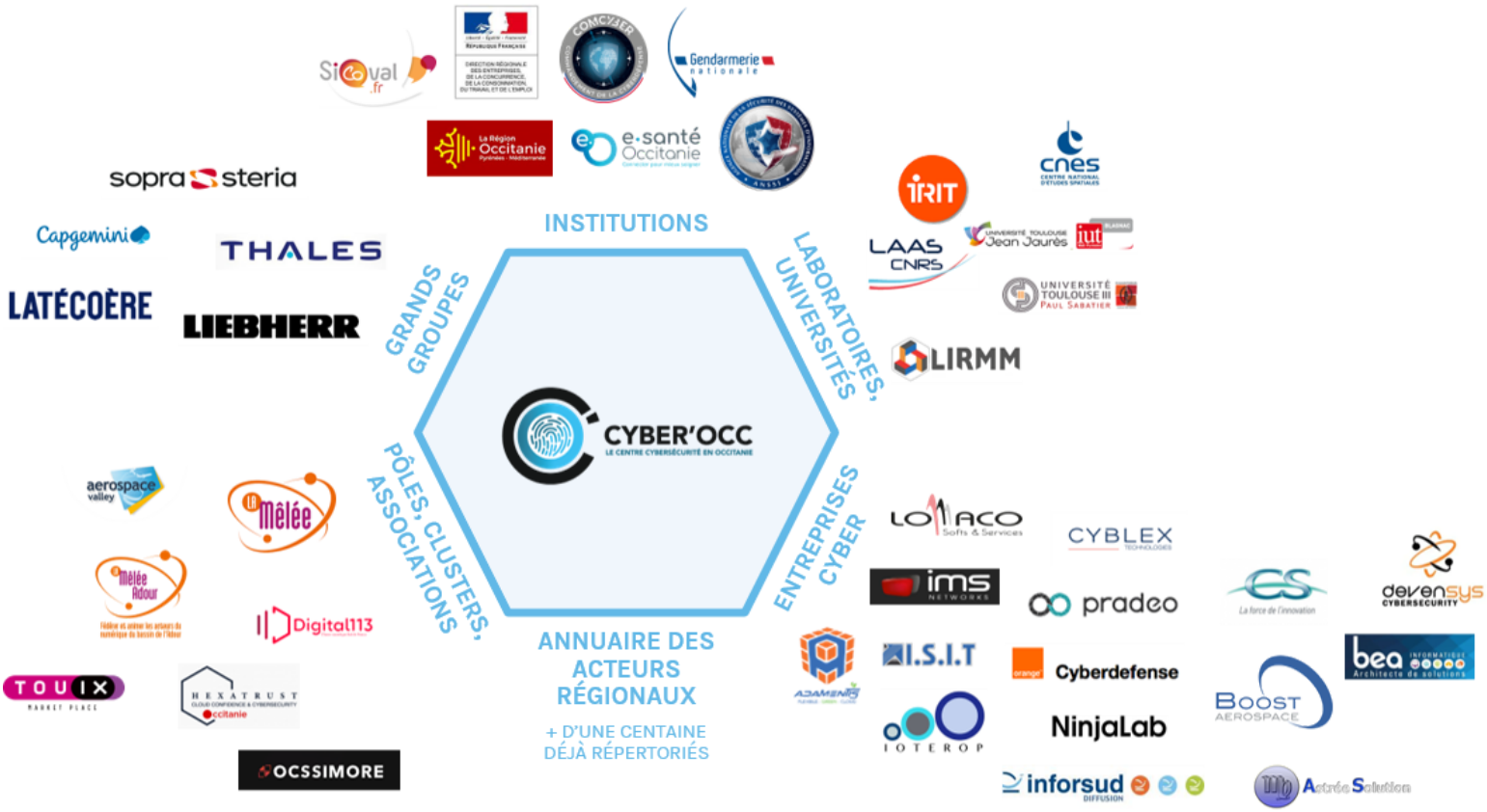
CYBER'OCC LE CENTRE CYBERSÉCURITÉ EN OCCITANIE — STRATÉGIE RÉGIONALE DE L'INNOVATION Occitanie / Pyrénées - Méditerranée — & — LA SPÉCIALISATION INTELLIGENTE

UNE DOUBLE AMBITION :

#1 Accompagner les entreprises régionales pour les aider à se prémunir contre les risques Cyber sur leurs SI et leurs produits

#2 Répondre aux besoins de la filière : pénurie des talents, visibilité nationale, innovation, ...

UN ÉCOSYSTÈME RICHE ET IMPLIQUÉ



ORGANISATION DU CENTRE AUTOUR DE 5 THÉMATIQUES PHARES

VOLET CYBERSÉCURITÉ DU PLAN FRANCE RELANCE

1ER SEMESTRE 2022

UN PORTAIL ET DES OUTILS EN LIGNE DEPUIS JUIN 2019

Veille et Information

Approfondir

Métiers et Formations

Cyberthèque

Outils en ligne

Parcours d'accompagnement

Visibilité de l'écosystème

Du portail de la Cybersécurité en Occitanie au Hub régional, un projet co-construit avec l'ensemble de l'écosystème

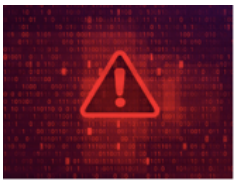
https://www.cyberocc.com/

ACTIONS CONCRÈTES

Partenariats :

10aine interventions entre 2020-2021

Cellule de crise COVID19



Campagnes :

Stéphane REVEL
Expert en solutions de Paiements
Stephane.REVEL@bpoc.fr

Daniel LEGROS
Expert en solutions de Paiements
DANIEL.LEGROS@bpoc.fr

COMMENT SE PRÉMUNIR CONTRE LA FRAUDE BANCAIRE ?
QUELS SONT LES DIFFÉRENTS TYPES DE FRAUDES ?

FOVI : Mode opératoire

Réalisée par téléphone ou par mail, l'escroquerie aux Faux Ordres de Virement (FOVI) concerne les entreprises de toute taille et de tous les secteurs.

La "Fraude au dirigeant" consiste pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.

Le "Changement de RIB" consiste pour les fraudeurs à envoyer un mail à un salarié du service de comptabilité ou trésorerie de l'entreprise en se faisant passer pour un fournisseur, et lui demander de diriger ses versements vers un autre compte bancaire appartenant aux escrocs.

LA PRISE DE CONSCIENCE DES ENTREPRISES PROGRESSE

ATTAQUES

Plus de 7 entreprises sur 10
ont été victimes d'au moins une tentative de fraude en 2020

Plus d'une entreprise sur 4
a subi au moins une fraude avérée en 2020

PRÉJUDICE

1 ENTREPRISE SUR 3
A SUBI UN PRÉJUDICE
SUPÉRIEUR À 10K€ EN 2020

10 % DES ENTREPRISES
ONT SUBI UN PRÉJUDICE
SUPÉRIEUR À 100K€ EN 2020

TOP 5 DES TENTATIVES DE FRAUDE

#1	Fraude au faux fournisseur	48%
#2	Fraude au faux président	38%
#3	Autres usurpations d'identité (banques, avocats, CAC, ...)	31%
#4	Intrusion dans les systèmes d'information	29%
#5	Fraude au faux client	24%

EXEMPLES D'ATTAQUES ET CONSEILS POUR LES DIRIGEANTS

- **Virement international non planifié et inhabituel**
- **Changement de RIB intempestif d'un fournisseur**
- **Urgence / Isolement / Discrétion**
- **Flatterie ou menace**
- **Usurpation d'identité d'une personne de confiance**

COMMENT S'EN PREMUNIR ?

CONSEIL N°1 : Sensibiliser et former les collaborateurs.

CONSEIL N°2 : Mettre en place et respecter une procédure confidentielle pour l'exécution des virements.

CONSEIL N°3 : Maitriser et sensibiliser les employés sur la diffusion des informations concernant votre entreprise.

CONSEIL N°4 : Mettre en place un système de délégation pour les opérations bancaires.

CONSEIL N°5 : Ne pas rester isolé et prendre le temps d'effectuer des vérifications.

CONSEIL N°6 : Limiter les accès physiques aux postes de travail et sécuriser les installations informatiques.

SOLUTIONS POUR SÉCURISER LES TRANSACTIONS

#1 **La signature électronique :** En choisissant la signature par certificat électronique en remplacement des confirmations par fax / email / téléphone, le client sécurise les télétransmissions.

#2 **La validation à distance :** Lors de ses déplacements, le décideur aura la possibilité de garder le contrôle des opérations bancaires réalisées par ses collaborateurs à partir d'un smartphone, tablette ou montre connectée. Il pourra consulter ses relevés de comptes et se réserver la possibilité de valider ou refuser les opérations de télétransmission initiées.

#3 **Une liste de pays autorisés avec un système de plafonnement des montants :** Avec le passage au SEPA (Single Euro Payements Area), il est devenu très facile de faire un virement vers n'importe lequel des pays de la zone EURO. Dans Suite Entreprise.com, le client peut facilement créer une liste des pays autorisés, ceux avec lesquels il a l'habitude de travailler

DEMONSTRATION DE NOTRE SOLUTION SUITE ENTREPRISE

https://integration.suiteentreprise.banquepopulaire.fr/Account/Login?returnUrl=%2F&isConnexionCyber=False

Guillaume Gaillard
Attaché temporaire
d'enseignement et de recherche
guillaume.gaillard@univ-tlse2.fr

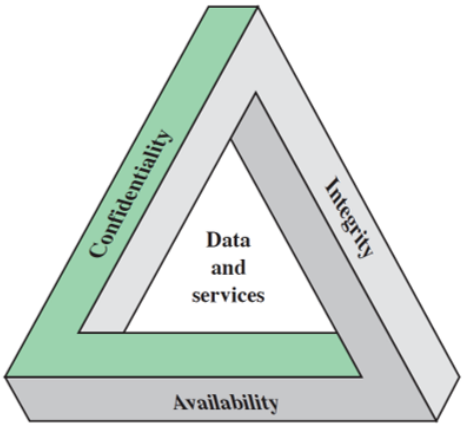
IuT Blagnac
Département Réseaux et Télécom, IRIT RMESS

LA CYBERSÉCURITÉ DANS LA FORMATION À L'IUT DE BLAGNAC

DÉFIS DE LA FORMATION RÉSEAUX ET CYBERSÉCURITÉ

Former à la technique (bac +3)	BUT, LP à l'IuT
Préparer l'ingénierie (bac +5)	
Rechercher l'expertise (bac +8)	Recherche à l'IuT
Sensibiliser en général (tous ages)	Formation continue

FORMER À BAC+3 AUX TECHNIQUES DE LA CYBERSÉCURITÉ



Stallings, Data&Com Com 10th, 2014

Description des risques numériques
Attaques
Principes de chiffrement
Base de bonnes pratiques
Administration de services réseaux
Sécurisés / sécurisant

FORMATIONS À L'IUT

- **Parcours cybersécurité dans le BUT (2021)**

1500 candidats 2021 parcoursup

- **Sécurité dans le parcours IoT**

Vulnérable et quotidien

- **Licence professionnelle Réseaux Informatiques Mobilité Sécurité**

Administrer, Superviser, Parer

S3-4	S5-6
CY1 Administrer un système d'information sécurisé	**CY2** Surveiller un système d'information sécurisé
IO1 Gérer les infrastructures des réseaux mobiles	IO2 Mettre en œuvre des applications et des protocoles sécurisés pour l'Internet des Objets

LP RiMS CyberSécurité

CERTIFICATIONS CYBER : LES + DE L'IUT

LP RiMS : Certification SecNumedu
- ANSSI 2021-2024

Académie Cisco :
- CCNA 1 à 4 Routing & Switching
- CCNA CyberOps

Académie Stormshield
- Stormshield CSNA
- par expert CSNE

MÉTIERS VISÉS PAR LA FORMATION

En interne/en prestation

- **Administrateur de systèmes** d'informations et de réseaux
- **Superviseur** sécurité des réseaux d'entreprises et des réseaux opérateurs
- **Intégrateur** de réseaux informatiques, de systèmes de télécommunications et de téléphonies sur IP
- **Chargé d'études** et déploiement réseaux téléphoniques sans fil 3G-4G-5G
- **Installateur** de faisceaux hertziens
- **Chargé de la maintenance** de systèmes de transmission
- **Administrateur d'infrastructures** Cloud et de virtualisation
- **Chargé d'affaires** de solutions téléphoniques et réseaux
- **Analyste** Cybersécurité
- **Architecte / Consultant** réseaux
- **Développeur de solutions** Internet des Objets

RECHERCHE À L'IUT

- Ressources administratives
- Ressources externes
- Plateformes de recherche
- Équipement perso / éducatif /expérimental
- Wi-fi public, Eduroam
- Publications
- Résultats d'expérience
- Télétravail / distanciel

Protection des données sensibles

Zone à Régime Restrictif (ZRR)

Cloud IRIT

Isolation des architectures

https://www.irit.fr/la-recherche/domaines-dapplication/securite-du-patrimoine-et-des-personnes/

Recherche en cybersécurité

Vie Privée :

- Design du protocole Robert⋆, appli Stop Covid

Réseaux, télécom :

- fiabilité des systèmes cyber-physiques

Math, info :

- Chiffrement, algorithmes

Écosystème Occitan

Plus de 150 personnes

(chercheurs, enseignants-chercheurs, ingénieur de recherche, doctorants, post-doctorants)

DÉFI CLEF ICO :
INSTITUT DE CYBERSÉCURITÉ DE L'OCCITANIE

- Matériel, logiciel, systèmes, réseaux, IoT, vie privée, Intelligence Artificielle
- Financement 2M€ région
- 2022-2025

Mohamed Kaâniche
Vincent Nicomette

Fabien Laguillaumie
Florent Bruguier
Lionel Torres

Abdelmalek Benzekri

Mélanie SPECHT
Responsable Technique Pôle ACPS, Entreprises, Collectivités, Associations et Assurance collective
05 61 99 46 17
melanie.specht@groupama-oc.fr

ASSURANCE DES RISQUES CYBER

QUELS RISQUES POUR QUELLES GARANTIES?

Le risque Cyber: qui est concerné?
Comment cela se traduit ?


Le vol de données


La destruction du matériel informatique


Le vol d'argent

Prendre le contrôle des systèmes pour effectuer des opérations illégitimes

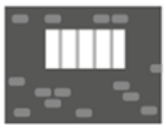

Espionner les concurrents

Quelles sanctions possibles en cas de non respect du RGPD ?


Réputation


Amende


Sanctions


Frais de notification de la violation


Responsabilité Civile

QUELQUES EXEMPLES

<u>Exemples issus de faits réels...</u>

<u>Vol de données</u>

Une entreprise s'est fait dérober ses données personnelles.
20 000 clients

<u>Cryptovirus</u>

Paralysie complète des systèmes d'informations.
Arrêt de l'activité
Demande de rançons pour décrypter

<u>Hameçonnage</u>

Une entreprise reçoit sur plusieurs postes informatiques en réseau, plusieurs mail de **demande d'argent pour éviter la divulgation de données.**

LES ENJEUX/RISQUES POUR LES ENTREPRISES

Quels sont les impacts et les conséquences ?

Demande de **rançons**

Responsabilité personnelle engagée du dirigeant

Risque d'image & Interuption d'activité

Obligation de déclarer dans les 72H la perte de données (CNIL)

60% cessent leur activité dans les **6 mois**

Sanction financière : Jusqu'à 20 M€ ou 4% du CA mondial

La couverture assurance

Gestion de crise

-coûts d'investigation, d'enquêtes et de consultant en sécurité informatique.

-Frais de consultant juridique (qualification des obligations réglementaires applicables)

-En cas d'atteinte aux données à caractère personnel

-En cas de frais de restauration d'image

Frais et pertes subis par l'Assuré

-Frais de reconstitution des données suite à un incident de sécurité

-Frais de décontamination de maliciels suite à incident de sécurité

-Frais supplémentaires d'exploitation

-Pertes d'exploitation....

Cyber responsabilité

-Responsabilité de l'Assuré encourue suite à un incident de sécurité

-Responsabilité de l'Assuré encourue suite à une atteinte aux données à caractère personnel

Les mesures de protection contre le risque cyber

La couverture assurance, une composante de la gestion du risque cyber:

La protection des systèmes d'information

La formation des salariés

La couverture assurance

La réalisation de sauvegardes complètes et régulières

La prévention Identifier les failles pour améliorer la sécurité

EXEMPLES DE TRAITEMENTS DE BOUT EN BOUT

Exemple 1 : Ransomware

Un cabinet d'expertise comptable a été victime d'une intrusion dans son système d'information. Un ransomware a été activé par le cyber criminel chiffrant les données stockées sur un premier serveur et contaminant les dix autres serveurs utilisés par le cabinet comptable ainsi que les dispositifs de sauvegardes.

Une rançon de 15 000€ par serveur est demandé par l'attaquant pour libérer les données chiffrées. La plateforme CYBEX ASSISTANCE est immédiatement saisie et procède à la constitution en urgence d'une cellule de crise composée des dirigeants du cabinet, du prestataire informatique assurant l'infogérance du parc informatique, d'un consultant en communication de crise et d'experts techniques CYBEX ASSISTANCE.

L'objectif est de comprendre l'attaque, son mode opératoire et de prendre les mesures pour limiter l'impact de l'incident.

L'assureur a pris en charge les frais d'experts techniques pour restaurer le système, la perte d'exploitation subie par le cabinet durant la période d'inactivité, les frais de communication de crise auprès des partenaires, clients, organismes publics en lien avec le cabinet comptable ainsi que les frais de reconstitution des données pour un montant de 570 000€.

Exemple 2 : Ransomware

Une société spécialisée dans l'emboutissage de bouteilles de vin fait l'objet d'une attaque ciblée sévère de son système d'information et voit sa production totalement à l'arrêt suite à la mise en œuvre d'un ransomware chiffrant toutes les données utilisées par les logiciels et outils de production.

La situation est critique, chaque heure sans activité l'entreprise perd 10 000€. Le pirate informatique réclame le versement immédiat d'une rançon en monnaie virtuelle, rançon qui augmentera chaque jour.

En lien avec le prestataire informatique et la DSI de l'entreprise, des consultants CYBEX ASSISTANCE réalisent une réponse à incident afin de comprendre rapidement l'origine de l'attaque et proposent une solution technique pour y mettre fin. Le prestataire n'a plus qu'à effectuer les tâches recommandées et à suivre les directives de CYBEX ASSISTANCE.

Au final, avec la mise en œuvre des garanties Gestion de Crise et Frais de décontamination, l'entreprise a pu bénéficier du rétablissement de son système d'information dans des délais très brefs, sans conséquence financière.

En parallèle, elle a pu bénéficier de l'expertise des consultants CYBEX ASSISTANCE qui ont recommandé la mise en œuvre de mesures techniques pour limiter le risque de réitération et sécuriser son infrastructure.