Orange Cyberdefense

Comment réussir sa sortie de crise

Webinar du 8 juin 2020

orange™

OrangeCyberdefense.com

Les intervenants

Laurent LEMAIRE
Orange Cyberdefense

Chief Business Officer

Eric METRAL
Métropole
Aix-Marseille-Provence
DGA des Systèmes
d'Information

Marc TOLUB
Orange Cyberdefense

Manager Gestion de Crise
Cyber Résilience

Julie VALLEE
IREMOS

Directrice de pôle
Gestion de Crise

La crise dans la crise

Un hôpital tchèque frappé par une cyberattaque en pleine épidémie de COVID-19

Coronavirus : le Département de la Santé américain cible d'une cyber-attaque

Le ministère de la Santé américain a été victime dimanche 15 mars d'une cyber-attaque, visant à ralentir ses systèmes informatiques. Ce département d'Etat est au centre de la stratégie de Washington pour contrer l'épidémie de coronavirus.

L'AP-HP touchée par une attaque en déni de service

Today, the President and the CEO of the CyberPeace Institute, Marietje Schaake and Stéphane Duguin, joined Madeleine Albright, Desmond Tutu, and Mohamed ElBaradei Among More Than Forty International Leaders Calling on All Governments to *Work Together to Stop Attacks Hampering Hospitals and International Organizations Fighting COVID-19*

Loudenot
@philippeloud

#Cyber & #Covid. Un énorme merci à @OrangeCyberFR pour leur appui cyber auprès des établi de santé et médico-sociaux. Cette solidarité est particulièrement appréciée. Les échanges avec la cellule #ACSS DE @esante_gouv_fr et l'équipe FSSI ont été d'une qualité extraordinaire.

@orangecyberFR se mobilise pour protéger ceux qui soignent

Orange Cyberdefense

Tandis que les soignants assurent leur service auprès des patients, les équipes @OrangeCyberFr se mobilisent pour assurer la protection de leurs outils numériques.
Les experts d'Orange Cyberdefense proposent gratuitement aux établissements hospitaliers et de santé :

- une hotline pour les conseiller et les aider à adopter les gestes et mesures utiles pour renforcer leur cybersécurité
- l'activation de solutions de mitigation en cas d'attaque en déni de service (DDoS)

Les nouveaux usages induits par la crise
augmentent notre vulnérabilité au risque cyber

Cybersécurité : la moitié des employés admettent qu'ils prennent des raccourcis en télétravail

Technologie : *Les distractions lors du travail à domicile, la pression pour respecter les délais et l'utilisation d'appareils personnels sont autant de risques supplémentaires pour la sécurité des travailleurs à distance juge une nouvelle étude.*

- Moins de frontières dans les utilisations pro-perso
- Poste de travail infectés durant le télétravail
- Stockage des données sur des dispositifs personnels ou cloud public
- Shadow IT
- Mise à jour ou correctifs non installés
- Dérogations à la politique de sécurité
- Attribution de droits d'accès exceptionnels aux utilisateurs
- Acceptation de non-conformités aux réglementations

Les attaquants s'adaptent pour exploiter
ces nouvelles opportunités

- Phishing
- Noms de domaines frauduleux
- Attaques en déni de service
- ...

https://orangecyberdefense.com/fr/insights/livres-blancs-et-reportings/covid-19-quand-un-risque-biologique-devient-numerique/

Les menaces d'attaques sur les clouds en hausse de 630% avec le télétravail

Crise COVID
Crise Cyber

Contenir l'épidémie

Soigner les malades

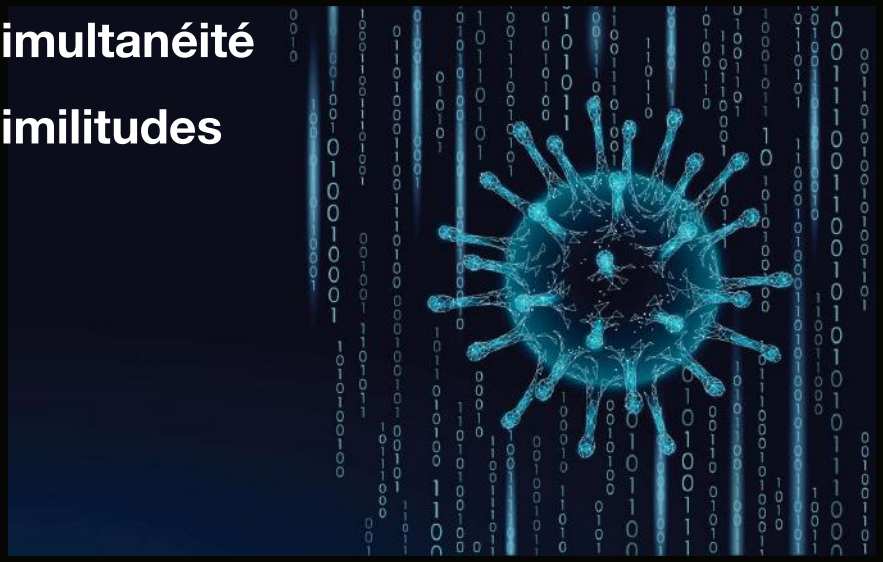
Relancer l'activité

Une double approche

Orientée **système**
Orientée **individu**

Simultanéité

Similitudes



Agenda

- **3 essentiels pour réussir votre déconfinement**
  Tester – Protéger - Redémarrer
- **Retour d’expérience client**
- **Capitaliser sur la crise & anticiper l’avenir**

1. Réussir votre déconfinement 3 essentiels

Déconfinement : enjeux sanitaires, enjeux cyber

Tester → Identifier les populations à risques
Tester massivement

Protéger → Réagir
Isoler & Soigner
Prévenir

Redémarrer → Relancer l'activité
Trouver une nouvelle normalité

Tester

Une approche progressive de test de votre SI
du scan de vulnérabilités aux tests des équipements

Etablir la stratégie de test

Identifier les populations vulnérables

Tests des individus

Système

- Audit SI déconfinement
- Scan de vulnérabilités
- Sonde comportementale

Utilisateur

- Phishing campaign
- Malware check-up

Protéger

Isoler, soigner, prévenir
pour éviter la propagation du virus et traiter ses effets

Isoler

Confiner, mettre en quarantaine pour éviter la contagion

Soigner - Remédier

Traiter les symptômes, chercher un traitement

Prévenir

Suivre les contaminations, identifier la contagion

Système | **Utilisateur**

- DDoS Protection
- Email Protection
- Micro-SOC Endpoint Detection & Response
- Réponse à incident et gestion de crise
- Protection des mobiles

Redémarrer

Trouver une nouvelle normalité
vivre avec le virus, anticiper le prochain confinement

Distanciation

Gestes barrières

Préparer la deuxième vague

Système

Utilisateur

Télétravail : solutions de sécurisation d'accès à distance

Sensibilisation aux bons gestes de cybersécurité

Retour sur la crise et prochaines étapes

Digitalisation des processus, cloud… sécurité des nouvelles architectures

Maîtriser le risque cyber lors du déconfinement en 3 étapes

Tester

Système	Utilisateur
Audit SI déconfinement	Phishing campaign
Scan de vulnérabilités	Malware check-up
Sonde comportementale	
Test d'intrusion	

Protéger

Système	Utilisateur
DDoS Protection	Email Protection
Micro-SOC Endpoint Detection & Response	
Réponse à incident et gestion de crise	Protection des mobiles

Redémarrer

Système	Utilisateur
Télétravail : solutions de sécurisation d'accès à distance	Sensibilisation aux bons gestes de cybersécurité
Retour sur la crise et prochaines étapes	
Digitalisation des processus, cloud… sécurité des nouvelles architectures	

2. Retour d’expérience

La gestion d’une crise dans la crise
Retour d’experience client

Avant l’attaque

Préparation à la crise sanitaire
Révision des PCA, PRA
Veille des élections municipales
Confinement sanitaire à J+2

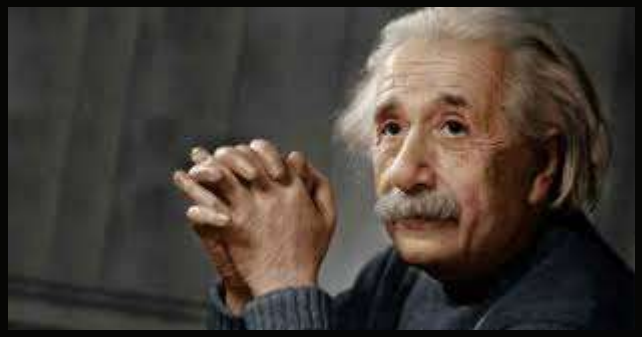
Faire face à 2 crises

Analyser / Comprendre
En faire une opportunité
S’organiser / Prioriser les actions
L’humain au coeur

Enseignements

Durée et coût de la crise
Importance de la communication
Sortie de crise

3. Capitaliser sur la crise et anticiper l’avenir



« La connaissance s’acquiert par l’expérience, tout le reste n’est que de l’information »

Albert Einstein
1879-1955

Un retour d’expérience sur la gestion d’ une crise, c’est quoi ?

1. Analyser les actions et décisions prises pendant la crise

2. Identifier les dysfonctionnements et réussites

3. Formaliser et proposer un plan d’amélioration

- Partager
- Repérer
- Identifier
- Reconnaître
- Valoriser
- Sensibiliser

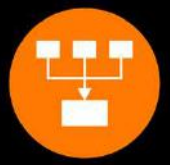
Capitaliser

Apprendre de la crise du COVID pour mieux savoir gérer la prochaine crise cyber.

Impact Covid sur le pilotage de la crise cyber – notre constat

Impact Cyber

La grande difficulté, voire l'inefficacité de la mise en œuvre des plans de continuité



La crise cyber dans la crise sanitaire nous oblige à revoir notre organisation de crise

Impact Général

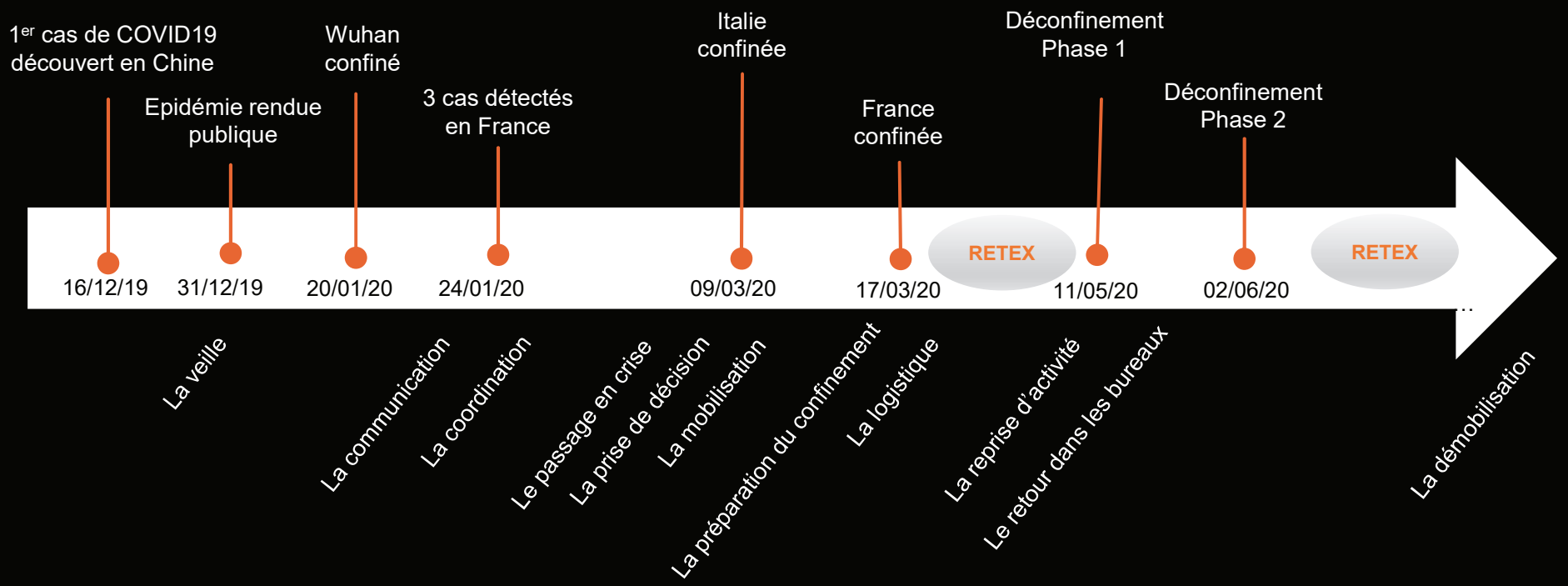
Humain

Image/ Réputation

Opérationnel

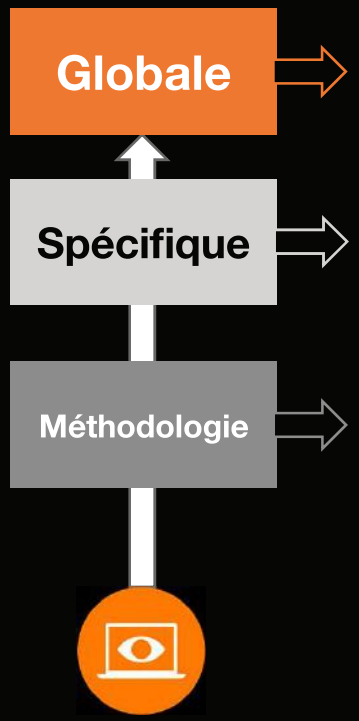
Juridique

La crise est encore longue, ne pas attendre !



Quelle approche ?

Cybersécurité ou sanitaire c'est la même chose !



Approche horizontale et transverse qui va regarder l'ensemble des directions de l'entreprise et ses interactions

Approche verticale par domaine comme celui de la cybersécurité

- ✓ Réaliser un Retex individuel puis collectif
- ✓ Avoir des outils conçus d'avance
- ✓ Définir un plan d'action à court/moyen/long terme
- ✓ Définir un planning projet

Les bénéfices du RETEX

Adhésion → Recréé de l'adhésion après une épreuve difficile

Amélioration → Initie une démarche positive d'amélioration continue

Résilience → Renforce la résilience face à l'évolution des risques

Risques dans la pratique du RETEX

- Recréer de la tension au sein des équipes
- Être juge de ses propres actions
- Ne disposer que de son propre vécu
- Se perdre en n'adoptant pas de méthode dédiée

Facteurs clés de succès

- Avoir un regard externe sur la situation
- Prendre de la hauteur avec une personne neutre
- Bénéficier de l'expérience d'autres entreprises
- Avoir des outils conçus pour le retex et éprouvés

Pour aller plus loin

- Organiser un RETour d'EXpériénce
- Identifier les chantiers prioritaires
- Capitaliser sur la crise & mettre à jour son organisation de crise et son PCA
- Virtualiser sa cellule de crise en s'appuyant sur un outillage indépendant du SI
- Mettre en place des indicateurs & suivre la progression du plan d'action
- Renforcer les actions de formation et de sensibilisation
- Communiquer
- Accompagner la reprise & préparer un éventuel reconfinement

https://orangecyberdefense.com/fr/services/conseil-audit/savoir-faire-face-a-une-cybercrise/
https://orangecyberdefense.com/fr/insights/blog/gestion_de_crise/crise-cyber-comment-gerer-lapres/

Pour conclure

Réussir sa sortie de crise COVID : enjeux cyber

Tester → Identifier les populations à risques
Tester massivement

Protéger → Réagir
Isoler & Soigner
Prévenir

Redémarrer → Relancer l'activité
Trouver une nouvelle normalité

orangecyberdefense.com/fr/deconfinement-tester-proteger-redemarrer/

Deux guides de bonnes pratiques offerts

Système

https://orangecyberdefense.com/fr/insights/blog/fuite_de_donnees/covid-19-les-bons-gestes-de-securite-informatique-a-adopter/

Utilisateur

https://orangecyberdefense.com/fr/insights/blog/fuite_de_donnees/covid-19-les-bons-gestes-de-securite-informatique-a-adopter/

Q&A

Orange Cyberdefense

Merci !

Remerciements

- **Métropole d'Aix-Marseille-Provence**
- **IREMOS**

Pour toute question

- Contact-fr.ocd@orange.com
- **Votre contact commercial Orange habituel**