Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREFET DE L'EURE

I3E

Intelligence Économique, l'action de l'État dans l'Eure.

Lettre N° 9 – 2ème semestre 2016

FOCUS : PASSEPORT DE CONSEILS AUX VOYAGEURS

à télécharger à l'adresse suivante :

http://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

L'emploi de téléphones connectés (ou ordiphones/smartphones), d'ordinateurs portables et de tablettes facilite et accélère le transport et l'échange de données. Parmi les informations stockées sur ces supports, certaines peuvent présenter une sensibilité importante, tant pour nous-mêmes que pour l'administration ou l'entreprise à laquelle nous appartenons. Leur perte, leur saisie ou leur vol peut avoir des conséquences majeures sur nos activités et sur leur pérennité.

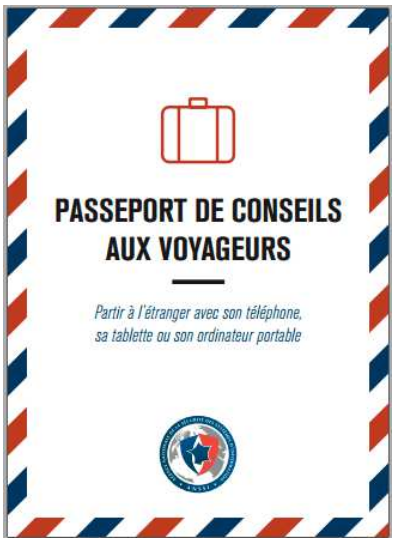
Il nous faut donc, dans ce contexte de nomadisme, les protéger face aux risques et aux menaces qui pèsent sur elles, tout particulièrement lors de nos déplacements à l'étranger. Des règles simples peuvent être mises en œuvre pour réduire les risques et les menaces, ou en limiter l'impact.

Des risques et des menaces supplémentaires pèsent sur la sécurité des informations que vous emportez ou que vous échangez, et notamment sur leur confidentialité.

Vos équipements et vos données peuvent attirer des convoitises de toute sorte : il faut rester vigilant, malgré le changement d'environnement et la perte de repères qu'ils peuvent provoquer.

Les cybercafés, les hôtels, les lieux publics et les bureaux de passage n'offrent aucune garantie de confidentialité. Dans de nombreux pays étrangers, quel que soit leur régime politique, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains cas, les chambres d'hôtel peuvent être fouillées sans que vous ne vous en rendiez compte.

Les conseils exposés dans le passeport de conseils aux voyageurs vous permettront de vous familiariser avec les menaces identifiées et de savoir quelles réponses apporter.



Ingérence économique (flash DGSI septembre 2016)

Certaines pratiques assurantielles peuvent induire des vulnérabilités en termes d'ingérence économique.
En cas de sinistre, les assurances, qu'elles soient facultatives ou obligatoires, contribuent à préserver la pérennité des entreprises. Au-delà de la protection des actifs corporels, la gestion des risques, indissociable du processus assurantiel, aide les entreprises à adapter leurs prises de décision dans un environnement incertain.
Dresser la cartographie des risques de l'entreprise assurée nécessite l'acquisition d'une connaissance fine de son *« business model »* et un diagnostic précis de ses vulnérabilités. Or, ces informations, utiles dans une démarche d'assurance et de gestion des risques, relèvent de la stratégie de l'entreprise.
En outre, face à l'émergence de risques nouveaux, certaines compagnies d'assurances n'hésitent pas, lors de la souscription, à effectuer des audits et à demander des informations très sensibles aux entreprises.
Ainsi, une vigilance particulière doit être portée au maintien de la confidentialité de ces informations, eu égard aux différents traitements dont elles pourraient faire l'objet.

Vous trouverez ci-dessous deux exemples représentatifs de scénarii de menaces :
Exemple 1 : Proposition d'externalisation de la gestion du risque entreprise. Une entreprise française en restructuration a récemment été démarchée, avec insistance, par un courtier en assurances qui proposait l'externalisation de la fonction gestion des risques, elle-même à la base de l'évaluation des besoins assurantiels de la société. Un engagement dans cette démarche aurait permis aux prestataires extérieurs d'avoir une connaissance approfondie de la société induisant, de fait, un risque de captation de ces informations stratégiques par des acteurs tiers.
Exemple 2 : Audits des réseaux informatiques lors de la souscription d'une «assurance-cyber». Victime de plusieurs tentatives de faux ordres de virements bancaires déjouées, une entreprise française s'est récemment intéressée aux assurances nouvellement proposées contre les cyberescroqueries. Elle constate cependant que sont exigés par les compagnies d'assurances, à l'appui de ces contrats, des audits poussés des réseaux informatiques des entreprises assurées. Ces dispositions inquiètent d'autant plus que les assureurs recommandent des audits effectués par des sociétés de services et d'équipements informatiques qui, pour beaucoup, sont étrangères à la France.
Si le recours aux assurances est indispensable pour la pérennité de l'entreprise, notamment face à la montée de risques émergents, il convient de s'assurer du respect de la confidentialité des échanges etdes données transmises.

Préconisations de la DGSI :
- Prévoir avec soin le périmètre des données qui seront transmises et éventuellement protéger celles-ci par une clé de chiffrement connue seulement de l'entreprise ;
- S'enquérir des éventuelles transmissions externes de ces données que le prestataire de services pourrait être amené à faire ;
- Signer, avec l'appui du service juridique, un accord de confidentialité précisant les modalités d'accès et de traitement des données, assorti d'un état nominatif - et évolutif - des personnes autorisées ;
- S'assurer des conditions de stockage et de sécurité des données transmises ;
- Lorsqu'un audit est nécessaire, recourir à un Prestataire d'audit de la sécurité des systèmes d'information (PASSI) qualifié par l'ANSSI ou, a minima, à un prestataire n'ayant aucun lien avec une activité de vente de matériels ou de services informatiques.

Informations utiles :

Le « **guide du routard de l'intelligence économique** ». est un outil pédagogique et concret qui enseigne comment mettre en œuvre et organiser sa veille stratégique, comment identifier et protéger les informations stratégiques et les savoir-faire.
Basé sur des cas concrets et des témoignages, ce guide illustre l'implication de l'Etat en faveur du développement de l'IE. Il est téléchargeable en ligne :
http://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/routard-guide-intelligence-economique.pdf
La lettre d'information de l'intelligence économique des ministères économiques et financiers (IE Bercy) est téléchargeable en ligne http://www.portail-ie.fr/article/1131/Publication-de-la-lettre-d-information-Bercy-IE-No40

Adresses utiles dans l'Eure :

Référent départemental IE : directeur de cabinet du préfet de l'Eure - 02.32.78.27.02
Référent sûreté gendarmerie nationale
MDL/Chef MEIGNEN Frédéric - Référent Sûreté Prévention technique de la malveillance et Vidéoprotection 02.32.29.57.27 - frederic.meignen@gendarmerie.interieur.gouv.fr
Référent sûreté police nationale - Capitaine Francis MONET - 02.32.39.90.02 – francis.monet@interieur.gouv.fr
*La gendarmerie et les services de police apportent leur expertise aux entreprises en matière de sécurité économique par le biais de « diagnostics de vulnérabilité ». **Ces diagnostics sont gratuits**.*
Référent IE DGSI drri76-ie@interieur.gouv.fr
Sur sollicitation, des intervenants experts se déplacent dans les entreprises. Ils évaluent les vulnérabilités des sites. Des solutions pragmatiques et adaptées sont proposées.

CCI Normandie, service innovation et IE : Florence FENIOU Coordinatrice régionale intelligence économique - florence.feniou@normandie.cci.fr, 02 35 88 38 41

CCI Portes de Normandie Département Industries et Services aux Entreprises, Fabien MENISSEZ, *Conseiller Innovation, Propriété industrielle et Intelligence économique.*
fabien.menissez@normandie.cci.fr – 02 32 38 81 53
L'INPI *propose des pré-diagnostics gratuits destinés à amener les entreprises à définir une stratégie de protection et, notamment de protection juridique, de leur patrimoine industriel.*
DIRECCTE NORMANDIE - Auréline CARPENTIER Déléguée à l'information stratégique et à la sécurité économiques Correspondante Direction Générale de l'Armement **aureline.carpentier@direccte.gouv.fr**

Réunions organisées dans l'Eure au titre de I3E :
Le 3 juillet et le 16 octobre 2012 ont eu lieu deux réunions d'information générale sur l'IE
Le 18 décembre 2012 - 3ème réunion IE sur le thème de la maîtrise de l'information et de la protection des données informatiques.
Le 03 juin 2013 - 4ème réunion IE dans l'Eure sur le thème de la veille sur internet
Le 30 septembre 2013 - 5ème réunion sur la protection des savoir faire
Le 10 février 2014 6ème rencontre sur les relations partenariales
Le 05 mai 2014 - 7ème rencontre « finance et gouvernance »
Le 03 novembre 2014 - 8ème rencontre « escroqueries aux virements internationaux
Le 1ER juin 2015 – 9ème réunion sur la sécurité des systèmes d'information et protection des données
Le 2 novembre 2015 – 10ème réunion sur la communication en situation de crise (comment protéger votre entreprise d'une crise médiatique)