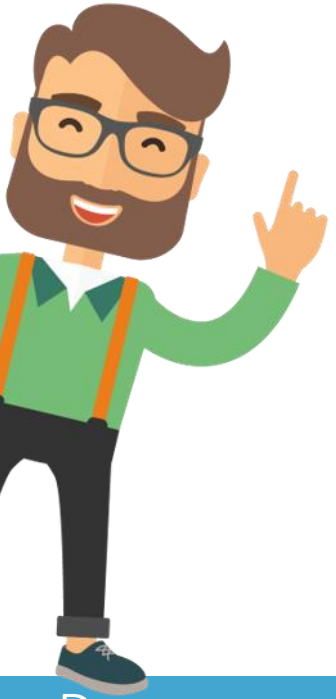
aDvens

SECURITY FOR THE DIGITAL AGE

LA CONFIANCE NUMÉRIQUE

Une dimension stratégique pour cette nouvelle décennie

INTRODUCTION



2020, début d'une nouvelle décennie…
2020, début d'une nouvelle étape dans vos démarches de sécurité ?

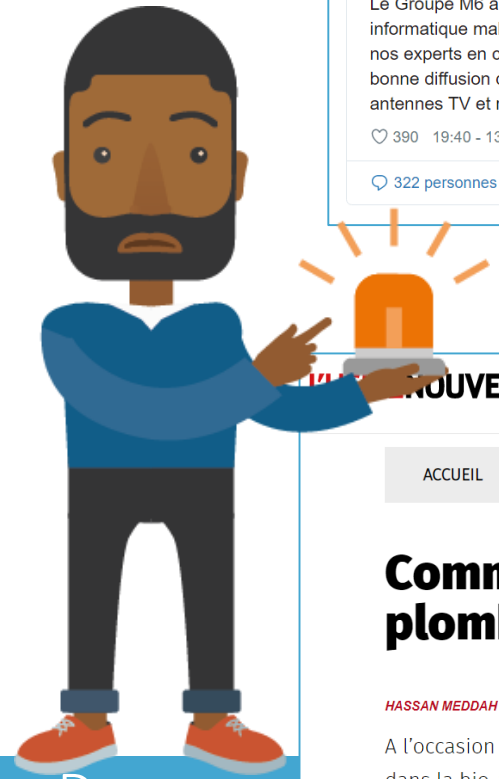
Quelles sont les leçons à tirer de 2019 ?

Comment faire évoluer vos actions pour en augmenter l'impact ?

Quelle posture pour préparer 2020 et cette décennie ?

QUELLES SONT LES LEÇONS À TIRER DE 2019 ?

2019, UNE ANNÉE… INTENSE ?



Groupe M6 @M6Groupe

Le Groupe M6 a été la cible samedi matin d'une attaque informatique malveillante. L'intervention rapide et efficace de nos experts en cybersécurité a permis de continuer à assurer la bonne diffusion des programmes sur l'ensemble de nos antennes TV et radio.

♡ 390 19:40 - 13 oct. 2019

322 personnes parlent à ce sujet

altran

CONSULTING • DIGITAL • ENGINEERING • WORLD CLASS CENTERS • INDUSTRIALIZED GLOBALSHORE®

MISE À JOUR SUR LA CYBERATTAQUE

NOUVELLE Aéro Auto Énergie Agro Ma région Innovation Plus

ACCUEIL | COSMÉTIQUE | PHARMACIE / BIOTECHNOLOGIES | ENTRETIEN / HYGIÈNE

Comment l'attaque par ransomware a plombé les résultats d'Eurofins

HASSAN MEDDAH | L'USINE SANTÉ , NUMERIQUE | PUBLIÉ LE 29/08/2019 À 18H10

A l'occasion de la publication de ses résultats trimestriels, le groupe français Eurofins, spécialisé dans la bio-analyse, a chiffré à 62 millions d'euros le préjudice financier lié à l'attaque par ransomware subie en juin dernier.

AUTRES

23 OCTOBRE 2019

GRAND COGNAC FAIT FACE À UNE CYBER-ATTAQUE INÉDITE

Depuis la semaine dernière, Grand Cognac est confronté à une panne informatique liée à l'attaque d'un virus. Ce virus informatique, d'un genre nouveau, a infecté un serveur de l'agglomération samedi 12 octobre…

2019, UNE ANNÉE… INTENSE ?

Tous les secteurs sont visés…

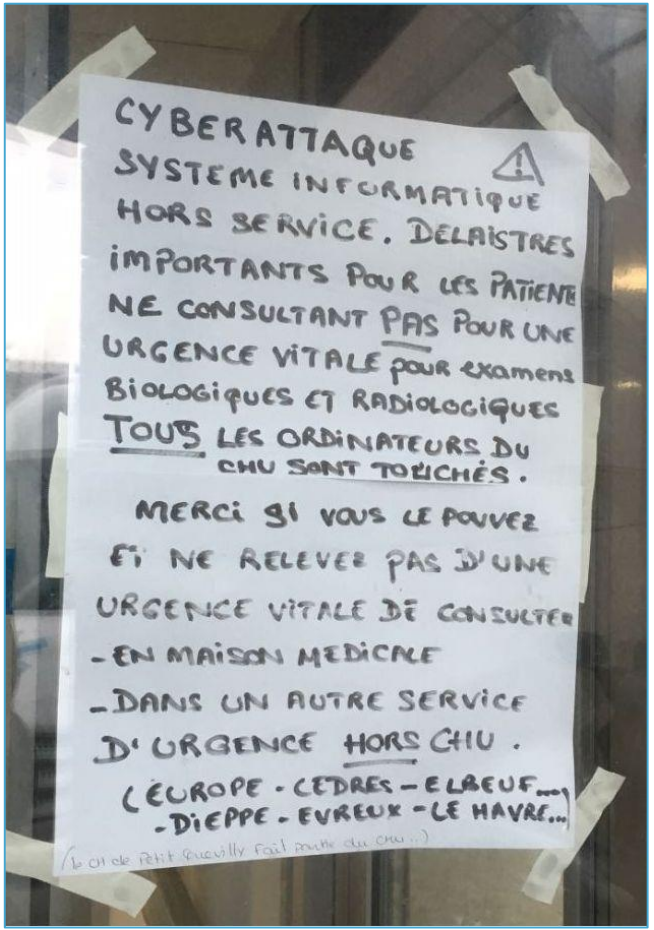
Les impacts sont de plus en plus violents.

INTERVENTION DU CSIRT ADVENS

1ère vague de nettoyage	2ème vague de nettoyage	+ 3 serveurs avec backdoors actives…
1768 Virus différents sur 1500 postes	**Virus persistants sur 650 postes** (EMOTET)	

L'apport de l'EDR

- La nature d'EMOTET rend les solutions antivirales peu-efficaces.
- Le CSIRT a déployé un EDR dans le cadre du traitement de l'incident
- **1 745 agents installés en 3h**
- Déploiement via SCCM sans impact négatif identifié



2019, UNE ANNÉE… INTENSE ?

MARKETING

Mort du général Soleimani : l'Iran pourrait lancer une vague de cyberattaques

Le Conseil suprême de la sécurité nationale iranien a déclaré que les États-Unis devaient s'attendre à subir une "dure vengeance".

Par Valentin Cimino - @ciminix

Publié le 4 janvier 2020 à 14h11 - Mis à jour le 7 janvier 2020 à 15h52

Israel Defense Forces @IDF

CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

QUELLES LEÇONS TIRER DE 2019 ?

Les Echos

une Idées Économie Élections Politique Monde Tech-Médias Entreprises Bourse Finance - Marchés Régions Patrimoi

Cyberrisque : la grande peur des assureurs

Le risque cyber est devenu la première menace des entreprises dans le monde, selon le baromètre Allianz. Les assureurs traînent des pieds pour couvrir ce nouveau risque systémique.

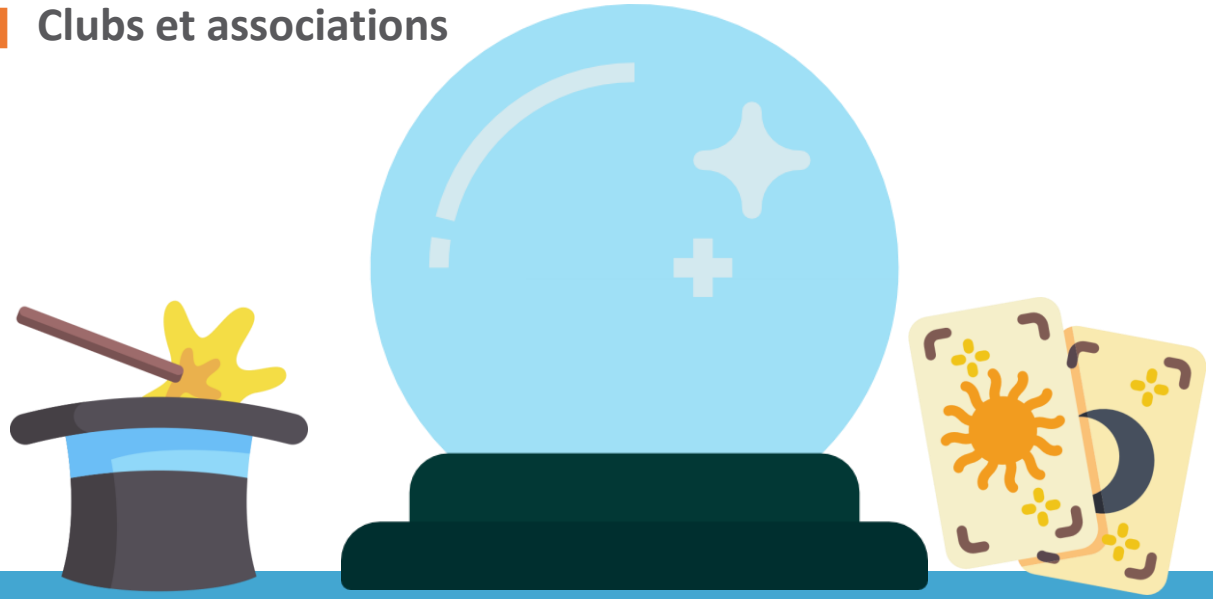
Au cas où vous en doutiez encore… sachez que la cybersécurité n'est plus une option !

QUELLES ORIENTATIONS POUR 2020 ?

QUELLES ORIENTATIONS POUR 2020 ?

La nouvelle rime avec l'arrivée des prévisions…

- Editeurs et fournisseurs de solution
- Cabinets d'analyses
- Clubs et associations



QUELLES ORIENTATIONS POUR 2020 ?

Nouvelles tendances du côté des attaquants

- Attaques étatiques ou assimilées… et utilisation plus large des outils de ces attaquants
- Multiplication des attaquants et flou dans leur profil
  Un jour dans la blue team, le lendemain chez les assaillants…
- Nouvelles techniques de piégeage
  Deepfake, DNA leaks, etc.
- Et toujours et encore (plus fort) : les ransomwares

QUELLES ORIENTATIONS POUR 2020 ?

De nouveaux périmètres à intégrer

- Tout ce qui sort du périmètre de la DSI traditionnelle :
  OT & IoT
  Cloud sous toutes ses formes (IaaS, PaaS, SaaS)
- Les nouveautés technologiques : l'exemple de la 5G
- L'entreprise étendu et son écosystème
  Focus fort : les fournisseurs et la « supply-chain »
- Et en « bonus »
  La supply-chain logicielle et les mécanismes de mise à jour automatique
  Les utilisateurs à privilège… pas que les admins sys !

QUELLES ORIENTATIONS POUR 2020 ?

Vous reprendrez bien un peu de conformité ?

- La directive NIS, pour les OSE et pour les FSN aussi !
- La LPM 2018
- Le cyberSecurity Act
  Institutionnalisation de l'ENISA
  Définition d'un cadre européen de la certification de cybersécurité
- Et du côté de la privacy ?
  La GDPR version « Californienne » : le CCPA
  ePrivacy, la suite ?

COMMENT SE PRÉPARER POUR 2020 ET LA DÉCENNIE ?...

COMMENT SE PRÉPARER ?

Faire évoluer la gouvernance et renforcer le sponsor de la direction

- Faire face à un COMEX de plus en plus curieux
- Embarquer les métiers et les responsabiliser
- Préparer la transition de RSSI à Directeur Cybersécurité ?

COMMENT SE PRÉPARER ?

Focus sur l'étude menée par Advens et le CESIN

Identifier l'ensemble des risques Cyber et spécifier les stratégies et politiques pour y faire face.

Elaborer et animer un catalogue de services et de solutions qui vont permettre à chaque partie d'intégrer la sécurité en amont dans ses activités et dans les projets de l'entreprise, en couvrant les dimensions techniques, contractuelles, assurancielles, organisationnelles et humaines.

Concevoir et mettre en œuvre les stratégies de continuité et cyber résilience des Systèmes d'Information.

Identifier, choisir et déployer les dispositifs opérationnels de surveillance, détection et réponse aux incidents et de gestion de crise.

Développement la culture sécurité, en filigrane de toutes ces activités.

COMMENT SE PRÉPARER ?

Intégrer la sécurité dans toutes les facettes de la transformation numérique

- Ne pas laisser le « digital » oublier la sécurité… ni se faire « uberiser »
- Tisser des liens avec les équipes DevOps et trouver des relais

  Identifier des « Security champions » pour porter la bonne parole et intégrer la sécurité dans la chaine d'intégration continue
- Appliquer à la sécurité les nouvelles méthodes

  Rendre sa démarche de sécurité plus agile

  Prendre le temps de tester des solutions innovations

  Fail fast, learn faster

- ANALYSE DE RISQUES
- IDENTIFICATION DES EXIGENCES DE CONFORMITÉ
- PLAN D'ASSURANCE SÉCURITÉ
- DÉFINITION DU PLANNING
- DÉFINITION DES COMITÉS ET DE LA GOUVERNANCE SÉCURITÉ

AJOUT DES MESURES DE SÉCURITÉ DANS LE BACKLOG (PLAN DE TRAITEMENT)

SPRINT 0
- SENSIBILISATION DE L'ÉQUIPE PROJET
- PROTECTION DES DOCUMENTS PROJET ET DES DONNÉES DE TESTS
- SÉCURISATION DE L'ARCHITECTURE DE DÉVELOPPEMENT
- DÉPLOIEMENT DES OUTILS DE TESTS DE SÉCURITÉ

SPRINT 1
- REVUE D'ARCHITECTURE
- DURCISSEMENT DES SOCLES
- SÉCURITÉ DE L'HÉBERGEMENT

SPRINT 2
- DÉFINITION DES ALERTES SÉCURITÉ
- DÉFINITION DES TRACES ET DES LOGS
- GESTION DE CRISE ET D'INCIDENT

SPRINT N
- INTÉGRATION DE LA SÉCURITÉ DANS LES ATELIERS DE CONCEPTION (COUVRANT A MINIMA : DONNÉES, FLUX, TRANSACTIONS, ACCÈS)
- TESTS UNITAIRES DE SÉCURITÉ / REVUE DE CODE
- CORRECTION DES CODES

TEST
- TESTS DE SAUVEGARDE
- TESTS DE BASCULE
- TESTS DE GESTION DE CRISE

RETRO
- COMMUNICATION / TUTO D'ACCÈS À LA SOLUTION
- SENSIBILISATION DES UTILISATEURS CLÉS
- DIFFUSION DES CHARTES D'USAGE ÉVENTUELLES

BUG ANOMALIE
- INTÉGRATION DANS LE SOC / DANS LES OUTILS D'ALERTING

aDvens
@advens
linkedin.com/company/advens

COMMENT SE PRÉPARER ?

Prendre en compte tous les périmètres

Cloud

CSPM : Cloud Security Posture Assessment

OT & IoT

Comprendre les possibilités techniques et les contraintes opérationnelles

Etudier les solutions spécialisées

Supply-chain

Quel avenir pour le « questionnaire Fournisseur » ?

Vers un fonction à part entière dans la filière Cyber ?

COMMENT SE PRÉPARER ?

Se préparer au pire et muscler ses capacités de détection et réaction

- Gagner en visibilité et en capacité d'action grâce à l'EDR
- Challenger sa stratégie de résilience et y intégrer la Cyber
- Entrainer ses équipes pour les temps de guerre et pas uniquement les temps de paix

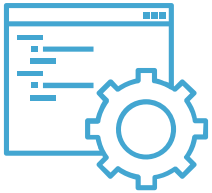
  Le « cyber-range » se développe et peut être une opportunité de team building !

COMMENT SE PRÉPARER ?

Développer les nouvelles compétences attendues par la filière Cyber

Connaitre et comprendre les nouvelles technologies

Être « code-fluent »

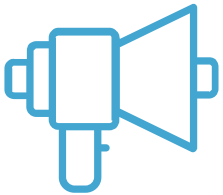


Décrypter les tendances et les nouveaux usages

Maitriser les data sciences

Conjuguer agilité et réactivité

Communiquer à tous et dans tous les contextes



POUR CONCLURE

LA ROUTE SERA LONGUE !

Benjamin Leroux

benjamin.leroux@advens.fr

advens

SECURITY FOR THE DIGITAL AGE

advens.fr

Paris +33 1 84 16 30 25

Lille +33 3 20 68 41 81

Lyon +33 4 28 29 08 29

Bordeaux +33 5 35 54 82 84