Sûreté, Sécurité, Contre-Espionnage

Guide de bonne conduite pour éviter les fuites d'informations !

Gaby Wald

to be defined

8 avril 2025

Sommaire

Définitions et pourquoi

Sûreté et Sécurité et ...

- Complémentarité et différences entre Sûreté et Sécurité ;
- Sûreté : surveriller, éviter l'intentionnel et la malveillance ;
- Sécurité : éviter et soigner (voire guérir) l'accidentel

- Ensuite 3 axes : bonne conduite, protection de l'information et sécurité informatique ;
- Contexte de "Guerre Économique", sans "Convention de Genève" (chômeurs et autres exclus) ;
- Contestation et créativité : protéger compétences, techniques, expertises, découvertes... ;
- ...

Contexte et nécessités

- Problème identifié rendu public (vol de portable, cyberattaque)... ;
- Taille critique de l'entité et exposition automatique : besoin, d'une sûreté interne (et / ou aide externe) ;
- Menaces identifiées et à identifier : introduction téléphonique / physique / "cyber" ;
- Préconiser, répondre, supporter ;
- Standards à mettre en place (physique : grillages, sas, tourniquets, procédures...)
- ...
- ...

Sûreté et Menaces

- 3 niveaux sûreté
  - DSSEP
  - Correspondants sûreté
  - Collaborateurs / Agents (internes à l'entité)
- Menaces sur l'entité (quelque soit l'entité)
  - Sûreté nécessaire ;
  - Malveillance ;
  - "Délinquance au quotidien" qui cible particuliers et organisations ;
  - Informatique, matériel, stylos, montres... ;
- Caméras : protéger l'infrastructure (limité par la CNIL, l'inspection du travail et le code du travail) ;

Attaques internes / externes : typologie et impacts

- Espionnage industriel ;
- Contrefaçons ;
- Image de l'entité (et notoriété) ;
- Intégrité physique des collaborateurs / agents ;
- Lutte anti-(anti-exploitation animale) ou équivalent (lié à activité entité) ;

- $\Rightarrow$ Réagir vite car opinion publique malléable !

Problématiques connexes pas si annexes

Contrefaçons

- Produits contrefaits $\Rightarrow$ Autres soucis bien supérieurs au manque à gagner !
- Impacts sur la santé publique (pharmacie, cosmétique, tabac, autres...) ;
- Impacts sur l'environnement (production, déchets...) ;
- Impacts sur la santé publique (pharmacie, cosmétique, tabac, autres...) ;
- À l'image de l'entité, si contrefaits adroitement ET de mauvaise qualité : mauvaise image de l'entité !

Image (médiatique) de l'entité

- "Entité" : entreprise, agence gouvernementale, administration...
- Emploi, recrutement, fournisseurs, clients... De nombreux liens !
- Visibilité gérée :
  - Badges (couleur selon typologie de personnel : permanent, temporaire...) ;
  - Tours de cou aux couleurs de l'entité : gérer l'accès et éviter captation / vol / copie et risques liées à cette visibilité ;
  - Supports de communications diverses : identifiables, diffusion contrôlée, peut toujours être copié / détourné ;
- ...

Intégrité physique des collaborateurs / agents

- Trajets domicile / travail (conditions, navettes, contrôles d'accès à l'entrée...) ;
- Conditions de travail ;
- Voyages d'affaire (le plus important) : localiser et récupérer en cas de prise d'otage, guerre, négociation... : Déclaratif voyages et situation dans la destination (blanc, jaune, orange, rouge) + déclaratif pour joindre en permanence, motivation manuscrite si besoin ;
- ...
- ...

Lutte anti-(anti-*) : groupes opposants

- Lutte anti-(anti-*) : groupes opposants, quelqu'en soit le sujet / contexte...
- Lié à une activité légitime de l'entité (exploitation animale, matériaux radioactifs...) ;
- Groupes d'activistes et communauté en lien, contestation parfois sportive des manifestants ;
- Réponses téléphoniques et problèmes d'appels récurrents ;
- ...
- ...

Espionnage économique industriel

- Augmentation depuis la fin de la Guerre Froide (ne concernait QUE le militaire pendants cette période ? ?) ;
- L'information est un produit marchand (devis, factures...) ;
- Espions, fonctionnaires ordinaires ? (Convention de Vienne) ;
- Arme Ultime : Intelligence Économique (légale),
  pratique collective (recueil, analyse et distribution informations par voie légale) ;
  veille et captation de l'information : rapport d'étonnement !
- Coups classiques : ordinateur / téléphone / blackberry ou autre smartphone dans les transports
  mais aussi : restaurants, bar, ascenseurs, hôtels, taxi, coiffeurs... ("n'est sourd que celui qui ne veut pas entendre")

Protection, des bases

Documentation "sensible"

- Classification des documents (diffusable, interne, et différents niveaux de confidentialité et TLP / couleurs) ;
- Clefs / armoires / coffres ; broyeuse ; "clean desk" ...
- Ordinateur : câble antivol (qui doit remplir sa fonction) ;
- Ne pas laisser de clefs ou de badges sur les portes ;
- Impression : aller chercher le résultat sur l'imprimante papier au moins 2 fois par jour
- Supports d'échanges, confidentialité des échanges, ...
- ...

Externes, Stagiaires, Visiteurs...

- Stagiaire (plus de cinq jours) : référent + considération + savoir où + confidentialité + suppression éléments rapports et thèses
- Visiteurs : communication / vitrine ;
  Organiser le temps et l'espace de la visite
  Jamais la personne questionnée qui doit répondre ! Détourner la question, aiguillonner sur une autre personne...
  Personne(s) qui a (ont) l'habitude d'accompagner.
  Montrer ce que l'on veut montrer.
- Prestataires : limiter à la nécessité absolue ? !
- Bienveillance malgré surveillance : "le stagiaire d'aujourd'hui peut être le Nobel / Turing / Fields de demain : autant qu'il ou elle se rappelle de vous dans ses bons souvenirs !"

Intelligence économique / Espionnage Industriel

- Protéger activité de l'entité et éviter diffusion de données pouvant nuire (données internes, bénéficiaires, salariés...)
- **Suivi et traçabilité** ;
- Prestation / sous-traitance : points sensibles, RH et informatique ;
- Également : prestataires, stagiaires, technologie sous toute ses formes (ordinateur, écran, photocopieuse, fax, téléphone...)
- "Coup classique" et lieux communs / publics : ascenseur, métro, train, avion, hôtel, transports...
- "Documents sensibles" : clefs, armoires, coffres, broyeuses, "clean desk"...
- Anticvls fonctionnels, pas de clefs laissées en place (portes, caissons...) ;
- ...

Ingénierie Sociale (1)

- "Confiance Spontanée", échanges pas forcéments contraints, obtenir information ou accès par symptathie ou crédibilité ;
- Vérification (systématique) des informations, interlocuteurs connus et reconnus ;
- Mettre en confiance (contexte, costume, ambiance sonore...) ;
- Pression / manipulation : ne pas laisser le temps de réfléchir, "le culot", "la drague"...
- "Contre SE" : confidentialité, escorter inviter, sensibilisation (affichage, conférences, rappels...)

Ingénierie Sociale (2)

- Préparer la situation (nom, acolyte) ;
- Scénarios (support technique fallacieux, faux fournisseur, faux concours, faux sites web / employés / visiteurs / recruteurs...
- Objectifs : accès (clefs, badges, identifiants, propriété intellectuelle, informations sur employés, liste des clients / prospects / bénéficiairees...
- Poubelles : listings, annuaires, organigrammes, carnets, règles, organisation réseau, mots de passe...
- "Contre SE" : préparation(s), exercices, sensibilisation...

Introduction Vigilance Renseignement

OSINT et OPSEC (1)

- OSINT (Open-Source Intelligence)
  - Recherches en Sources Ouvertes (SO) ;
  - Rapatriement de données et requêtage, services spécialisés, outils en accès libres ;
  - Outils et Données peuvent être récupérés puis analysés offline ;
- OPSEC (Sécurité Opérationnelle)
  - Ne pas montrer ce que l'on fait (de façon intentionnelle) ;
  - Minimiser la divulgation intentionnelle (contrôle) ;

OSINT et OPSEC (2)

- Sujets non abordables en dehors d'un cadre défini (physique, temporel) :
  - Nucléaire ;
  - Renseignement (services) ;
  - Présidence / Direction ;
  - Opérations ;
- "Moche à Paris, Moche en Russie" ;
- "Ce qui se passe à bord du Galactica..." ;

OSINT et OPSEC (3)

- Segmenter et attention aux "amitiés" ;
- Accès professionnels sont... professionnels ! (codes, VPN, ...) ;
- Pas de mise en évidence ;

Charte SI, et rappels de bonnes pratiques (1)

- Yubikeys et autres MFA (Multi-Factor Authentication) ;
- Consignes mises à jours régulièrement pour trajets à l'étranger ;
  - prévenir trajet en amont ;
  - délais ;
  - durées séjours ;
  - briefing avant ;
  - destinations ET escales avec durée ;

Charte SI, et rappels de bonnes pratiques (2)

- Déplacements, formations, passeports de services (pour déplacement pros !) ;
  - Ojectif de passeport de service est déviter la diffusion des adresses personnelles et l'association de visas exotiques
  - En binômes le plus souvent ; et sensibilisation le plus souvent (formation "évoluer en contexte international")
  - Valise blanchie (spécifique ET ne rien laisser trainer (idem coffre), toujours conserver sur soi ;
  - Que les données nécessaires ;
  - Équipements éteints pendant le trajet ;

Labels de Classification

- Visibilités et limitations, restrictions, notamment sur documents (physiques, numériques...) ;
- TLP "Traffic Light Protocol" : pour DIFFUSION ;
  - Non-Classifié ; Diffusion Restreinte ; Secret ; Top Secret ;
- PAP "Possible Action Protocol" : pour UTILISATION ;
  - CLEAR / WHITE ; YELLOW ; AMBER ; RED ;
- Attention aggrégation [DR $\Rightarrow$ S $\Rightarrow$ TS] : SECRET (et mention) ;

$\Longrightarrow$ Ce n'est pas le support ou la transmission qui fait la classification (c'est le **contenu qui est classifié** !)

IG 1300

- Directive Inter-Gouvernementale / Ministérielle (France) ;
- Définitions pour : mobiliser, protéger, limiter l'accès aux données, informations, supports ;
- Accès et habilitations, besoin d'en connaitre (exercice, accomplissement, ...) ;
- Choix, tampons / templates (modèles), page de garde, mentions particulières ;
- DR : Diffusion Restreinte = protection ;
- Supports amovibles : demander, usage dédié (échanges d'un certain niveau uniquement, dans un sens unique) ;

Supports d'échanges et de transports

- Enveloppes dédiées et sur-enveloppe (ouverture des deux est un accès significatif) ;
- Pour types de transports (documents, outil informatique...) ;
- Supports amovibles : échanges d'un certain niveau uniquement ou dans une direction unique ;
- Déclassification : au cas par cas, automatique 50 / 15 / 75 ans ;
- Nettoyage (par logiciel, commandes spécifiques, ou matériel) ;

Renseignement / Espionnage / Contre-Espionnage

Espionnage Universel (public, privé...), objectifs :

- Accéder à des informations sensibles ;
- Avoir un coup d'avance ;
- Se rassurer ;
- Peser sur les processus décisionnels ;
- Influencer ;
- Maitriser des problématiques internes ;

"Vous êtes des cibles. "

- Prendre du recul ;
- Analyser les leviers psychologiques ;
- Entité, réseau, badges, accès bâtiment, habitudes...
- Sociogramme ; sur un temps plus ou moins long ;
- Faisceaux d'indices concordants ;

- "Processus long cabinet de conseil" et autres cas : ne pas hésiter à dire non !

Processus de recrutement

- Ciblage ;
- Environnement ;
- Approche ;
- Recrutement
- Phase d'activation ;
- Traitement ;

Le recueil de renseignements

- Informations classifiées ;
- Informations grises ;
- Information ambiance ;

- Documents internes et plus ou moins classifiés ;

- Puzzle de petits éléments : petits détails de sécurités, négligences...

Préparation et évitement

- Vitesse → comme le marketing → sentiment d'urgence : si pas de danger de mort ou danger immédiat → être moins reptilien ! !
- Préparer, éviter le chaos, ne pas sortir du cadre de sécurité : fiabilité et règles et temporiser
- Moyens des espions : OSINT ; HUMINT ; Réseaux Sociaux ; Petites Annonces ; Compromission ;

Facteur humain et leviers de recrutement

- Effet d'habitude ; démarches banales ;
- "Voyager léger" (séparer mondes pro / monde perso) ;
- Entretiens de recrutement "rémunérés" (?) ;
- Prudence au quotidien (et prévenir) ;
  - Lieu de travail et environs ;
  - Sollicitations d'anciens collègues , amis ;
  - Vols ciblés : bien vérifier ;
  - Activités extérieures ;
  - Trajets ;
- ...