LES RENDEZ-VOUS DE LA CHAÎNE LOGISTIQUE DU FROID

MARSEILLE, 17 MAI 2019

TRANSFRIGOROUTE FRANCE

UNTF Union Nationale du Transport Frigorifique

USNEF

IRENCO
ACTIONABLE
KNOWLEDGE
DESIGNERS

LA CHAÎNE LOGISTIQUE DU FROID

SURETE DE L'INFORMATION ET FACTEUR HUMAIN

Mémento

Edition 2019. v0-2

NE PAS DIFFUSER EN DEHORS DE LA CHAINE LOGISTIQUE DU FROID

TABLE DES MATIERES

LES ENJEUX

Transmission non contrôlée d'informations, fuite d'information, diffusion inappropriée… quels que soient les termes employés, toutes les organisations sont aujourd'hui exposées à ce type de risque.

Si elles prennent généralement des mesures pour protéger leurs infrastructures physiques et leurs systèmes d'information, l'expérience montre pourtant qu'elles négligent bien souvent l'importance du facteur humain.

Les secteurs stratégiques ou sensibles présentent des dangers accrus en matière de risque informationnel, notamment en raison du volume d'informations échangées et de la sensibilité des informations traitées. Les déplacements, les missions ou le détachement de collaborateurs peuvent en outre constituer un facteur aggravant de risque en raison du changement d'environnement socioculturel.

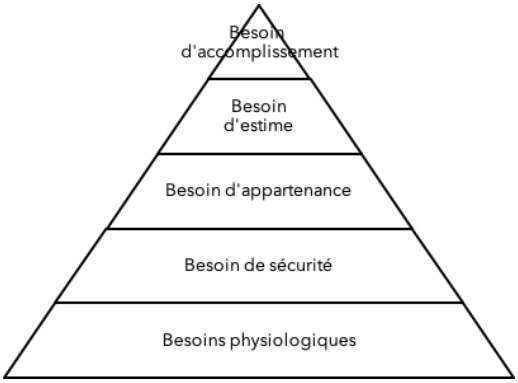
Ce mémento rappelle un ensemble de bonnes pratiques pour se prémunir contre ces risques. Il s'articule en trois parties : les risques liés au facteur humain, les risques liés aux technologies, et les risques liés aux déplacements.

RISQUES & FACTEUR HUMAIN

PSYCHOLOGIE HUMAINE ET MANIPULATION

Dans des situations données, les réactions des individus peuvent être anticipées : réaction instinctive (la peur ou de la colère par exemple) ou en fonction des sensibilités culturelles ou individuelles de chacun (honte, gêne…

Ces sensibilités sont généralement liées à la volonté de satisfaire des besoins : réussite, amour, orgueil, argent, idéologie, ego, reconnaissance, sexe, loyauté, confiance… En nous caractérisant, elles nous rendent donc prévisibles. Les travaux de Maslow proposent une hiérarchie de ces besoins qui déterminent la motivation et donc le comportement des individus.



- **Exemples de besoins physiologiques :** Respirer, dormir, se nourrir, se chauffer, recevoir une juste rémunération, bénéficier de bonnes conditions de travail…
- **Exemples de besoins de sécurité :** satisfaire ses besoins matériels, avoir de la stabilité, vivre dans un environnement sécurisé, être professionnellement stabilisé…
- **Exemples de besoins d'appartenance :** Obtenir un statut social, intégrer un groupe, pouvoir s'exprimer, avoir l'occasion être en contact avec d'autres personnes…
- **Exemples de besoins de reconnaissance :** Être reconnu, être apprécié, être visible, faire un travail utile et apprécié, participer à la définition d'objectifs professionnels…
- **Exemples de besoins de réalisation de soi :** S'épanouir, méditer approfondir sa culture, être autonome, être consulté et écouté, se développer professionnellement…

LES FORMES DE LA MANIPULATION

La manipulation permet d'agir sur le comportement d'autrui. Il est important de connaître les rudiments des techniques de manipulation pour pouvoir les détecter si on en est la cible.

La prévisibilité évoquée ci-dessus rend les individus manipulables par des personnes capables d'identifier nos faiblesses. Laisser filtrer des informations sur soi, même celles qui semblent anodines (discussions, exposition sur les réseaux sociaux…), accroit son exposition.

Les formes de manipulation sont variées : il est possible d'adopter la technique dite « du mimétisme » (vous ressembler pour vous attirer) pour vous faire croire que vous avez énormément de points communs. Une autre technique consiste à vous renvoyer l'image de ce à quoi vous aspirez (situation sociale, physique, réussite financière…). Dans tous les cas, la personnalité de votre manipulateur s'adaptera à vous.

Plus la manipulation sera subtile, plus vous aurez l'impression d'avoir volontairement consenti aux choix qui vous piègent.

LES VULNÉRABILITÉS LIEES AUX DÉPLACEMENTS

En situation de déplacement, vous êtes d'autant plus vulnérable que vous êtes privé d'une partie de vos repères : cadres familial et amical, environnement et lieux familiers…

Le sentiment de liberté peut vous amener à vous comporter de façon inhabituelle, loin du contrôle social.

A l'inverse, nous avons naturellement tendance à reconstituer notre environnement social et affectif. Tout élément qui vous rappellera votre vie « hors déplacement » ou « normale » pourra alors servir d'accroche pour vous manipuler.

SE CONNAITRE POUR MIEUX SE PROTEGER

Nos faiblesses étant liées à nos aspirations, nos besoins et nos frustrations, il est nécessaire de pouvoir s'autoévaluer afin anticiper ses propres risques. Par exemple, chacun pourra, à titre individuel, se poser les questions suivantes :

Dans ma vie personnelle, je suis :

- Seul et heureux / seul et frustré ? En couple et comblé / j'ai des problèmes conjugaux ? Je suis plutôt solitaire / je supporte mal la solitude ? …

Dans ma vie professionnelle, je suis :

- Reconnu dans ce que je fais / pas assez reconnu par ma hiérarchie ? Satisfait de ma rémunération / mal payé ?
- Passionné par mon travail / ce que je fais m'ennuie ?

RISQUES & TECHNOLOGIES

Aujourd'hui, les appareils numériques contiennent non seulement des informations personnelles, mais aussi des informations professionnelles. Leur perte, leur saisie ou leur vol peut avoir des conséquences importantes. Voici quelques mesures simples à mettre en œuvre pour réduire les risques et les menaces, ou en limiter l'impact.

LE TELEPHONE PORTABLE

Le vol

Le vol de votre téléphone peut être purement crapuleux (revente de l'appareil, utilisation pour passer des communications sans être identifié…) ou à dessein pour récupérer certaines informations (agenda, journal d'appel, carnet d'adresses, emails…).

Les écoutes

Vous pouvez être écouté lorsque vous parlez à voix haute dans des lieux publics, mais votre téléphone peut également être utilisé comme dispositif-espion. Avec le matériel approprié, il suffit de quelques minutes pour copier l'intégralité des données ou installer des logiciels qui transmettront toutes vos données personnelles, vos déplacements, vos messages, vos appels, vos photographies, vos historiques de recherches Internet...

Même à distance, votre téléphone peut être l'objet d'attaques. Il existe des appareils qui se substituent aux antennes relais des opérateurs et permettent d'intercepter vos conversations ou toute information transitant par votre téléphone.

Enfin, sans même avoir accès à votre téléphone, et sans être à proximité, il est encore possible de recueillir de l'information grâce aux écoutes judiciaires / administratives, ou encore par l'analyse de vos factures détaillées, qui permet de reconstituer par recoupements et analyses des informations sur le microcosme d'un téléphone (réseaux, localisations, déplacements, communications, contacts, habitudes…).

LES DISQUES DURS EXTERNES ET LES CLES USB

Les disques durs externes ou les clés USB peuvent véhiculer à votre insu des virus ou des logiciels malveillants qui viendront récupérer des informations sur votre ordinateur, endommager son fonctionnement ou même permettre à une personne extérieure d'en prendre le contrôle. Il est fortement recommandé de préférer l'échange de fichiers par email.

Les informations échangées via ce type de support peuvent généralement être récupérées même après un effacement ou formatage rapide (via des logiciels de récupération de données). Il est donc conseillé de n'y déposer que des fichiers préalablement chiffrés ou de s'astreindre à formater en mode « bas niveau » le support après chaque utilisation.

A l'inverse, un moyen de stockage, comme une clé USB, peut être victime d'un l'ordinateur malveillant sur lequel il est connecté : copie du contenu du support à l'insu de l'utilisateur, installation d'un code malveillant visant à contaminer les prochains ordinateurs sur lesquels le support sera connecté... Des fichiers peuvent également être déposés à l'insu de l'utilisateur ayant vocation à porter atteinte à son image.

Nous recommandons de préférer des supports externes sous forme de disque dur avec chiffrement intégré (ex. le disque dur Globull).

L'ORDINATEUR PORTABLE

Même sans être physiquement connecté (câble réseau, clé USB…) votre ordinateur peut être la cible d'attaques via tous ses moyens de connectivité (Wifi, Bluetooth, infrarouge…) : nous vous recommandons donc de les désactiver par défaut.

Laissé sans surveillance, votre ordinateur peut être la cible d'actions malveillantes, par exemple une copie du disque, une pose de keyloggers (logiciel ou matériel permettant d'enregistrer et/ou de transmettre les frappes clavier), la modification de fichiers système pour récupérer des informations d'authentification... Pour parer à ce type de menaces, vous ne devez jamais vous séparer de votre ordinateur portable au cours d'une mission.

Par ailleurs, il est fortement conseillé d'installer systématiquement toutes les mises à jour de sécurité proposées (système, logiciel, antivirus) et de respecter scrupuleusement les consignes de sécurité édictées par votre RSSI.

Évitez également de connecter un appareil inconnu sur votre poste, car il existe un risque de contamination (cf. chapitre sur les moyens de stockage).

Dans la mesure du possible, minimisez l'information contenue sur votre ordinateur et faites en sorte que l'intégralité du disque soit chiffrée (système et données).

Enfin, mettez en veille (réactivation par mot de passe) votre ordinateur dès qu'il y a un risque qu'une personne puisse y accéder et n'installez que les logiciels nécessaires et dont l'origine est connue.

INTERNET ET LES EMAILS

Les cybercafés, les hôtels, les lieux publics et même les bureaux de passage n'offrent pas de garantie de confidentialité. Dans de nombreux pays, les centres d'affaires et réseaux téléphoniques sont surveillés et les chambres d'hôtel peuvent être fouillées ou équipées de matériels d'écoute.

Tout flux Internet doit impérativement passer par le VPN mis en place par votre entreprise. En cas d'indisponibilité, il est préférable d'utiliser une clef 3G/4G plutôt qu'un réseau inconnu.

Pour les courriels, n'ayez pas une confiance aveugle en fonction du nom de l'expéditeur : n'importe quel nom peut être remplacé dans l'en-tête d'un mail, et une adresse mail peut être usurpée… Méfiez-vous aussi des pièces jointes qui peuvent contenir de nombreux virus, parfois indétectables.

Évitez de répondre à une demande d'informations confidentielles par mail, car un compte mail peut être piraté pour en usurper l'adresse ou intercepter les messages.

Gardez en mémoire que l'on peut donner un nom à un lien hypertexte différent de l'adresse vers lequel il renvoie. Passez votre souris au-dessus des liens hypertextes : l'adresse réelle de destination s'affiche alors dans une bulle.

Faites attention aux caractères accentués dans le texte ainsi qu'à la qualité de la langue pratiquée par votre interlocuteur, ce qui permet d'identifier une grande partie des spams.

RISQUES & DÉPLACEMENTS

En raison du changement d'environnement et de la perte de repères qui y est généralement associée, les déplacements présentent un risque particulier. Cette partie ne traite pas des risques encourus « physiquement » par un voyageur, mais des déplacements vus sous l'angle du risque informationnel.

AVANT DE PARTIR

Comme nous l'avons vu précédemment, il est nécessaire de connaître ses besoins et ses désirs pour connaître ses limites et ses points faibles.

Relisez attentivement et respectez les règles de sécurité édictées par votre entreprise, vos référents et vos contacts. Prenez également connaissance de la législation de votrre lieu de déplacement, notamment en matière d'importation ou d'utilisation de systèmes de cryptographie. En effet, dans certains pays, l'utilisation d'équipements de cryptographie est limitée, voire interdite (Israël, États-Unis, Emirats-Arabes-Unis, …)

Le passage de la douane ou d'un contrôle de police est toujours délicat si vous transportez des documents sensibles. Préparez vos outils et limitez les informations qu'ils contiennent au strict minimum : ordinateur, téléphone portable, documents papier, informations sur d'autres domaines… Utilisez de préférence du matériel dédié aux missions, et ne contenant aucune autre information que celles dont vous avez besoin pour la mission, y compris les photos, vidéos ou œuvres numériques qui pourraient vous placer en difficulté vis-à-vis de la législation ou des mœurs du pays visité.

Sauvegardez les données que vous emportez, ainsi, en cas de perte, de vol ou de saisie de vos équipements, vous pourrez récupérer vos informations à votre retour.

Évitez de partir avec vos données sensibles : préférez la récupération de fichiers chiffrés sur votre lieu de mission en utilisant une liaison sécurisée (VPN par exemple) pour accéder au réseau de votre entreprise, une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées et en supprimant les informations de cette boîte après lecture.

En cas d'inspection ou de saisie par les autorités, perte ou vol, informez-en immédiatement votre RSSI.

EN VOYAGE ET PENDANT LES DÉPLACEMENTS

Emportez un filtre de confidentialité pour l'écran de votre ordinateur et de votre téléphone si vous êtes obligé de travailler pendant les trajets afin d'éviter les regards indiscrets par-dessus votre épaule. Placez un signe distinctif sur vos appareils et leurs housses. Cela vous permet de vous assurer qu'il n'y a pas eu d'échange.

Gardez vos appareils, supports et fichiers avec vous. Ne les laissez jamais sans surveillance, gardez-les en cabine pendant le trajet, ne les laissez ni au bureau ni dans une chambre d'hôtel. Souvenez-vous que vous n'êtes pas seul : la cohésion du groupe, vos collègues, votre famille sont vos meilleurs garde-fous.

N'utilisez pas les équipements qui vous sont offerts avant de les avoir fait vérifier par votre service de sécurité. Ils peuvent contenir des logiciels ou des équipements malveillants (systèmes d'écoute, enregistreurs…).

Au Bureau

Si des locaux sont mis à votre disposition, attention à ne pas les considérer comme un sanctuaire tel que pourrait l'être votre propre bureau en France :

- Respectez les mesures de sécurité informatique, notamment dans l'emploi d'Internet et des différents réseaux
- Attention à la gestion de vos documents papier
- Prenez conscience des personnels « invisibles » autour de vous (stagiaires, agents d'entretien, prestataires externes…)

A la maison/à l'hôtel

Les réflexes doivent être les mêmes qu'au bureau pour le téléphone, le net, les documents… mais pensez aussi aux objets de valeurs (ie : cartes diverses) et aux papiers personnels. Surveillez également le comportement des employés de maison qui peuvent être manipulés ou employés par des personnes malveillantes à votre égard.

Avant votre retour

Transférez vos données sur le réseau de votre entreprise par connexion sécurisée ou par messagerie dédiée puis effacez-les de vos appareils de façon sécurisée (videz les poubelles en mode sécurisé et réalisez des formatages niveau bas des supports externes). Effacez systématiquement vos historiques d'appels et de navigation.

Au retour de mission

Changez les mots de passe et faites analyser vos équipements. Ne connectez pas les appareils à votre réseau avant d'avoir fait au minimum un test antivirus.

POUR ALLER PLUS LOIN

ADAPTEZ VOTRE COMPORTEMENT

Souvenez-vous qu'aucune technologie ne peut pallier un mauvais comportement. Adopter un comportement adapté suppose de suivre un cheminement intellectuel qui part de la prise de conscience des enjeux et des menaces pour aboutir à l'appropriation des mesures de protection adaptées.
Pour vous accompagner d'avantage l'IRENCO propose des

actions de formations ciblées :

CONFERENCES DE SENSIBILISATION

SESSIONS DE FORMATION

Points clés :

Appréhender les points clés d'une démarche de sûreté de l'information
Vision globale de la sûreté de l'information,
Introduction aux méthodologies de sûreté de l'information

Évaluer son niveau de risque comportemental et celui de son équipe :
En fonction du contexte et dans la relation aux autres
Dans l'emploi des technologies de l'information

Se protéger contre les risques et menaces actives :
Connaître les processus possibles (méthodes de manipulation, déconflictualisation)
Connaître les outils utilisés

Adopter les réflexes adaptés :
Disposer de repères comportementaux
Identifier les tentatives d'intrusion
Savoir réagir vis-à-vis de ses partenaires et clients

Contact :

FORMATION@IRENCO.ORG

IRENCO
ACTIONABLE
KNOWLEDGE
DESIGNERS

IRENCO

ACTIONABLE
KNOWLEDGE
DESIGNERS

INSTITUT DE RECHERCHE
SUR LES ENVIRONNEMENTS COMPLEXES

156, rue du président Wilson
92300 Levallois-Perret (France)

hello@irenco.org

www.irenco.org