Club de la sécurité de l'information français

ECRANS 2017

Exercice de Crise Réaliste, Annuel et Nécessaire à la Sensibilisation

Ouverture de la Conférence de restitution d'exercice de crise

Discours de M. Michel DELPUECH
Préfet de Police

PREFECTURE DE POLICE

Club de la sécurité de l'information français

CLUSIF

Présentation de l'exercice

Jean-Marc GREMY, Président du CLUSIF

Genèse du projet « ECRANS 2017»

Nos motivations

- Peu d'occasion pour les entreprises, notamment les PME, de tester leur réaction face à une crise, cyber
- Sensibiliser les membres du CLUSIF, mais également l'ensemble de la communauté
- Proposer à nos adhérents une activité supplémentaire au sein de l'association

Nos objectifs

- S'appuyer sur cet exercice pour identifier les bonnes pratiques et les actions à dérouler lors d'une crise cyber
- Valoriser les travaux déjà réaliser en la matière, principalement au sein du CLUSIF (livrable du GT Gestion de crise)
- Renouveler l'expérience tous les ans dans le but de sensibiliser le plus de monde possible

Pourquoi « ECRANS » ?

- Exercice de Crise Réaliste
  - Il n'est sans doute pas à démontrer le lien avec l'actualité de cette année quant aux cyrptolkers (i.e. Wannacry, Petya/noPetya)
- Annuelle
  - L'objectif est bien d'utiliser cet exercice comme une base d'entrainement de nos adhérents, de façon régulière
  - En collaboration avec notre réseau : les CLUSIR
- Nécessaire à la Sensibilisation
  - Ce qu'en retireront les joueurs
  - Et pour ce premier exercice, la conférence de ce jour et ses livrables

Synopsis de l'exercice

- 4 équipes
  - Une équipe basée à Bordeaux représentant un laboratoire d'analyses médicales
  - Une équipe basée à Paris représentant un hôpital
  - Une équipe d'observateurs réparties entre les deux sites
  - Une équipe d'animation orchestrant le tout

- Un scénario
  - Simulation d'attaque par rançongiciel du laboratoire AMEDIC, dont le principal client, l'Hôpital de Lutèce, subit les conséquences
  - Proposé par François Paget (Merci François) ex Animateur de notre Panorama de la Cybercriminalité®
  - Etayé, développé par un groupe de travail, composé des adhérents du CLUSIF, du CLUSIR Nouvelle-Aquitaine, du Ministère de l'Intérieur, de la Préfecture de Police et de l'ANSSI

Une réussite collective

- De solides appuis
  - ANSSI
  - BEFTI
  - Clusir Aquitaine
  - Ministère de l'Intérieur
  - Préfecture de Police
- Des participants investis
  - Cellule d'animation
  - Observateurs
  - Joueurs

Équipe Parisienne

- Madame le Directeur
  Mme Afaf FAFI

- Chef de service
  Mr Michael JACQUES

- Responsable Comm'
  Mr Eric VAUTIER

- Responsable Juridique
  Mme Garance MATHIAS

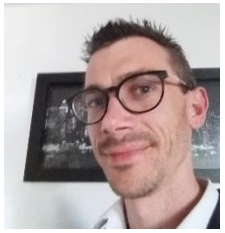
- RSSI
  Mr Luc MENSAH

- DSI
  Mr Arnaud MASSIAS

- Informaticiens
  Mr Christophe BREGERAS

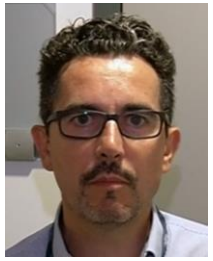
- Médecins
  Mr Laurent BEAUSSART

Équipe Bordelaise



- Monsieur le Directeur
  Mr Damien VINOT

- Équipe Technique
  Mr Frédéric GOUTH



- Responsable Comm'
  Mr Stéphane JOURDAIN

- DSI / RSSI
  Mr Thierry MEYER

- RH
  Mr Guilhèm SAVEL

- Responsable Juridique
  Mr Michael CATROUX

Programme de la conférence

- Simulation de crise : la Cellule d'Animation doit aussi se préparer…
  - Lionel MOURER, Atexio
- Quelle organisation pour une crise, en particulier cyber
  - Damien LACHIVER, Wavestone
- Les obligations légales auprès des institutionnels
  - Guillaume CHEREAU et Samuel HASSINE, ANSSI
- La Communication, une dimension stratégique de la gestion de crise
  - Frédéric MALMARTEL, ACOSS
- Questions/Réponses avec la salle
- PAUSE

Programme de la conférence

- Gestion contractuelle : Fournisseurs et Clients
  - Raynald LASOTA, France Télévision
- Les coûts de la crise
  - Gurvan QUENET, CLUSIR Aquitaine
- La judiciarisation d'une attaque : préservation des traces et dépôt de plainte
  - Commissaire Sylvie SANCHIS, BEFTI
- Questions/Réponses avec la salle

Club de la sécurité de l'information français

CLUSIF

Présentation du film ECRANS 2017

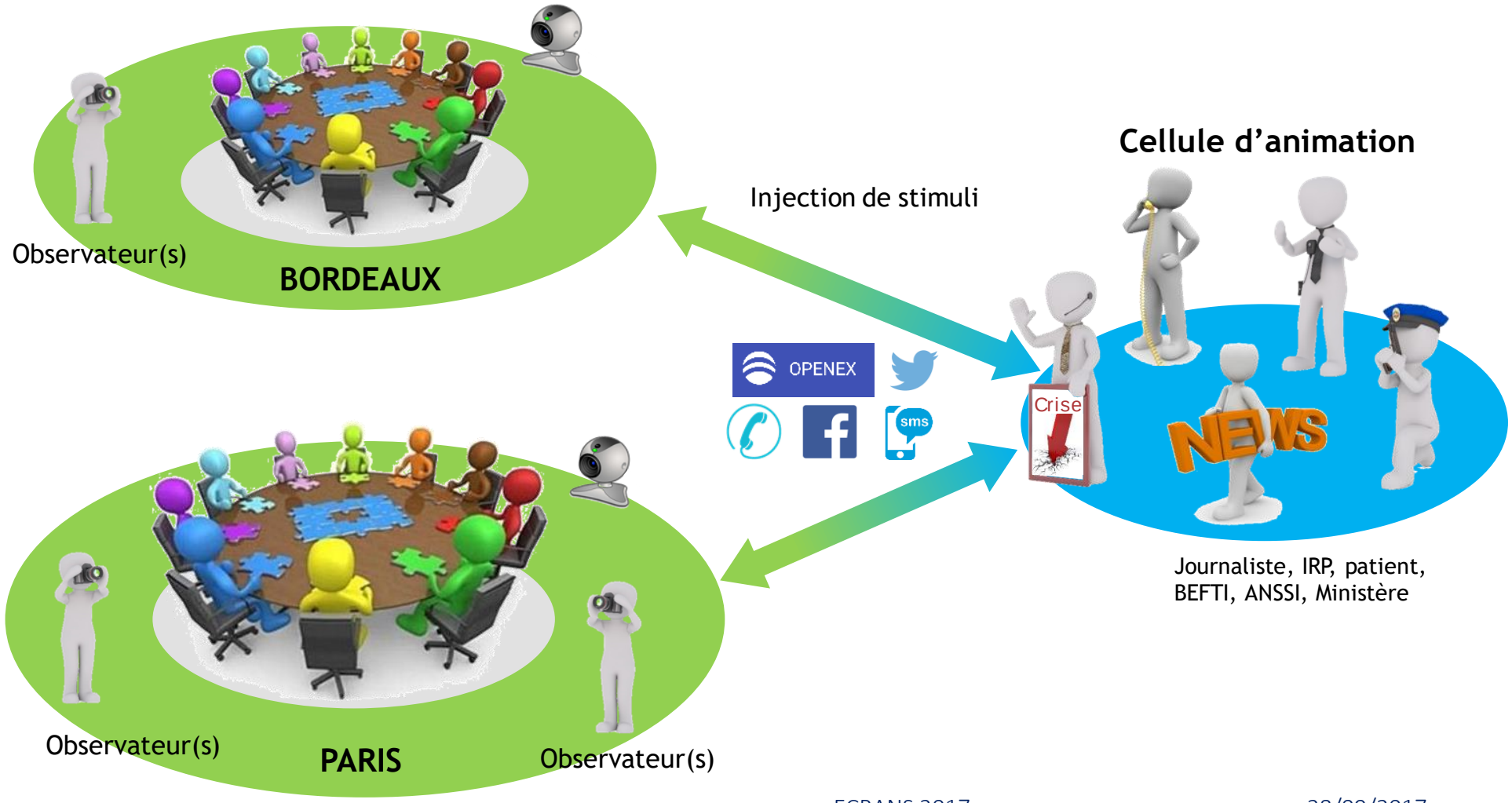
Club de la sécurité de l'information français

CLUSIF

La Cellule d'Animation doit aussi se préparer…

Lionel MOURER, ATEXIO
Animateur au sein de la Cellule d'Animation

Organisation de la Cellule d'Animation



L'animation : avant le test…

- Le périmètre doit être identifié et les attendus formalisés
- Le scénario doit être crédible !
- Les stimuli doivent être en nombre suffisants
- Chaque animateur doit se « préparer » à son/ses rôle(s)
- Il faut simuler le test

L'animation : pendant le test…

- Les « outils » doivent être prêts
  - Transmission des stimuli
  - Récupération de l'information en provenance de la CCRI
- Il faut être capable de réagir « en live » !
- Noter les points forts, les axes d'amélioration

L'animation : après le test…

- Faire un bilan à chaud
- Faire un bilan à froid
- Proposer des axes d'amélioration du dispositif de crise
- Préparer le prochain exercice… ☺

Club de la sécurité de l'information français

CLUSIF

Quelle organisation pour la crise, en particulier cyber ?

Damien LACHIVER, WAVESTONE
Animateur au sein de la Cellule d'Animation

Qu'est-ce qu'une crise ?

- Une crise est une situation de trouble, due à une rupture d'équilibre et dont l'issue est déterminante pour l'individu ou la société Dictionnaire ATTILF/CNRS

- Une crise est…
  - Une situation soudaine, souvent brutale, inattendue
  - Aux conséquences potentiellement très grave pour l'entreprise
  - Et pour laquelle les mécanismes et réactions habituels sont inadaptés

- Avec des origines extrêmement variées

- **Naturelles**
  - Inondations, tempêtes, grands froids, épidémies…

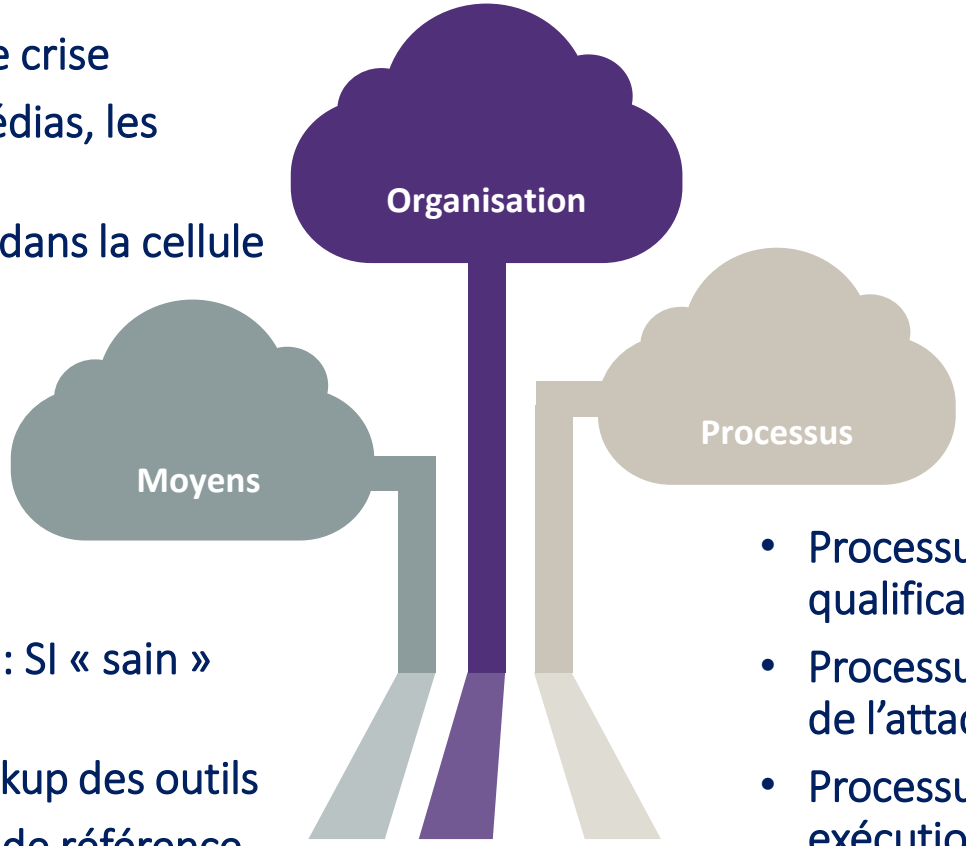
- **Environnementales**
  - Incendies, explosions liées à des sites à risques…

- **Humaines**
  - Défaillance de processus, erreur humaine, malveillance, attentat…

- **Technologiques**
  - Panne informatique, défaillance matérielle, virus, cyber-attaque…

Quels dispositifs pour y répondre ?

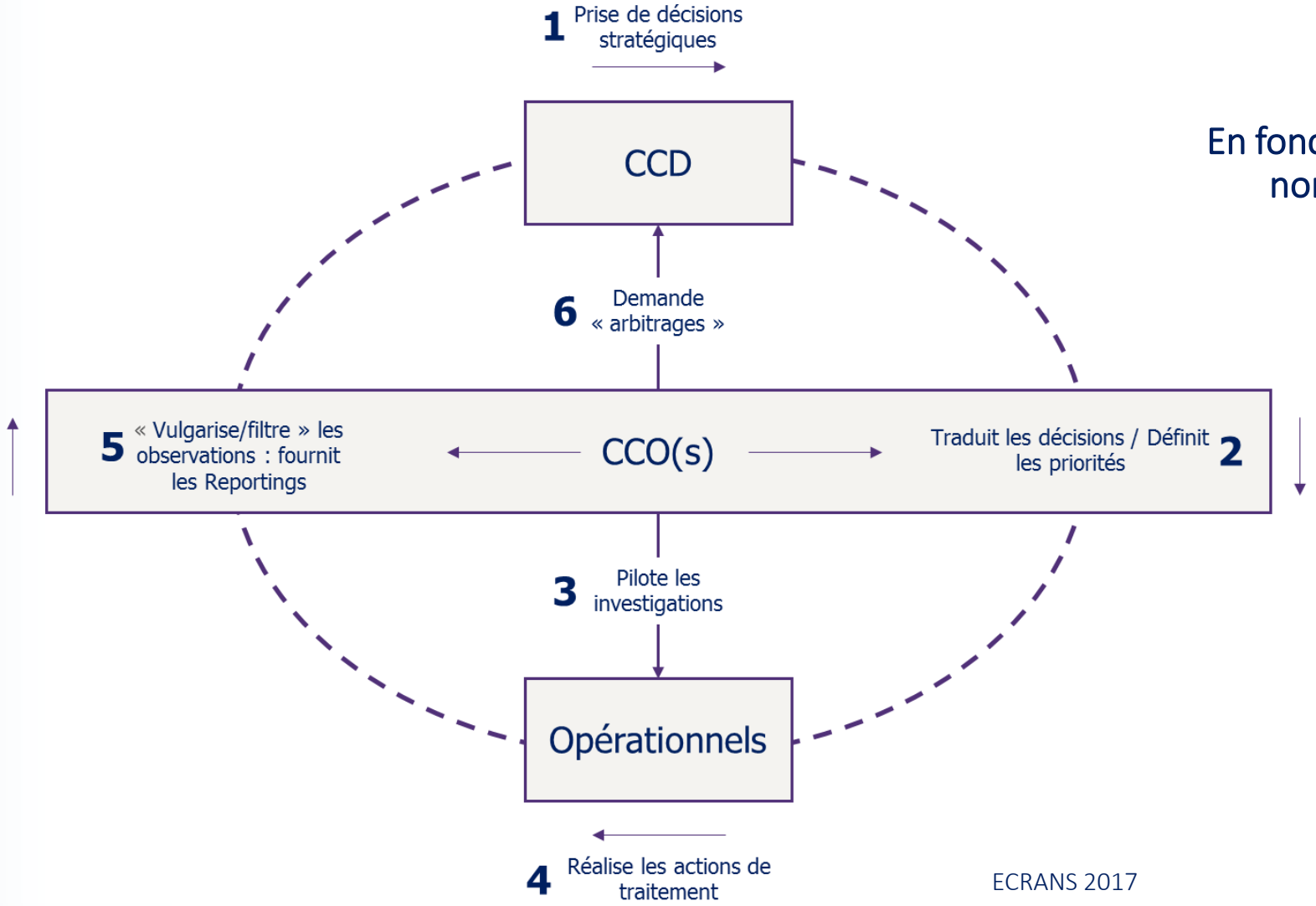
- Prise de décisions
- Organisation de la cellule de crise
- Communication avec les médias, les partenaires, les clients…
- Inclusion des acteurs cyber dans la cellule de crise



- Moyens de communication : SI « sain » de crise
- Moyens de traitement : backup des outils
- Informations et documents de référence

- Processus de déclenchement : qualification de l'incident cyber
- Processus de traitement : compréhension de l'attaque et préparation de la défense
- Processus de réaction : planification et exécution du plan de défense

Quelle organisation pour gérer une crise ?



En fonction de la taille de l'organisation, le nombre et le type de cellules peut fortement varier

Quels rôles propres au fonctionnement d'une cellule de crise ?

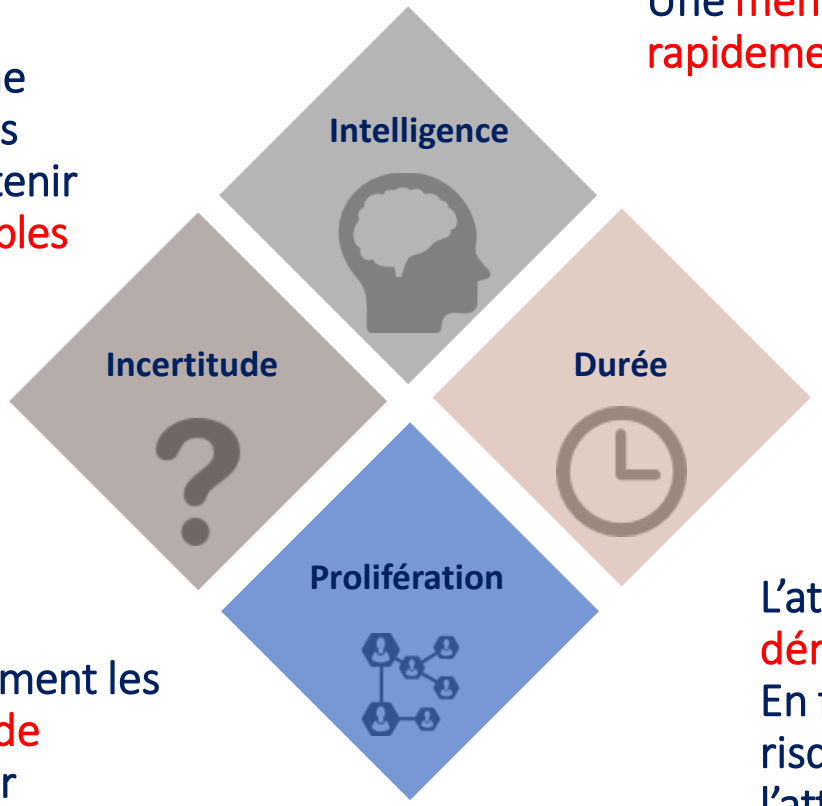
- Directeur de crise
  - Piloter la cellule et la réponse à la crise
  - Réaliser les arbitrages lorsque cela est nécessaire
  - Donner le rythme de la cellule
  - Faire le lien avec les autres parties prenantes de l'organisation

- PMO
  - Produire la main courante pour garder une traçabilité des actions et décisions
  - Formaliser les points de situations et plans d'action et les diffuser à ses homologues

- Conseiller de crise
  - Apporter un point de vue d'expert à la cellule
  - Prendre de la hauteur sur les évènements unitaires
  - Anticiper les évènements à venir

Quelles spécificités à prendre en compte pour les crises cyber ?

Face à la complexité d'un système d'information et à la diversité des menaces, il est très difficile d'obtenir rapidement des informations fiables sur l'attaque en cours et les motivations de l'attaquant



Une menace intelligente qui peut s'adapter rapidement aux réactions de l'organisation

Les attaquants utilisent généralement les réseaux et les nouveaux canaux de communication pour se propager largement au sein d'une organisation

L'attaquant, en général bien préparé, déroule un plan d'attaque très rapidement. En face, si l'entreprise est peu préparée, elle risque de répondre trop tardivement à l'attaquant et d'être dépassée par la menace

Quel bilan pour l'exercice ECRANS 2017 ?

- Des forces portées par de bons réflexes de gestion de crise et de connaissances cyber…

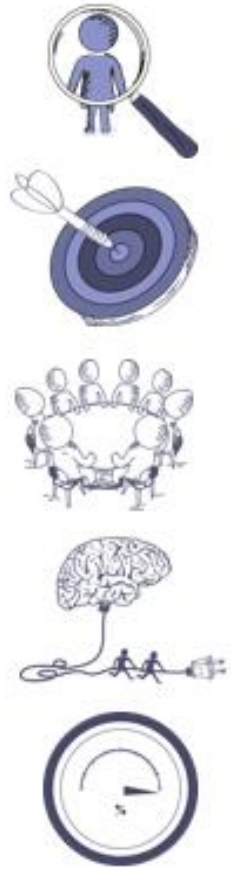
  - Les cellules se sont immédiatement organisées
  - Les participants ont définis clairement et respecté leurs périmètres de responsabilité
  - De bons réflexes en temps de crise sont partagés au sein des cellules : vérifier les identités, ne pas communiquer sans validation…

- Et des pistes d'amélioration pour corriger quelques points

  - Un manque de recul sur la situation globale et d'anticipation notamment en l'absence de partage centralisé de l'information au sein des cellules
  - Une désorganisation ponctuelle quand le responsable de la cellule doit s'absenter
  - Un manque de structure dans la prise de décision qui nuit à la prise en compte des aspects métiers

Les bons réflexes à respecter dans une crise cyber

1. Identifier Directeur, PMO et conseiller (et leurs backups !) et organiser la logistique de crise
2. Structurer, tracer et partager les décisions au sein de la cellule
3. Prendre le temps d'identifier les impacts de décisions
4. Prendre du recul et se mettre dans la peau de l'attaquant
5. Maitriser sa communication et rester discret sur la stratégie de défense



Se préparer et s'organiser en amont !

1. Formaliser et organiser		Définir et formaliser le processus et l'organisation de gestion de crise cyber du Groupe et des filiales
2. Monter en expertise		Identifier et impliquer des professionnels experts de la gestion de crise et du cyber
3. Tester les dispositifs		Tenir régulièrement des exercices de gestion de crise

Club de la sécurité de l'information français

CLUSIF

Obligations légales auprès des institutionnels

Guillaume CHEREAU et Samuel HASSINE, ANSSI
Animateurs au sein de la Cellule d'Animation

L'ANSSI, autorité de défense des systèmes d'information

Détecte
les attaques

Stoppe
les attaquants

Restaure
les systèmes

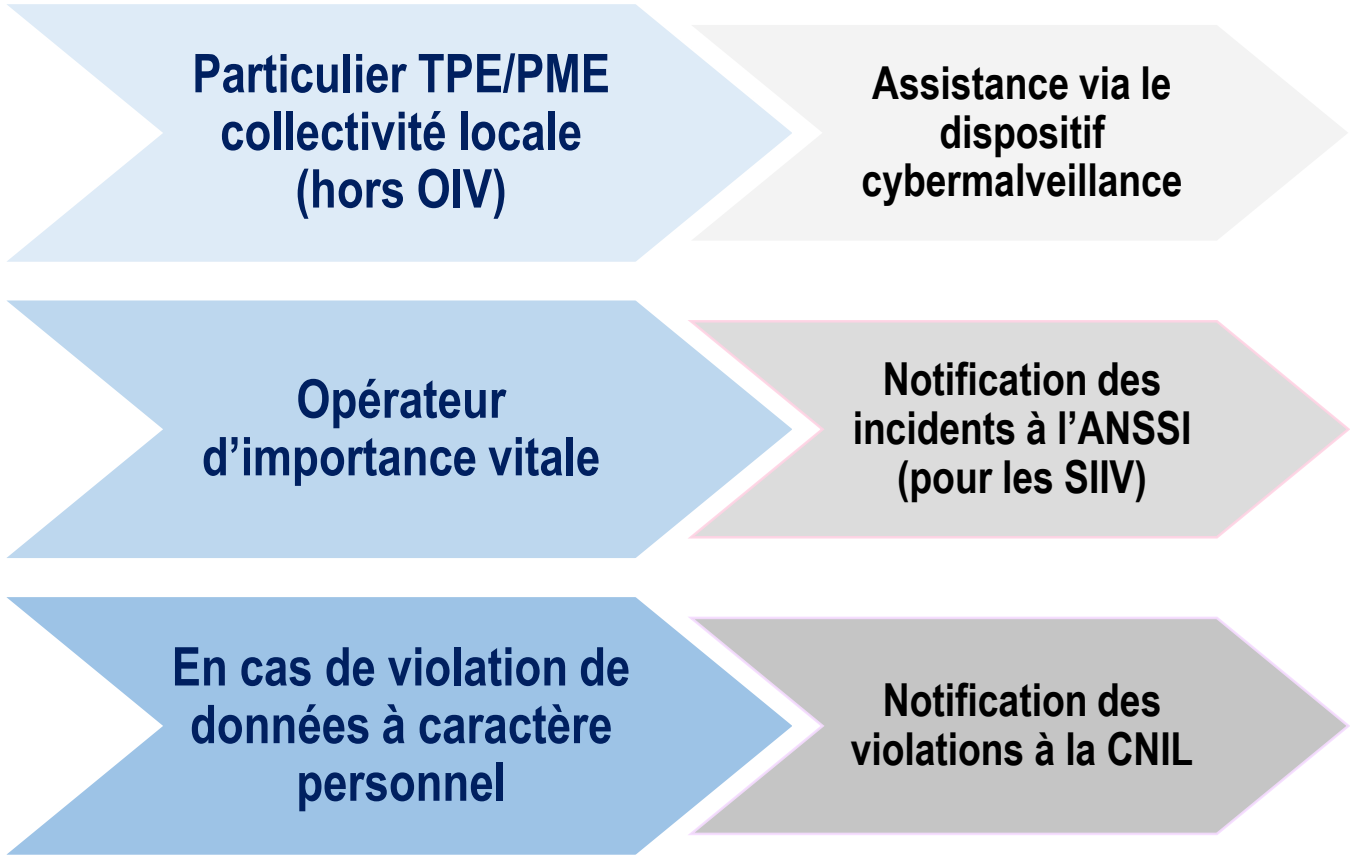
L'ANSSI, autorité de sécurité

- Réglementations

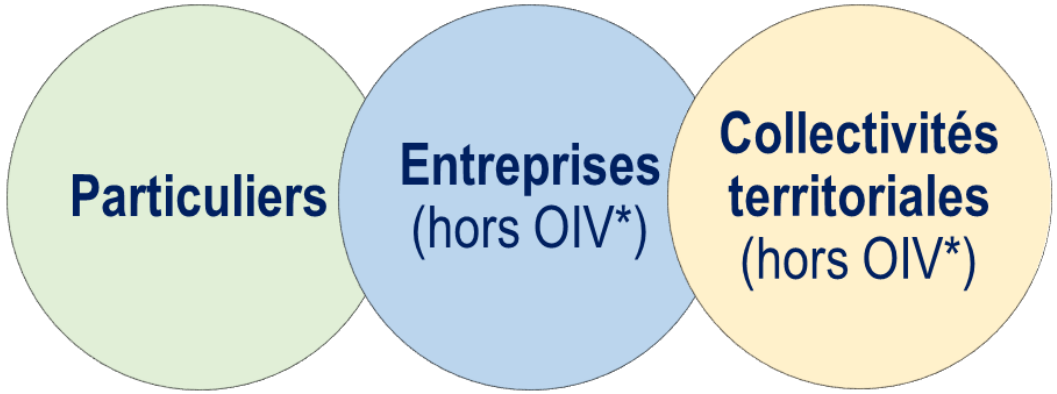
- Labélisation de produits et services

- Conseils et soutien

Qui et quoi notifier en cas d'incident de sécurité ?



Le dispositif
www.cybermalveillance.gouv.fr



Particulier TPE/PME collectivité locale (hors OIV) → Assistance via le dispositif cybermalveillance

Assistance aux victimes d'actes de cybermalveillance
(Mise en relation avec des prestataires de proximité)

Prévention et sensibilisation à la sécurité du numérique
(Campagnes de sensibilisation)

Création d'un observatoire de la menace numérique
(Remontées d'information, production d'analyse et de statistiques)

Notifier les incidents de sécurité à l'ANSSI

Opérateur d'importance vitale → Notification des incidents à l'ANSSI (pour les SIIV)

Prérequis

- Être un OIV dans un secteur avec arrêté
- Avoir déclaré ses SIIV

Condition

- Incident affectant un SIIV répondant aux critères de la règle de sécurité

Comment faire ?

- Formulaire en ligne : http://www.ssi.gouv.fr/entreprise/protection-des-oiv/la-cybersecurite-en-action/
- mailto:cert-fr.cossi@ssi.gouv.fr

Déclaration de violation de données à caractère personnel (cadre actuel hors RGPD)

Prérequis

- Être un FAI ou un opérateur télécoms
- Mise en œuvre d'un traitement de données personnelles

Conditions

- Données traitées, objet de la violation (perte, altération, divulgation,…)
- Intervenue dans le cadre de l'activité de l'opérateur

Comment faire ?

- Notification initiale sous 24H
- Notification complémentaire sous 72H
- Lien site CNIL : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Retour d'expérience ECRANS 2017
Préparation de l'exercice

Scénario

- Un scénario réaliste au regard de l'état des menaces, notamment autour des rançongiciels
- Le choix du secteur de la santé, qui est aujourd'hui particulièrement exposé
- Un intérêt à jouer la relation entre le client et son prestataire, souvent interconnectés et interdépendants

Implication de l'agence

- Une implication dans le groupe de travail afin de transmettre les messages et les bonnes pratiques de l'agence
- La possibilité de positionner des attendus de la part des joueurs afin de mieux connaître les missions de l'ANSSI

Retour d'expérience ECRANS 2017
Conduite de l'exercice

- Des obligations respectées envers les autorités/référents
  - Bonne compréhension de la part des joueurs du contexte OIV/LPM
  - La dimension des données personnelles prise en compte (ANSSI/CNIL)
  - Des échanges constructifs sur le rôle de l'ANSSI en temps de crise et la relation avec la chaîne SSI des ministères de tutelle

- Pédagogie sur les capacités de l'ANSSI
  - Manque de connaissance des missions mais surtout du périmètre d'intervention de l'ANSSI
  - Une appréhension encore marquée de la part des dirigeants à partager l'ensemble des informations avec un acteur étatique

Club de la sécurité de l'information français

CLUSIF

La communication, une dimension stratégique de la gestion de crise

Frédéric, MALMARTEL
Animateurs au sein de la Cellule d'Animation

Identifier l'importance de la communication

- Erreurs à éviter
  - Négliger la communication
  - Négliger que l'on est en crise
  - Agir trop tôt ou trop tard

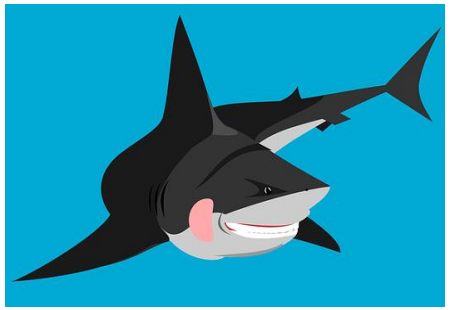
- Mesures à prendre
  - Identifier la criticité de la situation
  - S'organiser
  - Identifier les outils disponibles

Distinguer communication interne/externe

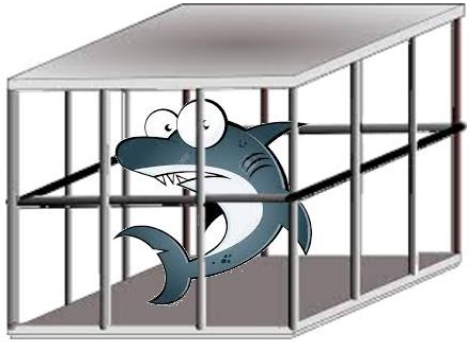
- Erreurs à éviter
  - Négliger l'une des deux communications

- Mesures à prendre
  - Dire qu'on est en crise, dire qui fait quoi
  - Faire des points réguliers d'information
  - Rassurer

Fixer les points de contact (porte-paroles)



- Erreurs à éviter
  - Laisser des acteurs non habilités s'exprimer
  - Laisser s'exprimer des personnes non coordonnées



- Mesures à prendre
  - Fixer le/les porte-paroles, les faire connaître
  - Prévoir des communicants différents pour des supports différents
  - S'appuyer sur une agence de com'

Réussir

- Erreurs à éviter : Les maladresses
  - Laisser planer un doute
  - Trop répondre

- Mesures à prendre : L'authenticité
  - Rassurer
  - Dire ce que l'on sait
  - Dire ce que l'on fait

CLUSIF

Questions / Réponses avec la salle

CLUSIF

Pause
(20 min)

Club de la sécurité de l'information français

CLUSIF

Cyber attaque ? Et les contrats clients/fournisseurs ?

Raynald LASOTA, France TELEVISIONS
Observateur au sein de la Cellule d'Animation

REX ECRANS 2017

- Problème d'engagement de résultat de la part de son fournisseur
- Problème de coupure de service → Risque sur l'exploitation
- Questionnement autour des clauses contractuels

Nouveaux risques

- Clauses sur les contrats existants / à venir
- Évolution des offres de services
- Interprétation / moralité / omerta autour de la relation contractuelle
- Encouragement des cyber attaquants du fait des failles que pourraient contenir les contrats

Contrat & sécurité : les clients / fournisseurs

- Le passé
  - Contrats existants : peu de clauses
  - Confidentialité
  - Secret des affaires
  - Cas de force majeur
  - Devoir moral / commercial

Contrat & sécurité : les clients / fournisseurs

- L'avenir
  - Obligations par le règlement
  - ISO 27001 : un objectif
  - Cyber assurance
  - Niveau de prestation sécurité
  - Encadrement des risques
  - Engagement sur la transparence
  - Responsabilité du prestataire

Contrat & sécurité : bonnes pratiques

Anticiper

- Avenant sécurité
- Charte de sécurité
- Calcul de risque
- Procédure en cas de cyber attaque
- Engagement fournisseur

Contrôler

- Revue des contrats
- Évolution au gré de l'actualité (règlementaire / technique)
- Analyse d'impacts

Club de la sécurité de l'information français

CLUSIF

Les coûts d'une cyber-crise

Gurvan QUENET, CLUSIR Aquitaine
Animateur au sein de la Cellule d'Animation

Des exemples récents

- Sony PSN : 172 M$
  - Mais une estimation prenant en compte les coûts indirects évoque 2 Milliards de Dollars
- Maersk : 400 M€ direct ; 1,5 Milliards indirect
- FedEx-TNT : 300 M$
- Saint Gobain : 250 M€ dont 220 M€ en perte de revenus
- Société de l'agro alimentaire : 10 M€

Des coûts mesurables

- Perte de production, d'exploitation, arrêt du SI / manque à gagner
- Coûts de mise en conformité, non respect de la législation (amendes)
- Coûts de justice (dommages et intérêts)
- Coûts contractuels / commerciaux
- Coûts de la remédiation et reconstruction IT
  - Sur le plan technique IT et SSI (expertise)
  - Organisationnel et gouvernance à repenser, au pire à définir !
  - Humain (sensibilisation / responsabilisation, compétences, …)

Des coûts difficilement mesurables

- Perte de confiance des fournisseurs et sous-traitants
- Perte de confiance des partenaires (financiers)
- Perte de confiance des clients
- Dégradation de l'image et réputation de l'entreprise (durée ?)
- Coûts sociaux, chômage technique, perte de poste
- Poursuites pénales (court ou moyen terme)

Des coûts complémentaires à prévoir

- Le RGPD
  - Sanctions de 4% du chiffre d'affaire mondial ou
  - Coût de notification aux tiers (violation de données) et indemnisations des clients (classe action…), ex : BtoC
  - Refonte du design du produit/service ou module défaillant, cible de l'attaque (ex : voiture connectée)

Objectif de la gestion de crise

- Évaluer la criticité de l'évènement
- Définir un plan d'action pour :
  - *Limiter les impacts métiers, financiers, juridiques*
- Maîtriser l'information tout au long de la crise (Réseaux sociaux à intégrer)
- Maîtriser la communication (à chaud) pour rassurer les salariés, les clients et partenaires
- Collecter les informations pour une communication (à froid) post-crise (anticipation des litiges potentiels, recours, etc.) pour un retour en mode nominal rapide
- Capitaliser sur l'historique post-crise et des incidents précédents (amélioration continue)

Pour

- **Maintenir les coûts directs ou indirects dans une enveloppe financière acceptable**

Comment limiter le coût d'une crise

- Anticiper en connaissant ses points de fragilité
- Analyse et traitement du risque
  - Mise en place de mesures de réduction du risques
  - Mise en place d'une cellule de gestion de la crise
  - Mise en place d'une communication maitrisée
  - Transférer le risque auprès d'une cyber assurance (indemnisation plafonnée et ne couvre pas tout)
- Acculturation digital / cyber sécurité
- S'inspirer des plans déjà mis en place (sanitaire/CHSCT, plan de secours usine, etc.)

Club de la sécurité de l'information français

CLUSIF

La judiciarisation d'une attaque cyber

Comment travailler avec un service de police en cas de cyber attaque ?

Sylvie SANCHIS
Commissaire de Police, Chef de la BEFTI

RETEX côté Police

- L'absence d'anticipation
  - Réduction du périmètre d'action ou dépassement du domaine de compétence des intervenants
  - Blocage des relations clients-prestataires

Les bonnes pratiques…

- Anticiper la crise
  - Définir les missions
  - Prévoir les absences
  - Connaître les contrats
  - Identifier des prestataires ponctuels

…conditionnent la plainte utile

- Préserver les traces
  Idéalement en numérique, sinon captures d'écran
  - Des serveurs et des sites internet compromis
  - Des fichiers chiffrés
  - Des journaux d'activité (logs)
  - Des éléments de communication avec les auteurs
  - Des paiements éventuellement effectués

La problématique des logs

- Vérifier les paramétrages des enregistrements
  - Nature et étendues des données enregistrées
  - Durée d'enregistrement et de conservation

- S'assurer de la disponibilité directe et rapide des journaux pour la victime (dispositions contractuelles)

Intérêt de la plainte

- Pour la victime
  - Comprendre les raisons et/ou le contexte de l'attaque
  - Identifier les modes opératoires
  - Identifier les auteurs
  - Récupérer les données métiers et limiter leur diffusion
  - Anticiper une nouvelle attaque

Intérêt de la plainte

- Pour les pouvoirs publics
  - Identifier et évaluer les menaces cybercriminelles
  - Lutter contre le chiffre noir
  - Attribuer des moyens adéquats

Modalité de la plainte

- Quand ?
- Où ? Commissariat ou service de Police Judiciaire
- Par qui ? Dirigeant ou mandataire
- Avec qui ? Technicien
- Avec quoi ?
  - Délégation de pouvoir, extrait Kbis
  - Premiers éléments
  - Évaluation du préjudice et des dommages

Orientation de la plainte

- Choix du service enquêteur par le Procureur de la République ou le juge d'instruction
- Si saisine BEFTI, contact régulier avec la victime
- Garantie de discrétion

Les investigations

- Contacts ANSSI, Inter-CERT, universitaires, chercheurs…
- Coopération en Europe et à l'étranger

CLUSIF

Questions / Réponses avec la salle