ATELIER CYBERSÉCURITÉ DU TIC SANTÉ

21/03/2022

PRÉSENTATION D'ADVENS

Ensemble… …en avance

« Donner du sens à nos métiers, au service de vos métiers
Donner du sens à nos entreprises, au service de la société »

#advensforcybersecurity **#advensforpeopleandplanet**

1ER PURE-PLAYER FRANÇAIS DE LA CYBERSÉCURITÉ

Depuis 20 ans, nous accompagnons nos clients pour les aider à prendre de l'avance et faire de la sécurité un actif différentiateur.

300
Collaborateurs
Paris, Lille, Lyon, Bordeaux, Nantes, Toulouse & Bruxelles

30%
Croissance annuelle

+300
Clients actifs
En France et à l'international

ZOOM SUR LA NOUVELLE-AQUITAINE

Advens travaille dans le Sud-Ouest de la France depuis 10 ans

- 30 collaborateurs rattachés au bureau de Bordeaux : experts, chefs de projet, analystes, forensics, auditeurs
- Mécène fondateur de la Chaire Cyber-résilience de l'ENSEIRB MATMECA
- Membre du futur Campus cyber porté par la Région Nouvelle-Aquitaine
- Organisation d'événements (CTF, Afterworks)
- Participation aux clubs DSI & RSSI

La FRENCH TECH BORDEAUX

Bordeaux INP ENSEIRB MATMECA

C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière

Région Nouvelle-Aquitaine

CLUSIR #Aquitaine

DIGITAL AQUITAINE

UGAP

CYBER'OCC

ADVENS EST LE PARTENAIRE DE CONFIANCE DU SECTEUR PUBLIC ET DES PME & ETI !

ENSEMBLE ET EN AVANCE,
À LA CONQUÊTE DE GRANDS DÉFIS !

Depuis 2017, Advens accompagne Thomas Ruyant dans sa conquête d'un immense défi sportif, humain et technologique : le Vendée Globe.

- Construction d'un voilier à foils dernière génération,
- Collaboration R&D pour augmenter la performance et la sécurité du bateau et du marin.

Convaincue que l'entreprise a un rôle sociétal clé à jouer, Advens a ouvert la voie de La Course Au Changement pour permettre un changement d'échelle à l'inclusion en France

- **Visibilité et naming du bateau offert à LinkedOut,** dispositif de la Tech positive qui accompagne des personnes en précarité dans leur retour à l'emploi
- **Engagement de l'entreprise :** sensibilisation des équipes, collaborateurs coachs bénévoles, audit de sécurité (mécénat de compétences), collectes de dons, partages de réseau, recrutements, workshops filière cyber inclusive…

Rejoignez vous aussi La Course Au Changement pour contribuer ensemble à un monde plus juste et plus durable !

WWW.LINKEDOUT-VENDEEGLOBE.FR

LA CHAIRE CYBER-RÉSILIENCE

CHAIRE CYBER RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES

POURQUOI UN DIPLÔME D'ÉTABLISSEMENT

Les motivations de l'ENSEIRB et des mécènes

Répondre à la menace qui explose dans un contexte de pénurie de compétences

- 3M d'experts cybersécurité manquent dans le monde

Former des profils variés et faire émerger des vocations

- Les professionnels déjà en poste
- Les étudiants souhaitant compléter leur formation

Proposer un contenu à 360°

- Réunir dans un même format toutes les facette de la cybersécurité : organisationnelle, réglementaire, technique

ÉTAT DE LA MENACE

LA MENACE CYBER DANS LE CONTEXTE DE LA GUERRE EN UKRAINE

Un contexte géopolitique inattendu, dans lequel la menace Cyber semble omniprésente…

Se tenir prêt en cas d'attaque

- Veiller à la bonne application des mesures « standard » d'hygiène informatique (Guide d'hygiène de l'ANSSI) comme l'authentification forte, la détection (via EDR notamment), la mise en place d'une capacité de réaction en cas de crise et la bonne gestion des sauvegardes...
- Intégrer dans votre SOC les indicateurs relatifs aux nouveaux malwares détectés (HermeticWiper et NotPetya notamment) ou botnet (Cyclops Blink)

Garder la tête froide

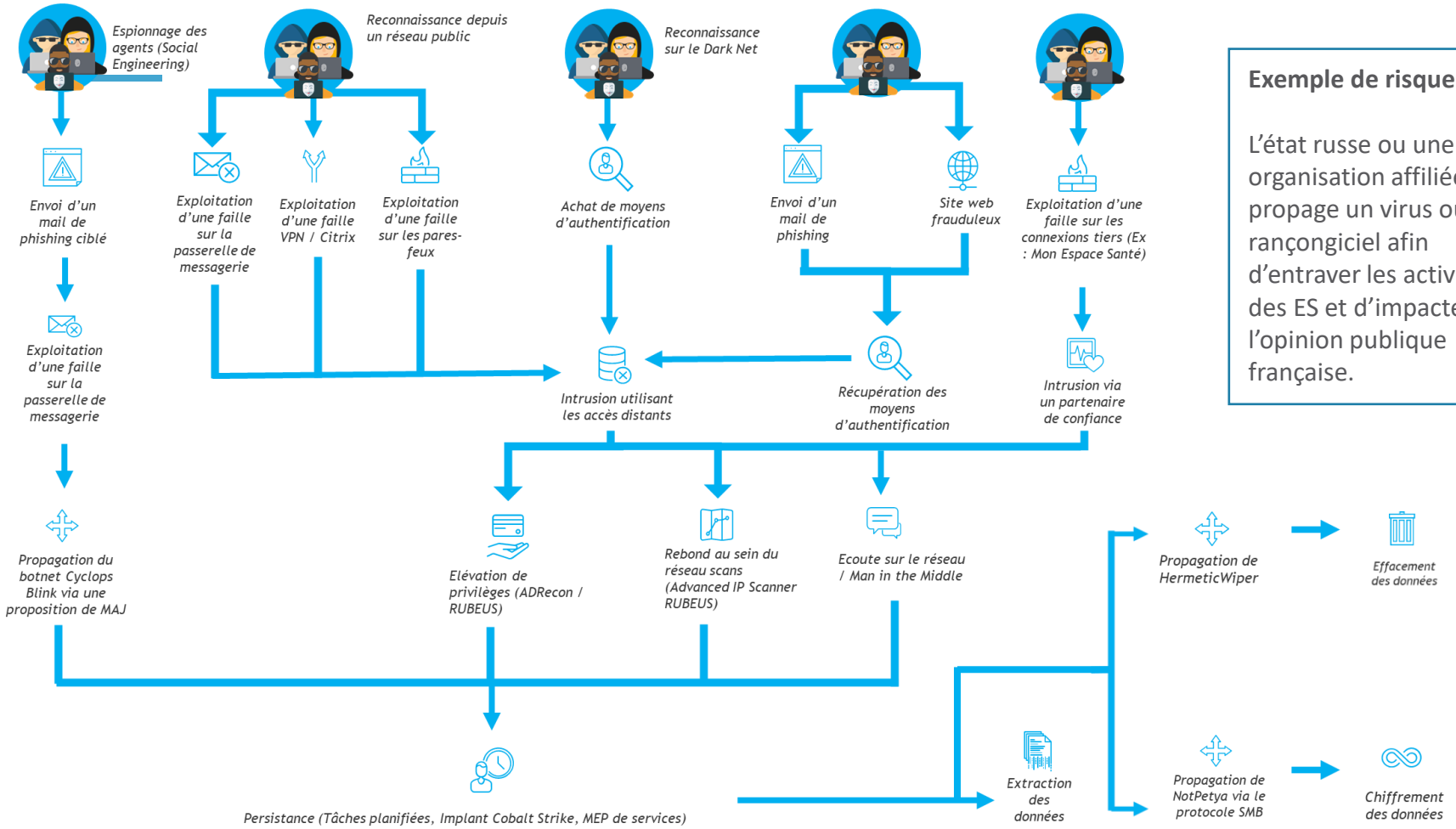
- Challenger les informations et ne pas céder à une forme de panique
- Ne pas se précipiter dans le changement des solutions technologiques mais penser à une approche long terme

Quelques liens utiles

- https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
- https://www.cybermalveillance.gouv.fr/

EVALUER LES MENACES DANS LE CONTEXTE

Sources	Description	Objectifs visés	Moyens d'attaque privilégiés
 **Etatique**	Etat ou agence de renseignement capable de mobiliser des ressources et des moyens importants sur un temps long, pour acheter ou créer des moyens d'attaque ou découvrir des vulnérabilités (zéro-day)	→ Entrave au fonctionnement / Black out → Influence / Déstabilisation → Prépositionnement stratégique → (Attaque opportuniste)	→ Désinformation s'appuyant sur des « Data leak » ou de fausses informations → Supply chain compromise → Malware (ex : HermeticWiper, Cyclops Blink, Sandworm…) → Attaques DDOS
 **Crime organisé**	Organisation cybercriminelle, potentiellement liées à l'état russe, disposant de moyens et ressources importantes pour réaliser des attaques sophistiquées.	→ Lucratif → Prépositionnement stratégique → Entrave au fonctionnement → (Attaque opportuniste)	→ Malware (ex : HermeticWiper, Cyclops Blink, Sandworm…) → Supply chain compromise → Attaques DDOS
 **Cybermilices / Cyberterrorisme**	Organisation indépendante disposant de ressources limitées mais d'une détermination forte pour nuire à leur cible (déstabilisation voire destruction)	→ Entrave au fonctionnement → Influence / Déstabilisation	→ Attaques DDOS → Défigurations → Désinformation s'appuyant sur des « Data leak » ou de fausses informations
 **Officine spécialisée**	Organisation de type cyber mercenaire disposant de compétences fortes pour créer des outils ou des kits de piratages.	→ Lucratif → (Attaque opportuniste)	→ Conception et/ou utilisation de malware → Reconnaissance
 **Activiste idéologique**	Individu ou groupes d'individus dont les modes opératoires se rapprochent des Cybermilices mais ayant des intentions moins destructrices.	→ Influence / Déstabilisation	→ Désinformation s'appuyant sur des « Data leak », de fausses informations → Utilisation des réseaux sociaux → Défigurations → Attaque DDOS



Exemple de risque :

L'état russe ou une organisation affiliée propage un virus ou un rançongiciel afin d'entraver les activités des ES et d'impacter l'opinion publique française.

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