7ème FRC - Des réponses concrètes

2009

2010

2011

2012

2013

2014

FORUM DU RHIN SUPERIEUR sur les CYBERMENACES

7ème édition FRC 2014

Le 4 Novembre 2014

à l'ENA - Strasbourg

Accès libre WiFi ?

Free Wi-Fi

Cloud ou non ?

Escroqueries, extorsions

Des réponses concrètes !

La cible : l'entreprise !

LA REGION DE GENDARMERIE D'ALSACE
LES OFFICIERS DE LA RESERVE CITOYENNE
ET LE RESEAU CYBERDEFENSE

7ème Forum du Rhin supérieur sur les Cybermenaces

Général Thierry Thomas

Commandant la Région de Gendarmerie Alsace
Commandant le Groupement du Bas Rhin

7ème Forum du Rhin supérieur sur les Cybermenaces

Jean Louis Hoerlé
Président de la CCI de la région Alsace

7ème Forum du Rhin supérieur sur les Cybermenaces

M. Stéphane BOUILLON
Préfet de la Région Alsace
Préfet du Bas - Rhin

FRC 2014 : Des réponses concrètes !

Les réponses concrètes à apporter aux PME PMI

par le général d'armée (2s)
Marc WATIN-AUGOUARD
Anc. inspecteur général des armées – gendarmerie
Directeur du Centre de recherche de l'école des officiers de la gendarmerie nationale

FRC 2014 : Des réponses concrètes !

Tables rondes

Le Cloud

Les Rançongiciels

Le Wifi

Animation par Gilbert Gozlan

Directeur Opérationnel Sûreté
Réseau La Poste Nord & Est
Chef d'escadron (RC) de la gendarmerie nationale

Cloud computing : Les entreprises s'engagent

M. Ludovic Haye

Responsable production SAP
PSA Peugeot Citröen
Chef d'escadron (RC) de la gendarmerie nationale

M. Daniel Guinier

Docteur ès Sciences
Expert judiciaire auprès de la Cour Pénale Internationale de la Haye
Colonel (RC) de la gendarmerie nationale

Mme. Delphine Roger

Expert comptable, commissaire aux comptes
Directrice du Système d'information, Cabinet FCN

Cloud computing : Les entreprises s'engagent

Cloud computing : phénomène, contours et maîtrise

par M. Ludovic HAYE

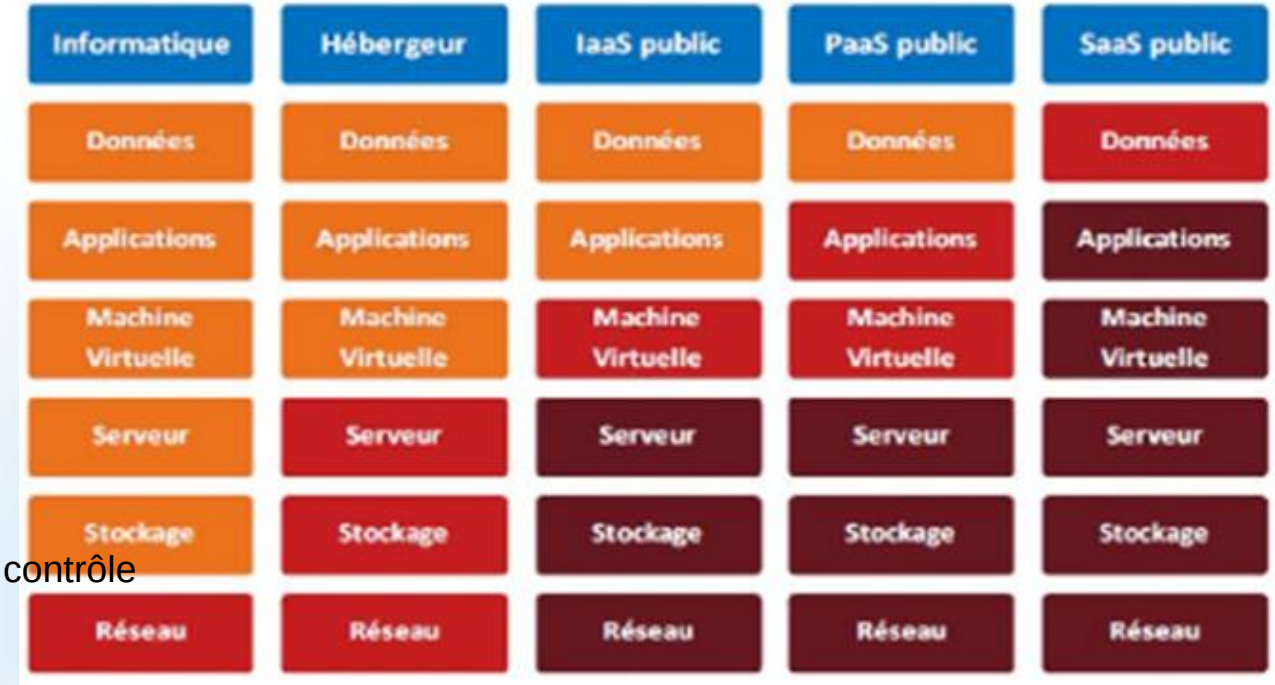
Responsable production SAP
PSA Peugeot Citröen
Chef d'escadron (RC) de la gendarmerie nationale

Le phénomène "cloud"

- Buzzword
- Enjeu économique en période de crise
- Explosion des nouvelles technologies
- Bien-être des salariés
- Société en pleine mutation
- Besoins d’interactivité et de réactivité

Les contours du cloud

- Les types de services : SaaS, PaaS, IaaS, DaaS, etc.
- Les modes de déploiement : public, privé, hybride, souverain ou non ...
- Les avantages/inconvénients



Source : AFDEL

Le cloud en quelques chiffres

- 66 % des personnes sondées pensent que c'est risqué
- 32 % ont l'intention de s'engager …

mais

- 50 % confient des données sensibles,
- 39 % sont peu sensibles à la sécurité des données
- 50 % chiffrent au préalable leurs données …

… tandis que 22 % des américains sondés pensent que le cloud computing est un vrai nuage …

Orientation vers un cloud maîtrisé

- Précautions indispensables pour les entreprises
- Politiques : personnel, incubateur, etc.
- Techniques : couverture, tri des données, dépendance, sécurité, etc.
- Prendre en compte l'échange et le partage des fichiers pour les PME / PMI

Conclusion

Cloud computing : Les entreprises s'engagent

Conséquences et risques pour les entreprises

par M. Daniel GUINIER

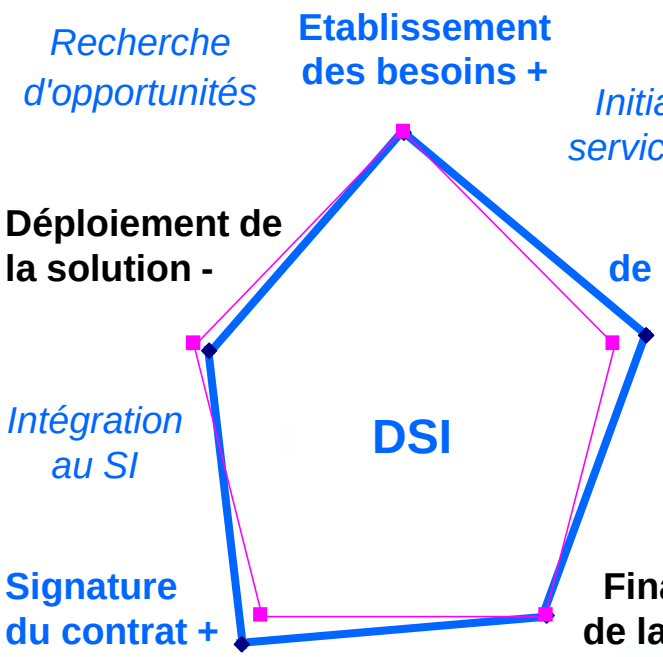
Docteur ès Sciences, certifications CISSP, ISSMP, ISSAP, MBCI
Expert en cybercriminalité près de la cour pénale internationale de La Haye
Colonel (RC) de la gendarmerie nationale

Conséquences du cloud sur les métiers

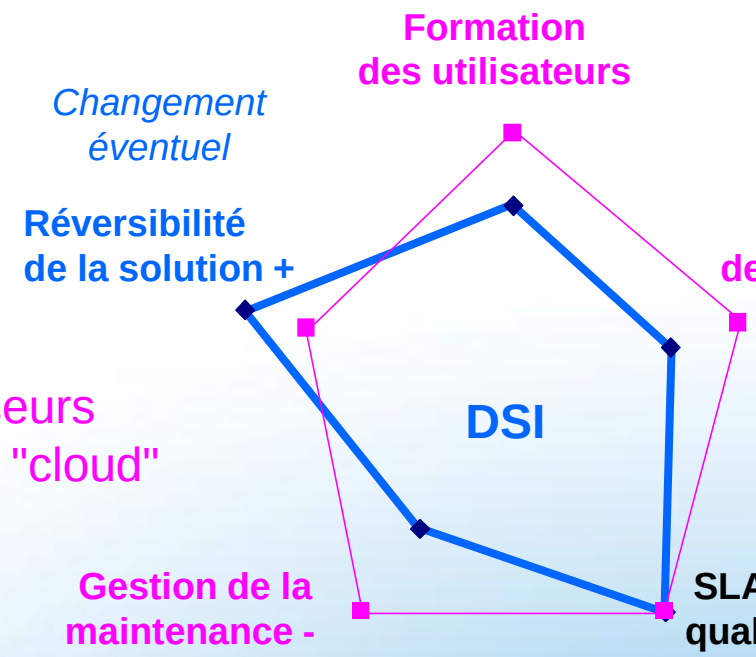
- **Les directions métiers** : Services centrés sur la demande
  - ++ Solutions standards et intégration dans le SI de l'entreprise
  - \+ Service désiré par les utilisateurs *"comme chez eux…"*
  - - - Solutions spécifiques, spécifications des besoins utilisateurs
- **La DSI** : Compétences orientées vers le management
  - ++ Pilotage de contrats, architecture et urbanisation
  - \+ Expertise en "cloud", gestion de projets et aide à MOA
  - - - Compétences informatiques : développement, architectures

La DSI est garante de la cohérence globale du SI, de la qualité et de la sécurité, avec le RSSI. Il ne faut pas négliger les risques de résistance au changement et de contournent de la DSI par des initiatives hasardeuses.

La DSI devient un partenaire ...aaS



Fournisseurs de services "cloud"



En amont

En aval

La DSI, dont la maturité est attendue, évolue au cœur de la relation métiers-DSI-fournisseurs de services "cloud", en intervenant de façon croissante et prédominante à différentes étapes.

Risques forts et contraintes standards

Non spécifiques 31%

Défaut de maîtrise de gestion réseau : mauvaise connexion, congestion, etc.
Vol ou perte de sauvegardes

Contraintes : Maintenance, PRA, Accès
Sécurité CDI-T, Habilitations

Contraintes : Interopérabilité, Supervision,
Sécurité CDI-T

Juridiques 14%

Localisation à l'étranger
Défaut de conformité

Protection des données insuffisante
Décision de justice & faillite FC

Contraintes : Garanties légales, Contrats,
Déclarations réglementaires

Contraintes : Disponibilité services et données,
SLA, Portabilité, Réversibilité

Analyse des risques pour l'entreprise

- **Données**
  Stockées et transférées, Vitales, sensibles, métiers, Clés de chiffrement, …
- **Infrastructures**
  FC et sous-traitance, Vitales, …
- **Traitements**
  Applications, Virtualisation, Licences, Sauvegardes, …
- **Humains**
  Comportements, Usages dont BYOD, …

Défaut d'isolation ou de compartimentation
Effacement de données non sûr
Compromission de gestion d'interfaces
Prise de privilèges, intrusion interne au FC

Techniques 36%

Verrouillage par FC - Irréversibilité

Perte de gouvernance

Organisationnels et politiques 19%

L'essentiel dans ce projet d'entreprise

Démarche pratique

- Impliquer au plus tôt les directions générale, SI et métiers
- Analyser les besoins …aaS et les risques de l'entreprise
- Comparer les offres et les clauses contractuelles
- Choisir le prestataire (FC) après inspection des garanties
- Planifier le changement en impliquant les personnels

Outils *non exhaustifs et autres publications CIGREF, IFACI, ENISA, etc.*

- ANSSI : Méthode et guides : analyse des risques EBIOS, hygiène externatisation, virtualisation, qualification des FC, etc.
- CNIL : Recommandations et modèles de clauses contractuelles

Cloud computing : Les entreprises s'engagent

Présentation d'un cas de déploiement opérationnel de "cloud" en mode privé

par Mme. Delphine ROGER

Expert comptable, commissaire aux comptes
Directrice de l'organisation du système d'information, Cabinet FCN

FCN vers le cloud computing

1985 — AS400 centralisé avec des terminaux passifs

1999 — Réseaux Ethernet
Serveurs d'agences hébergeant bureautique et messagerie Exchange centralisés et serveurs locaux en bureautique

2004 — Centralisation d'applicatifs métiers par CITRIX et bureautique

2013 — Data center Tier IV et un contrat d'infogérance – Un cloud Hybride

Gestion interne à FCN

- Interne privé
- Externe privé appelé CLOUD PRIVE
- Interne ouvert
- Externe ouvert appelé CLOUD OUVERT

Usage dédié aux besoins propres à FCN

Nos Clients
Les Administrations
Nos Agences
Nos Partenaires
Nos Institutions Professionnelles

FCN EXPERTISE AUDIT CONSEIL

Quel modèle de services ?

IaaS : le cloud d'infrastructure
PaaS : le cloud de plateforme
SaaS : le cloud d'application

Les apports pour FCN et ses clients

Une nouvelle vision de la production

Les atouts en matière d'organisation et de production

Flexibilité

Mobilité

Simplification du parc informatique

Respect de l'environnement

Accès à des services

Utilisation souple des services

Optimisation de la gestion des ressources humaines

Hébergement des données

Innovation et compétitivité

Mises à jour des logiciels

Collaboratif interne et externe

BYOD (Bring Your Own Device)

Externalisation pour se décharger des problèmes de sécurité et de disponibilité

De nouveaux services internes et externes

Un intérêt financier

- **Une messagerie accessible**
- **Du stockage en ligne**
- **Une plateforme collaborative**
- **Un web participatif**
- **Une Ged**
- **Une prise en charge de la comptabilité des petites structures**
- **Des offres d'outils client en mode Web**

Une volonté, un choix,
La mise en place avec des contraintes à respecter

S'assurer de l'indépendance, de la liberté et de l'autonomie de FCN vis-à-vis de notre principal prestataire (OCI)

La sécurité : quatre aspects principaux

- La confidentialité des données – Le cryptage
- La disponibilité des données et la résilience
- La sauvegarde des données par OCI
- La sécurité d'accès au service – L'authentification – la protection des données

La législation

- Localisation des données
  - Enjeu de la souveraineté des données – Datacenter Tier IV
  - Enjeu juridique de la localisation des données en UE ou pays avec qui la France a un accord de coopération fiscale.
  - Territorialité des litiges : tribunaux français et droit français
  - Information par le prestataire de la sous traitance et clause de porte fort
- Les autres obligations juridiques

Notre contrat de prestation

- Un partenariat avec OCI dans ce projet
- Analyse et définition des besoins internes et externes avec l'accompagnement d'un consultant en organisation
- Externalisation de la maîtrise d'œuvre de la fonction informatique
  - Hébergement dans le Data Center de Strasbourg TIER IV
  - Une ligne de secours externe à notre réseau central
  - Mise en place d'un contrat d'infogérance pour une qualité de service optimale

L'enjeu pour FCN : trouver l'équilibre entre l'identification des besoins et le niveau de service nécessaire pour un SI dans un cloud, au service de la performance de FCN et de ses clients dans un environnement complexe.

Cloud computing : Les entreprises s'engagent

Questions

Délinquance astucieuse et nouvelles technologies
Faux ordres de virements et rançongiciels

Maitre Cécile Doutriaux

Avocate au barreau de Strasbourg
Auditeur IHEDN
Membre de la chaire Cyberdéfense et Cybersécurité des écoles de St Cyr Coëtquidan
Chef d'escadron (RC) de la gendarmerie nationale

Colonel Hubert Charvet

Commandant de la section de recherche de Strasbourg
Ancien commandant de groupement du 67
Colonel de la gendarmerie nationale

M. Bernard Barbier

Conseiller Cybersécurité et cyberdéfense SOGETI
Diplômé de l'École Centrale de Paris
Ancien Directeur technique de la DGSE

CYBERCRIMINALITÉ : FOVI & RANÇONGICIELS

- 10 millions de cybervictimes en France en 2013
- pour un préjudice financier de 736 millions d'euros
- Les sociétés victimes ont leur siège social dans des zones économiques à forte activité ou dans des zones frontalières
- Des infractions qui touchent les entreprises de toute taille et de tout secteur d'activité

Des infractions qui ne sont pas nouvelles, mais une problématique toujours d'actualité !

ESCROQUERIE Un logiciel qui pirate les fichiers

Des entrepreneurs rançonnés

Deux entreprises basées à Bischheim et à Strasbourg ont été victimes d'escrocs, qui sont parvenus à pirater leurs fichiers par le biais d'un mail. Leurs représentants ont déposé plainte auprès de la police.

L'ESCROQUERIE est déjà connue au niveau national sous le nom de CryptoWall. Il semble qu'elle touche depuis peu le département du Bas-Rhin. Deux entreprises de la communauté urbaine de Strasbourg en ont fait les frais. En effet, un matin ils ont découvert qu'ils n'avaient plus accès à aucun de leurs fichiers texte. Un mail les informe qu'ils viennent « d'être cryptés par un virus. » « Ça veut dire que la structure et les données de vos fichiers ont été irrévocablement modifiées. Vous ne pourrez pas travailler avec eux ou les lire. Vous les avez perdus pour toujours, mais avec notre aide vous pouvez les restaurer », précisent les escrocs. Les cyberpirates demandent en contrepartie le paiement de 750 euros pour obtenir une clé de déchiffrement.

« Ne jamais payer »

L'arnaque venant des pays de l'Est peut cependant être évitée. Pour ce faire, la police conseille de ne jamais ouvrir de fichier en provenance d'un mail inconnu ou alors de vérifier au préalable les propriétés du fichier joint. Si jamais le document se termine par «.exe », cela signifie qu'un « exécutable se lance » dès que la victime double-clique sur le lien. « Dans ce cas, le premier réflexe à avoir, c'est de sortir la prise réseau » pour contrecarrer une attaque « de l'ensemble du réseau », confie le commissaire Patrick Roussel, chef de la sûreté départementale de Strasbourg. « Il faut ensuite passer son antivirus. »

« Il est également possible de configurer sa boîte mail pour qu'elle affiche les extensions cachées. Sinon, il convient d'effectuer des sauvegardes sur un disque externe », préconise la police.

Et si jamais votre ordinateur a été infecté, « ne jamais payer et faire appel à une société informatique », avertit le commissaire Roussel. ■

CÉL. L.

DNA 11 Juillet 2014

SUD OUEST

22/01/2014 Escroquerie : Géant Vert a été la cible de l'une des plus grosses escroqueries aux faux ordres de virements internationaux. La JIRS de Bordeaux enquête depuis la mi-décembre sur une escroquerie aux virements bancaires ayant atteint en quatre jours la somme de 17 millions d'euros.

650 000 données contre une rançon de 30 000 euros

L'affaire remonte au 9 juin 2014. Profitant d'une faille informatique sur les serveurs de Domino's Pizza, le groupe de hackers Rex Mundi parvient à dérober les données personnelles de quelque 650 000 clients. Rex Mundi demandait 30 000 euros à Domino's Pizza pour ne pas diffuser ces données, assorti d'un ultimatum fixé au 16 juin à 20 heures. La société Domino's Pizza a refusé de payer quoi que ce soit.

LA TRIBUNE Acteurs de l'économie 26/06/2014,

7,6 millions d'euros : c'est le montant de l'escroquerie record dont KPMG SA a été victime en 2012. Cette fraude, dite « au Président », résulte de méthodes et d'outils technologiques extrêmement sophistiqués. Elle engage aussi une chaine de responsabilités, qui interroge le contrôle interne d'un groupe lui-même chargé de le mettre en œuvre chez ses clients.

MODES OPÉRATOIRES : FOVI

- Le FOVI « simple » : L'escroc reproduit la signature d'une personne ayant la signature bancaire sur les ordres de virement qu'il adresse à la banque (usurpation d'identité, faux en écriture, usage d'une fausse qualité) pour bénéficier d'un virement de fonds direct.

- Le FOVI « client-fournisseur» : substitution par mail, courrier, fax, faux site fournisseur avec désignation d'un faux bénéficiaire.

- Le FOVI « au président » : OPA, marché urgent, contrôle fiscal, L'escroc usurpe l'identité d'un donneur d'ordre et s'adresse au service comptable, à la trésorerie de l'entreprise en prétextant l'urgence et la confidentialité. Les ordres de virement sont signés par une personne disposant effectivement de la signature sur le compte, mais sur les instructions reçues du « faux patron » et les fonds sont ensuite transmis à la banque par le salarié.

- Recours à l'ingénierie informatique : maîtrise des interfaces de paiement banque-société, mise en confiance et récupération des codes comptables réciproques, édition de faux certificats électroniques /Simulation de pannes techniques (ex : mise à niveau EBICS → SEPA)

SYSTÈMES CRIMINELS : DÉLINQUANCE ASTUCIEUSE

Donneurs d'ordres

Bandit

Transfert

Ingénierie sociale

Analyse et renseignement

Maîtrise et culture entre-preneuriale

Scénario

Exécution de l'escroquerie

1 - Structures soc. et fin.

2 - Usurpation de qualité

3 - Furtivité numérique

Contraints

Abusés

Victimes tiers

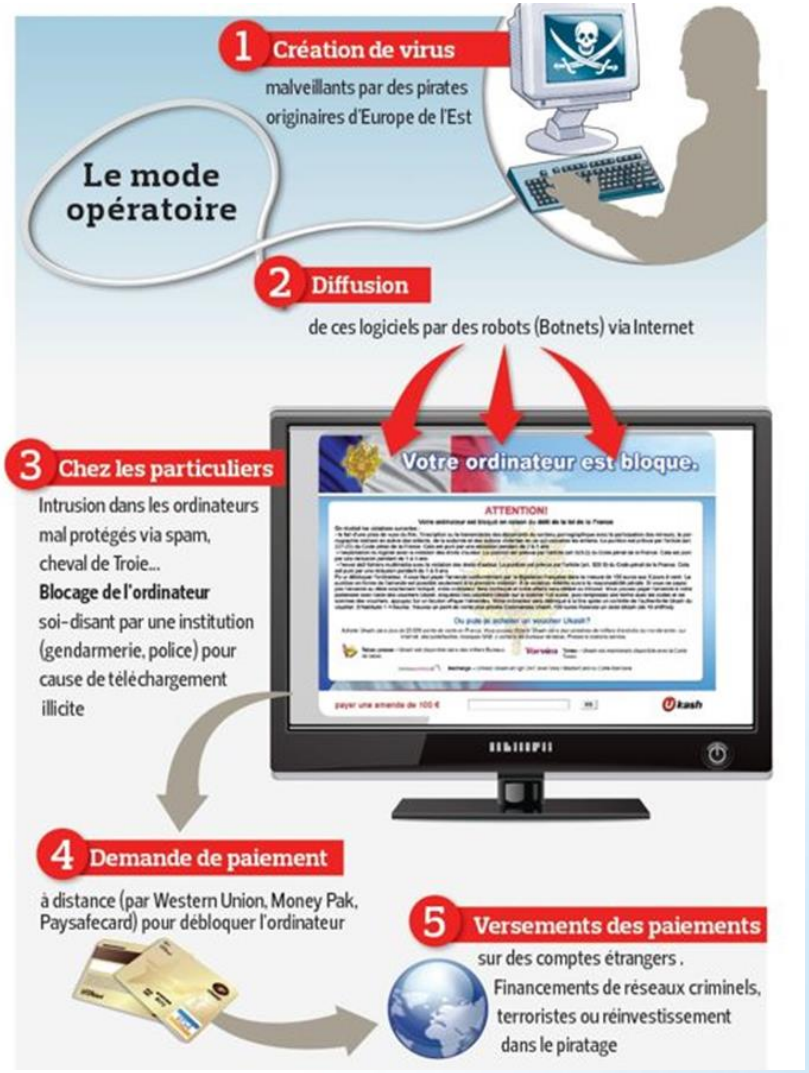
Escrocs

Maîtrise

Société victime

Transfert

MODES OPÉRATOIRES : RANÇONGICIELS



- Une contamination du poste à l'insu du propriétaire (clé usb, courriels avec PJ, liens vers des sites malveillants, faux antivirus)
- L'ouverture d'une fenêtre avec un message exigeant le paiement d'une somme élevée.
- En contrepartie du paiement, les délinquants indiquent qu'ils enverront la clé de chiffrement permettant de récupérer et de restaurer les données et fichiers compromis.

FOVI et RANÇONGICIELS : RÉAGIR VITE !

Ne jamais payer la rançon réclamée et ne pas cliquer sur des liens de sources inconnues/céder à la flatterie ou à l'intimidation pour procéder aux virements de fonds.

Dès la découverte de la fraude :

Informer sa banque et lui demander de contacter son homologue à l'étranger (coopération interbancaire) pour bloquer une partie des fonds envoyés et obtenir la réexpédition des fonds transférés.

Demander à sa banque de procéder immédiatement à une déclaration de soupçon auprès de TRACFIN (blocage des fonds transférés au plan international).

Gérer les répercussions de l'escroquerie ou de l'extorsion de fonds en terme de communication auprès de ses clients, fournisseurs, partenaires économiques et financiers.

Déposer plainte auprès des services de gendarmerie et se constituer partie civile.

FOVI et RANÇONGICIELS : PHASE D'URGENCE ET ENQUÊTE

Procédure commerciale par les banques (déclaration de soupçon / cellule anti-fraude des banques émettrice et destinatrice (réseau ASI) : blocage des fonds / demande d'annulation du virement)

Procédure judiciaire : parquet local / JIRS (JLD : blocage des fonds demande d'entraide pénale internationale)

Constatations : société cible / outils d'information publics et privés / FAI, registrars, … : importance du volet numérique et du caractère international !

Investigations : entraide pénale internationale / ECE-JIT

Recoupements : analyse criminelle / STRJD / coopération bilatérale / Europol et Interpol …

FOVI et RANÇONGICIELS : ACTIONS JUDICIAIRES

L'Escroquerie - Article 313-1 Code Pénal :
est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'emploi de manœuvres frauduleuses, de tromper une personne et de la déterminer à remettre des fonds
punie de 5 ans d'emprisonnement et de 375 000 € d'amende

L'Extorsion - Article 312-1 Code Pénal :
est le fait d'obtenir par violence, menace de violences ou contrainte la remise de fonds, de valeurs ou d'un bien quelconque
punie de 7 ans d'emprisonnement et de 100 000 € d'amende

La tentative est réprimée
Peines aggravées pour les infractions commises en bandes organisées :
- 20 ans de réclusion criminelle et de 150 000 euros d'amende (Extorsion)

10 ans d'emprisonnement et à 1 000 000 euros d'amende (Escroquerie)

Mais d'autres infractions sont aussi concernées
chantage, abus de confiance, faux et usage de faux, intrusion informatique, usurpation informatique, usurpation d'identité numérique …

FOVI ET RANÇONGICIELS : QUELLES INDEMNISATIONS ?

- L'évaluation du préjudice
  (montant des fonds détournés , désorganisation de l'entreprise, perte d'exploitation et atteinte à l'image)
- Les fonds d'indemnisation (CIVI, SARVI)
- Quelle possible prise en charge par les assurances ?

FOVI et RANÇONGICIELS : RECOMMANDATIONS

Se méfier des **demandes effectuées** la veille de week-end, de jours féries, de vacances, à des horaires particuliers (tôt le matin, à l'heure du déjeuner, tard)

- En **période de sous-effectif** / présence d'intérimaires : congés maternité ou maladie

- Des **destinations de fonds inhabituelles** vers l'étranger par rapport aux zones d'activités connues de l'entreprise

- Des **modalités de virement** manuels par télécopie, en dérogation avec les procédures d'authentification de l'entreprise et les process électroniques mis en place avec la banque

conserver la confidentialité des signatures manuscrites des dirigeants autorisés à valider des opérations

Limiter la diffusion des informations sensibles de l'entreprise sur les sites **Internet** et recommander aux collaborateurs de ne pas diffuser d'informations sur **les réseaux sociaux** professionnels et personnels

FOVI et RANÇONGICIELS : LA PRÉVENTION

Sécuriser ses systèmes d'information, chiffrer ses données finançières et effectuer régulièrement des sauvegardes externes

Définir des **processus clairs** et **formalisés et** Réaliser des **contrôles réguliers** Sécuriser l'accès aux **applications** et **données sensibles** et Limiter les droits des utilisateurs au strict nécessaire. Mettre en place des dispositifs d'authentification.

Mettre en place une **ségrégation des rôles** : Dissocier saisie et validation des ordres (virements, déclarations de BIC/IBAN).

Limiter les virements papier ou fax qui sont plus faciles à contrefaire que les autres moyens de paiement et Privilégier les **canaux automatisés** comme Ebics, SWIFTNet...et Respecter les **consignes de sécurité** afférentes à ces outils : clé e-secure, droits des utilisateurs...

Communiquer à sa banque les **contacts à joindre en cas de doute** sur des opérations bancaires.

Un préjudice majeur pour l'industrie

La cyber-criminalité coûterait 327 milliards d'euros par an

LE CHIFFRE DU JOUR

Géographiquement, la facture pèse surtout sur les grandes puissances économiques : le coût pour les Etats-Unis, la Chine, le Japon et l'Allemagne atteint un total de 200 milliards de dollars (près de 150 milliards d'euros).

latribune.fr | 09/06/2014, 17:21 - 231 mots

Selon un rapport publié lundi par le Center for Strategic and International Studies (CSIS), la cyber-criminalité coûterait environ 445 milliards de dollars par an (327 milliards d'euros) par an à l'économie mondiale en termes de croissance, d'innovation et de compétitivité.

Un nouveau fléau pour l'économie mondiale? Pour Jim Lewis, membre du CSIS *"la cyber-criminalité est un impôt sur l'innovation; elle ralentit le rythme de l'innovation dans le monde en réduisant la rémunération des innovateurs et des inventeurs".*

Les grandes puissances sont les plus touchées

The financial institutions are attacked

Cybersecurity firm says large hedge fund attacked

Eamon Javers | @EamonJavers
Thursday, 19 Jun 2014 | 9:05 AM ET

CNBC

Unprecedented cyberattack stopped
Thursday, 19 June 2014 | 3:05 null | 2:16
Earlier this year hackers penetrated a large hedge fund and sought to steal data and block the hedge fund's trading abilities, reports CNBC's Eamon Javers.

Cyberattacks against major corporations such as **Target** and Neiman Marcus have dominated the news in recent months, but in those cases attackers have typically sought relatively easy-to-exploit data such as credit card numbers.

In the new case, attackers went after the hedge fund's trade order entry system, seeking to disrupt the fund's trading strategy and to send details of the trades themselves outside the firm.

The financial institutions are attacked

Les données personnelles de 76 millions de ménages compromises lors d'une cyber-attaque contre JP Morgan

La banque reconnaît avoir été victime d'une attaque informatique de grande ampleur cet été. 7 millions de PME et 75 millions de ménage auraient été touchés.

01net avec AFP | 01net | le 03/10/14 à 08h19 | laisser un avis

J'aime 5 Recommander 5 Tweeter 65 +1 2

La banque américaine JPMorgan Chase a révélé pour la première fois ce jeudi l'ampleur de l'attaque informatique dont elle a été victime pendant l'été, faisant état de 76 millions de ménages et de 7 millions de PME touchés. Les hackers ont eu accès aux nom, adresse,

Les arnaques au président: préjudice de plusieurs centaines de millions d'euros, cachées par les entreprise victimes

KPMG : Les dessous d'une escroquerie de 7,6 millions d'euros

Crédns : DR (Crédits : DR)

Denis Lafay | 26/06/2014, 7:25 - 1696 mots

7,6 millions d'euros : c'est le montant de l'escroquerie record dont KPMG SA a été victime en 2012. Cette fraude, dite « au Président », résulte de méthodes et d'outils technologiques extrêmement sophistiqués. Elle engage aussi une chaine de responsabilités, qui interroge le contrôle interne d'un groupe lui-même chargé de le mettre en œuvre chez ses clients. Récit d'une incroyable arnaque.

L'affaire démarre en mai 2012. B.M*, comptable à la direction Rhône-Alpes de KPMG en charge des règlements fournisseurs, reçoit un appel téléphonique d'un interlocuteur se présentant sous l'identité de Jean-Luc Decornoy, le président du directoire de KPMG SA (http://acteursdeleconomie.latribune.fr/finance-droit/finance/2014-06-27/kpmg-jean-luc-decornoy-resident-suisse.html). Il la somme, sous le sceau de l'absolue confidentialité et après s'être inquiété de quelques soucis personnels qu'elle avait... réellement éprouvés - la mettant ainsi en confiance -, de procéder à un virement de 252 848 € nécessaire à l'accomplissement d'une étude de consulting *« qui doit demeurer totalement secrète »*. Elle insiste sur le caractère inapproprié de la demande, mais devant la persistance de son « grand patron » doit céder.

Une adresse IP aux Etats-Unis

Le bureau parisien du cabinet d'avocats Baker & McKenzie victime de l'escroquerie "au président"

INFO RTL - Baker & McKenzie a été la cible d'escrocs spécialisés dans les faux ordres de virements internationaux.

La page de l'émission : RTL Matin

PAR GEORGES BRENIER PUBLIÉ LE 17/09/2014 À 07:29 MIS À JOUR LE 17/09/2014 À 08:01

Le plus grand cabinet d'avocats d'affaires victime d'une énorme escroquerie. La semaine dernière, le bureau parisien de **Baker & McKenzie**, où la présidente du FMI Christine Lagarde a travaillé pendant près de 18 ans, a été **la cible d'escrocs spécialistes dans les faux ordres de virements internationaux.**

Les suspects ont réussi à obtenir quatre virements bancaires pour un préjudice total de plus de 900.000 euros. D'après les premiers éléments de l'enquête, **l'argent a été viré vers des comptes bancaires basés en Chine.** La Direction centrale de la police judiciaire est en charge de l'affaire.

Une arnaque très efficace

La technique utilisée n'est pas nouvelle. **Il s'agit de l'escroquerie "au président".** Une arnaque hors norme qui a déjà dupé de nombreuses entreprises françaises. Après un travail de longue haleine consistant à s'imprégner du vocabulaire propre à l'entreprise et à **collecter une kyrielle d'informations sur son environnement**, les escrocs appellent un salarié, souvent au sein du service comptable de l'entreprise.

Ils se font alors passer pour le président-directeur général et expliquent, avec le ton et les mots propres au patron, qu'il faut **effectuer rapidement un virement sur un compte secret et protégé.** Puis ils demandent à leur employé d'agir en toute discrétion et de ne surtout pas ébruiter la transaction.

Les arnaques au président: les escrocs utilisent le cyber espionnage pour identifier les failles

- Ces arnaques reposent de plus en plus sur du cyber espionnage
- Connaissance des processus de mise en paiement des factures
- Connaissance des personnes ayant les délégations (réseaux sociaux)
- Usurpation d'identité du président, des décideurs
- Faux email
- Faiblesse des processus automatisés par les ERP et mal contrôlés

Les principes d'une attaque

Le principe de base est d'introduire un MALWARE dans l'ordinateur de la cible. Un MALWARE est un logiciel qui va utiliser une faille du système pour prendre le contrôle de l'ordinateur (la faille est une vulnérabilité appelée 0 day car inconnue de l'éditeur de logiciel, qui permet d'augmenter les privilèges d'un processus)

Pour « injecter » le MALWARE, il faut « contourner » les protections: antivirus, firewall..le plus simple est le Phishing: mail piégé qui contient un lien vers un site « pirate »

Le MALWARE est « piloté » à distance par des serveurs de contrôle commande. Le MALWARE peut être très complexe, il peut s'auto propager de PC en PC, prendre le contrôle du clavier, de la caméra, aller chercher des données sensibles, casser (STUXNET)

La partie « injection » peut être très complexe, exemple QUANTUM ATTACK de la NSA

Les principes d'une attaque par cassage du mot de passe

Utilise la faiblesse des mots de passe.

Le mot de passe est conservé chiffré, on le déchiffre (décrypte) en utilisant des méthodes de forces brutes et des dictionnaires; (les hackers piratent des milliers de serveurs pour créer virtuellement un super calculateur qui sert à casser les mots de passe)

Le mot de passe chiffré peut être récupéré sur un site, par écoute, par un malware

Utilisation des mêmes mots de passe pour le travail et la vie privée, très grande vulnérabilité car on utilise le même (presque) mot de passe

L'Idéal: des mots de passe de **12 caractères avec le maximum d'éléments différents**: lettre, chiffre, caractères spéciaux, pas de nom propre….et utiliser un mot de passe différent par site…..

Les Écoutes des Smartphones

Méthodes passives: écoutes de proximité, complexes et couteuses (casser en temps réel la crypto GSM), faisable par les Etats, officines (plus de 1M€)
Non détectable

Méthodes actives à distance: IMSI CATCHER (fausse BTS). Localisation, écoutes, injection de MALWARE, par les états et les officines (300K€)
Détectable par l'opérateur mais l'opérateur s'en fiche….

Par attaque informatique: injection dans le téléphone, ou utilisation d'APPS contaminées (fausses APPS, attention aux jeux….)
Détectable par l'utilisateur, attention à garder toujours la maitrise de son téléphone.

Les données contenues dans le Smartphone sont en danger….keylogger qui capture vos numéros de compte bancaire…vos mots de passe…

Les Entreprises

Pour les entreprises, les administrations, les organismes publics, l'enjeu de la cyber sécurité impose une vraie transformation

La mise en place d'un programme volontariste de cyber défense doit être conduit au plus haut niveau de l'entreprise dans une volonté de transformation de l'entreprise.

La numérisation des entreprises, l'évolution vers le CLOUD COMPUTING, la mobilité, le BIG DATA, sont en danger face à la cyber insécurité.

Cette transformation (révolution) de l'entreprise vers le tout numérique oblige l'entreprise à se transformer dans son approche Sécurité Informatique.

La SSI classique, orientée procédure, muraille, moyens, statique, doit se transformer totalement vers une cyber défense dynamique, réactive, intégrée dans la culture de l'entreprise.

Les Entreprises

.

LA SURVEILLANCE DU SI: impossible de bloquer toutes les attaques, il faut détecter et réagir immédiatement, et remédier. **L'importance du SOC:** surveillance 24/24 de la sécurité du SI.

Les outils modernes d'analyses: SIEM, big data analysis

L'homme clé de l'entreprise : le DATA SCIENTIST, le monsieur BI de la sécurité

Les attaquants s'échangent de l'information, pourquoi pas les entreprises

Il faut faciliter les échanges État-Entreprise (casser le mythe du secret)

Les Entreprises, l'approche par la protection des données

- Mettre en place une politique donnée: classement, protection, sauvegarde, sécurité
- Protéger les données vraiment critiques
- Mettre en place une défense par silos (pelure d'oignons)
- Chiffrer les données, les communications, les entrepôts (PC portable..)
- Mettre en place une infrastructure des identités, des droits d'accès
- Contrôler la sortie des données critiques (DLP)

Délinquance astucieuse et nouvelles technologies
Faux ordres de virements et rançongiciels

Questions