ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

En partenariat avec :

EY Building a better working world

skema BUSINESS SCHOOL

Cyber Sécurité et Audit des vulnérabilités financières dont la chaîne de paiement

Avec le soutien des associations partenaires:

L'IFACI est affilié à The Institute of Internal Auditors

APDC Association des Professionnels et Directeurs Comptabilité & Gestion

DFCG Association Nationale des Directeurs Financiers et de Contrôle de Gestion

AFTE Association Française des Trésoriers d'Entreprise

Lille Place Financière

iae LILLE École Universitaire de Management

EPITECH. L'école de l'innovation et de l'expertise informatique

ifaci
institut français de l'audit et du contrôle internes

Notre partenaire méthodologique et conceptuelle

Intervenants et témoins pour cette conférence

- **Olivier PATOLE**, Senior Manager, Cyber Sécurité – EY

- **Ecole EPITECH** de Lille et son association de Cyber sécurité pour découvrir le Darknet

- **Christophe CAPON** – Directeur des Systèmes d'Information (DSI) de Vilogia

- **Olivier SIEROCKI -** Référent ANSSI Hauts-de-France

Les mensurations de cette conférence

151 inscrits provenant de 101 entreprises de la région

13 professions représentées sur toutes les lignes de maîtrise:

- Auditeurs internes, Auditeurs IT
- RSSI
- DSI
- Risks managers
- Contrôle interne
- Responsables assurances
- Directeurs administratifs et Financiers
- Contrôle de gestion
- Trésoriers
- Chefs comptables
- Commissaires aux comptes / Auditeurs externes
- Consultants en sécurité
- Inspecteurs Fraude

Des associations professionnelles et Ecoles œuvrant pour l'intérêt général :

Un grand cabinet:

ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

Introduction:

Cyber Sécurité et Audit des vulnérabilités financières dont la chaîne de paiement

L'IFACI est affilié à The Institute of Internal Auditors

ifaci
institut français de l'audit et du contrôle internes

Introduction….

Avec plus de 7000 participants lors de la neuvième édition du Forum international de la cybersécurité (FIC 2017), le forum Nordiste continue de s'imposer comme le salon incontournable de la cybersécurité en France.

FIC 2017 — 24 & 25 JANVIER 2017 | LILLE GRAND PALAIS | 9ème Forum International de la Cybersécurité

Le **commissaire Européen à la sécurité Julian King** a profité de l'occasion pour rappeler le rôle central de l'Europe dans le domaine de la cybersécurité "***Les cyberattaques peuvent être menée à coûts réduits pour des dégâts très importants et ne connaissent pas de frontières***" lors de la plénière d'ouverture le 24 janvier dernier.

.

Introduction….

Les attaques informatiques deviennent de plus en plus nombreuses et peuvent mettre parfois en péril les entreprises d'autant plus que celles-ci ne ciblent plus les seules grandes entreprises mais dorénavant aussi les ETI et les PME qui ne disposent pas toujours des mêmes moyens pour se défendre. **Les Cyber attaques changent aussi de physionomie en ciblant les systèmes financiers des entreprises permettant une source de revenu quasi assurée**. Le darknet, avec des logiciels comme TOR devient de plus en plus facile d'accès permettant dans l'anonymat le plus complet d'acquérir les outils nécessaires aux attaques pour de moins en moins cher ou de louer les services d'un hacker pour l'occasion.

La digitalisation de notre économie modifie en profondeur l'environnement dans lequel les entreprises évoluent et fait émerger de nouveaux risques. L'exposition pour les entreprises est d'autant plus importante, que celles-ci se concentrent sur le développement de nouveaux services et disposent de moins de temps pour appréhender les risques engendrés**. La cybercriminalité n'est plus seulement une menace, il s'agit d'une industrie organisée et structurée, une réalité dont l'impact devient considérable.**

La cybersécurité ne doit plus être l'affaire d'une seule fonction mais relève de la responsabilité de tous les acteurs d'une entreprise quelle que soit sa taille : chaque donnée peut présenter un risque et chaque collaborateur peut faire l'objet d'une tentative d'intrusion. Des mesures de sécurité basiques sont encore trop fréquemment négligées transformant les salariés non sensibilisés en vulnérabilités pour l'entreprise.

Introduction….

L'événement répondra notamment aux questions suivantes :

Quelles menaces faut-il craindre ?
Comment les anticiper ?
Notre système de sécurité est-il efficace pour lutter contre les risques et comment le savoir ?
Quels sont les impacts de ce type de vulnérabilité ? Comment s'en prémunir ?
Comment disposer d'une réponse adaptée à la taille d'entreprise (Grande Entreprise, ETI ou PME) ou à ses capacités financières ?
L'absence de RSSI ou de DSI au sein de l'entreprise permet-il d'être résilient ?
L'accès au darknet est-il si facile que cela ?
Un collaborateur insatisfait de son entreprise peut-il facilement s'improviser Hacker en toute impunité ?
Quels sont les 17 scenarios d'attaque interne ou externe sur la chaîne de paiement des entreprises?
Quelle cartographie des risques des vulnérabilités financières faut-il anticiper en 2017/2018?

ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

Le risque cyber, la cybersécurité et les vulnérabilités en 2017

Olivier PATOLE
Senior Manager, Cyber Sécurité – EY

Olivier.patole@fr.ey.com

EY Building a better working world

La cyber criminalité ?

ifaci

M International

INTERNATIONAL | Chroniques de la présidence Trump | Brexit | Etat islamique | Europe | Proche-Orient | Amériques | Afrique | Asie-Pacifique

ARTICLE SÉLECTIONNÉ DANS LA MATINALE DU 12/05/2017 > Découvrir l'application

Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays

Les attaques ont notamment perturbé les hôpitaux britanniques, le ministère de l'intérieur russe et le constructeur automobile français Renault.

LE MONDE | 13.05.2017 à 07h42 • Mis à jour le 13.05.2017 à 20h39 |

Par **Nathalie Guibert**, **Damien Leloup** et **Philippe Bernard** (Londres, correspondant)

Abonnez vous à partir de 1 € | Réagir | Ajouter | Partager | Tweeter

Piratage de TV5 Monde

La chaîne francophone TV5Monde a été la cible, mercredi 8 avril au soir, d'un piratage "inédit et de grande envergure" (TV, sites internet, réseaux sociaux ...

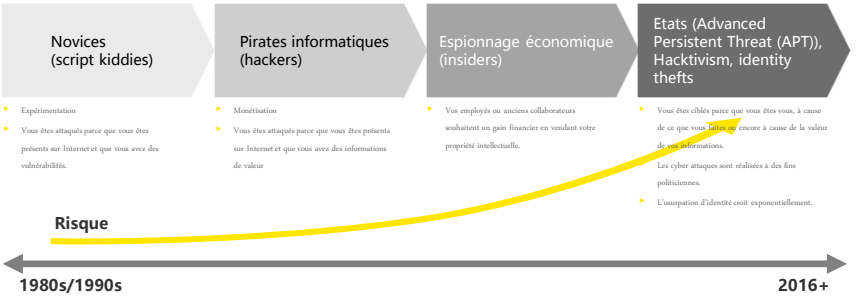
TV5 : Un piratage de la chaîne avec un interruption de service et message islamiste - *Pour un post-être un très grand mot, mais on a bien conscience qu'il faut qu'on fasse plus attention (...) C'est vrai, c'est assez stressant*", confie Estelle Martin, journaliste – Francetvinfo, Juin 2015

EY Building a better working world

Un secteur en pleine industrialisation

La menace Cyber évolue et s'industrialise

- Les attaquants sont de plus en plus patient, persévérant et compétents.
- La digitalisation de l'économie.
- La recrudescence des interconnexions.



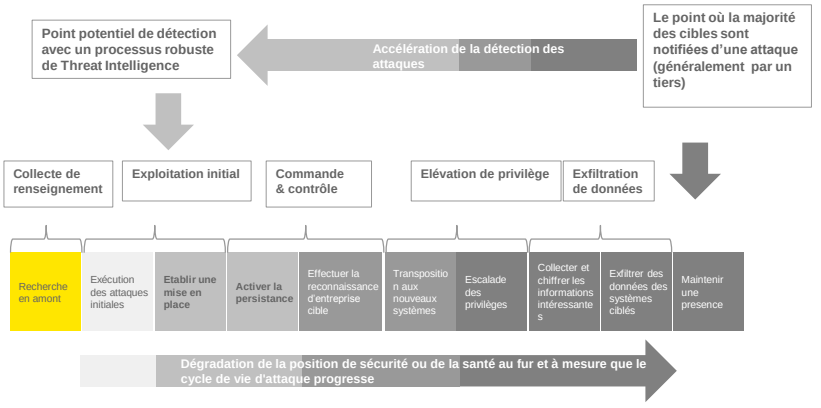
Un monde méconnu possédant des moyens inestimables

Un réseau ouvert où presque chaque élément d'information est stocké. Il contient à la fois des données consultables et non consultables, légaux et illégaux

Tout ce qui ne pourra pas apparaître dans une recherche Google / Yahoo / Bing / etc, mais qui est consultable avec des moteurs de recherche alternatifs.(silk Road, etc)

Tout ce qui est illégal sur internet. Des compétences et/ ou un logiciel spécial de piratage sont nécessaires pour y arriver.

La chronologie d'une attaque



Les nouvelles tendances en matière de cyber attaque

Le phishing

Un email frauduleux contenant un lien ou une pièce jointe est transmis à la cible pour le piéger. Le mail incite la cible à fournir des informations personnelles ou à ouvrir une pièce jointe infectée

Des ransomwares

Un logiciel, installé à l'insu de la victime, chiffre les données de celle-ci. Une rançon lui ait ensuite demandé avant la restitution ou non des données avec la menace de suppression des données.

La fraude au président

Un escroc se fait passer pour un dirigeant de l'entreprise auprès de personnes préalablement ciblées. L'objectif est d'extorquer de l'argent à l'entreprise en prétextant une opération financière urgente et importante.

Quel futur pour les demandes de rançon ?

- **Plus les données personnelles sont volées régulièrement, moins elles ont de la valeur sur le marché noir…**
- **… et plus les cybercriminels verront la rançon comme un moyen de gagner plus d'argent et plus simplement**

Les limites des approches traditionnelles

Un écosystème qui évolue

Emergence de cyber menaces dans l'écosystème :

- Emergence d'attaques de plus en plus sophistiquées et ciblées : Attaques 0-day, ransomware, vol de données sensibles, attaques sur les systèmes industriels.
- Les fournisseurs et partenaires sont de plus en plus exposés aux cyber risques

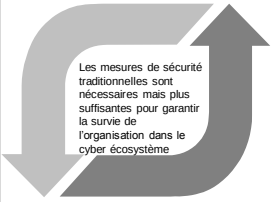
Forte dépendance à la digitalisation qui induit une augmentation de la surface d'exposition aux cyber menaces :

- La capacité du cyber écosystème à faciliter le partage d'information est à la fois son **plus gros atout** et son **plus gros danger**

Les limites du modèle de sécurité traditionnel :

- Besoin d'aller au delà de la sécurité périmétrique et tendre vers la sécurité en profondeur (au plus près de la donnée)
- Les plans de continuité métier sont axés uniquement sur la disponibilité (mais pas la confidentialité et l'intégrité des données)

Un changement important de la capacité de chaque individu et de chaque organisation est nécessaire afin de mieux collecter, analyser et utiliser les informations qu'auparavant



La maturité des défenses des entreprises

87% des membres de comités exécutifs ont des doutes sur le niveau de protection du dispositif de cyber sécurité de leur organisation.

64% **n'ont pas de stratégie de veille des cyber menaces,** ou seulement de manière informelle.

86% des répondants déclarent que **leur programme de cyber sécurité ne répond pas pleinement aux besoins de leur organisation.**

89% des entreprises n'évaluent pas l'impact financier de chaque infraction significative.

57% **des répondants ont eu récemment un incident important de cyber sécurité.**

5% affirment **avoir changé récemment et significativement leurs plans stratégiques après avoir pris conscience** qu'ils étaient exposés à de trop nombreux risques.

La maturité des défenses des entreprises

47% des organisations ne disposent pas de SOC (Security Operations Center).

54% indiquent ne pas avoir de fonction dédiée aux nouvelles technologies et à leurs impacts sécurité

36% n'ont pas confiance en leur capacité à détecter les attaques informatiques sophistiquées

36% n'ont pas de programme permettant d'anticiper les menaces et de réagir en cas d'attaque (threat intelligence).

57% mettent en avant un manque de ressources sécurité compétentes.

29% jugent mature la sécurité de leurs applications.

Les principales vulnérabilités des entreprises

La figure 1 présente le résultat de l'étude GISS de 2013 à 2016

	2013	2014	2015	2016
Vulnérabilités				
Salariés non sensibilisés	53%	57%	44%	55%
Systèmes obsolètes	51%	52%	34%	48%
Accès sans autorisation	34%	34%	32%	54%
Menaces				
Logiciels malveillants	41%	34%	43%	52%
Phishing	39%	39%	44%	51%
Cyberattaques conçues pour voler des informations financières	46%	51%	33%	45%
Cyberattaques conçues pour voler des données ou de la propriété intellectuelle	41%	44%	30%	42%
Attaques en interne	28%	31%	27%	33%

Figure 1 : Evolution des menaces/vulnérabilités

Constat

Cette figure montre que les vulnérabilités associées au **manque de sensibilisation des employés** et à **l'obsolescence des systèmes** sont les vulnérabilités les plus importantes. Parmi les menaces, on retrouve les logiciels malveillants et les tentatives de phishing

Quelques chiffres…

La figure 1 présente l'évolution du pourcentage des principales réponses, (notées 1 - la plus élevée et notées 2 - élevée), des **vulnérabilités** qui ont augmenté l'exposition aux risques des organisations en 2016.

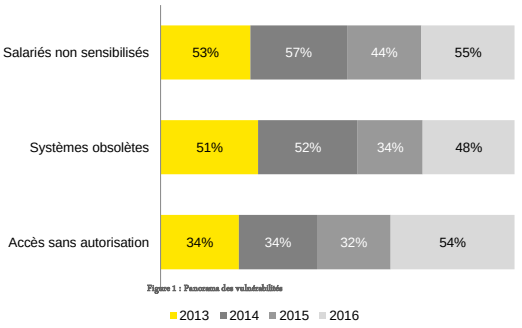


Figure 1 : Panorama des vulnérabilités

Constat

L'étude GISS de 2016 montre un **accroissement des vulnérabilités** liés aux comportements de salariés non sensibilisés aux enjeux de cyber sécurité, des systèmes obsolètes ou encore des accès sans autorisation.

Olivier Patole – Senior manager - EY

Quelques chiffres…

La figure 2 présente l'évolution du pourcentage des principales réponses, (notées 1 - la plus élevée et notées 2 - élevée), des **menaces** qui ont augmenté l'exposition aux risques des organisations en 2016.

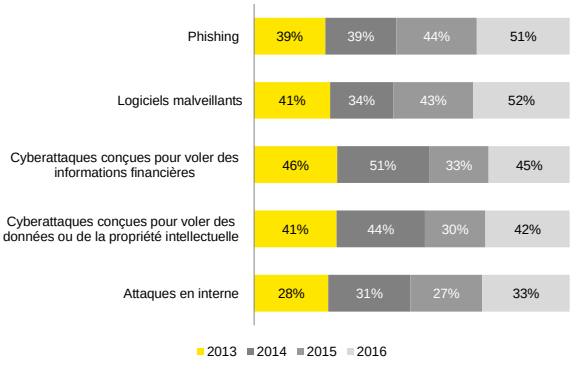


Figure 2 : Panorama des menaces

Constat

Cette année, on constate **une réévaluation de l'exposition aux risques des organisations**. Alors qu'elles affichaient un véritable optimisme en 2015, il semblerait qu'après une phase de rodage de leurs systèmes, elles aient finalement véritablement pris conscience de la nature de la menace.

Olivier Patole – Senior manager - EY

La maturité des entreprises au regard de la cyber résilience

Les **priorités** et les **investissements** des organisations sont surtout portés sur **les dispositifs de protection** et **beaucoup moins** sur les **solutions de réaction** suite à une attaque.

	Anticiper	Résister	Réagir
Domaines prioritaires pour les organisations	MOYEN	FORT	FAIBLE
Les investissements des organisations	MOYEN	FORT	FAIBLE
Engagement du comité exécutif et des C-Suites	FAIBLE	FORT	FAIBLE
Qualité du reporting à la direction ou au comité exécutif	FAIBLE	MOYEN	FAIBLE

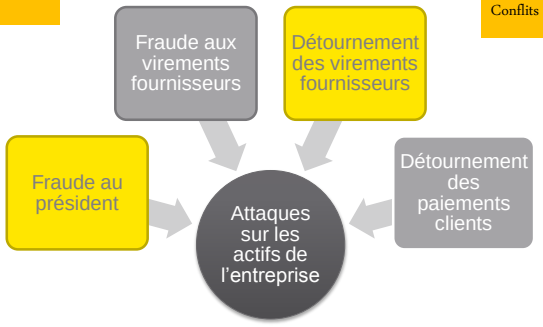
Focus sur les fraudes financières ciblant la chaîne de paiement

Attaques externes

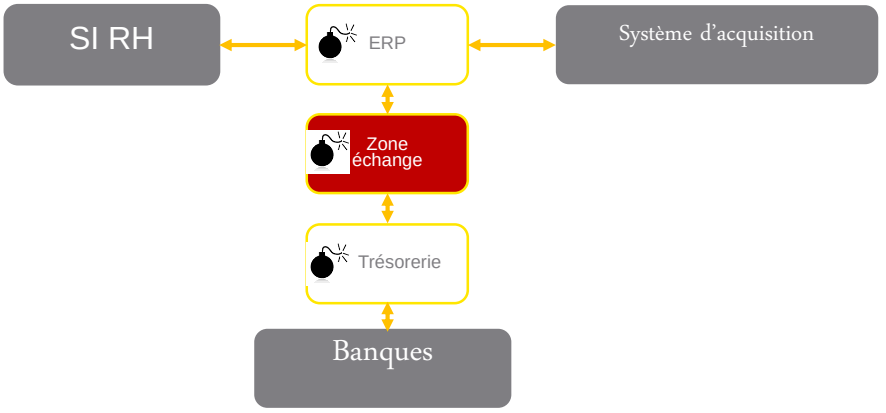
- Attaques simples mais efficaces (Exemple : détournements de fonds, fraude au président, avec des impacts significatifs)
- Attaques très complexes (prise de contrôle des ordinateurs des employés)

Attaques internes

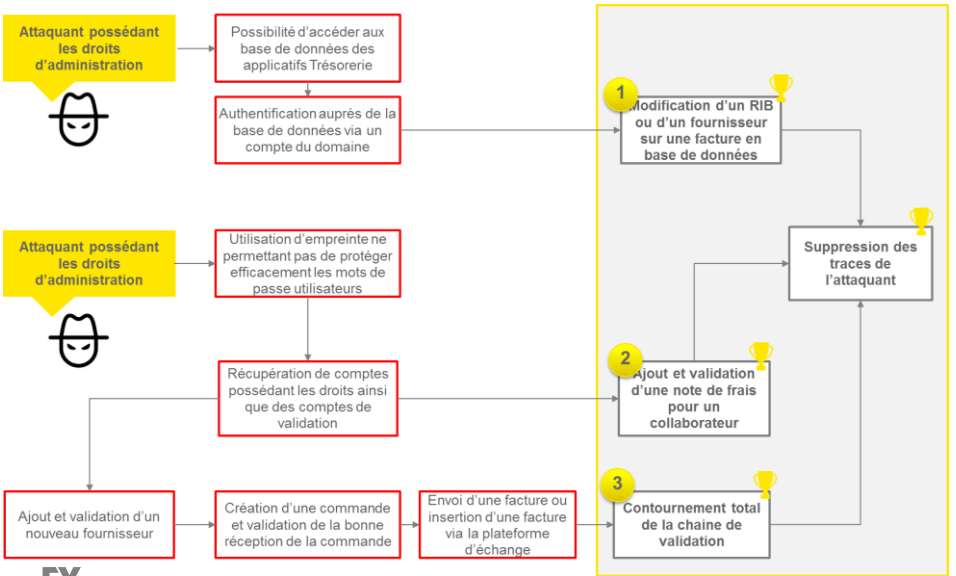
- Changement de RIB
- Auto-approbation des dépenses
- Abus sur les notes de frais
- Détournements de paiements et de remboursements
- Conflits d'intérêts



Les principales faiblesses de la chaine de paiement



Exemple de scénarii que nous retrouvons dans de nombreux environnements



17 Scénarios possibles identifiés

Depuis l'extérieur

1. Fraude au président (Appel téléphonique et demande de paiement sur un compte inconnu)
2. Appel téléphonique et usurpation d'identité d'un des fournisseurs pour effectuer une modification des coordonnées bancaires du fournisseur en question
3. Envoi d'email falsifié en usurpant l'identité d'un fournisseur demandant de modifier les coordonnées bancaires du fournisseur en question
4. Envoie d'une fausse facture reprenant la charte graphique de la société
5. Appel d'une hypothétique hotline informatique pour prendre le contrôle à distance sur le logiciel de trésorerie ou obtenir les mots de passe

Depuis l'intérieur

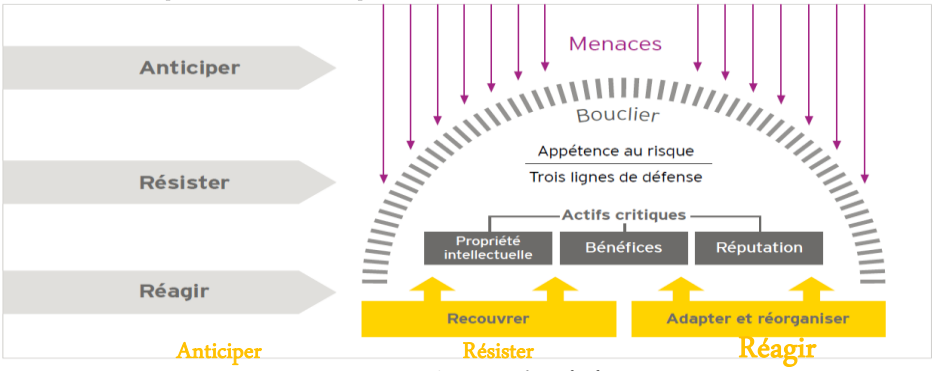
1. Usurpation d'identité des différents utilisateurs de l'ERP et/ou de la plateforme de trésorerie afin d'y soumettre des demandes et de les valider de manière transparente
2. Exploitation d'une vulnérabilité de l'ERP et/ou de la plateforme de trésorerie permettant d'élever ses privilèges et ainsi modifier le montant d'une facture
3. Exploitation d'une vulnérabilité de l'ERP et/ou de la plateforme de trésorerie permettant d'élever ses privilèges et ainsi créer un faux fournisseur, un faux bon de commande et une fausse facture
4. Exploitation d'une vulnérabilité de l'ERP et/ou de la plateforme de trésorerie permettant d'élever ses privilèges et ainsi modifier le montant d'une note de frais
5. Exploitation d'une vulnérabilité de l'ERP et/ou de la plateforme de trésorerie permettant d'élever ses privilèges et ainsi créer une fausse note de frais et la passer en paiement sans validation effective du justificatif
6. Détournement volontaire d'un pourcentage des montants (peu perceptible) de notes de frais payés aux collaborateurs la société
7. Modification du montant d'une facture en falsifiant le fichier des transactions positionné dans la zone d'échange entre l'ERP et la plateforme de trésorerie
8. Modification du RIB du fournisseur pour lequel une facture doit être payée
9. Falsification d'une facture reçu au courrier pour un paiement sans bon de commande
10. Changement des coordonnées bancaires des fournisseurs le temps d'une campagne de paiement et rétablissement des données initiales via un accès à l'ERP et/ou la trésorerie
11. Détournement volontaire d'un pourcentage des montants (peu perceptible) de factures fournisseurs
12. Enregistrement et paiement de fausses factures par un employé dans les rubriques fournisseurs divers

EY Building a better working world

Olivier Patole – Senior manager - EY

Comment s'en prémunir ?

La **cyber résilience** est une composante de la résilience économique : elle mesure la résilience d'une organisation confrontée à une cyber menace au cours de **trois phases** clefs d'actions : **l'anticipation, la résistance et la réaction**.



Anticiper, c'est être capable de **prévoir et de détecter** les cyber menaces. Pour cela, les organisations ont recours à une stratégie de veille (**cyber threat intelligence**) et à une démarche de défense active.

Résister, c'est mettre en place un **bouclier efficace** de protection. Il comprend **trois lignes de défense** (mesures de contrôle, déploiement de fonctions de suivi et recours au département d'audit interne).

Réagir, c'est disposer d'une capacité de **réponse adaptée** pour gérer la crise. Mais également **apprendre de l'incident** et donc adapter ses systèmes afin d'améliorer sa cyber résilience.

EY Building a better working world

Olivier Patole – Senior manager - EY

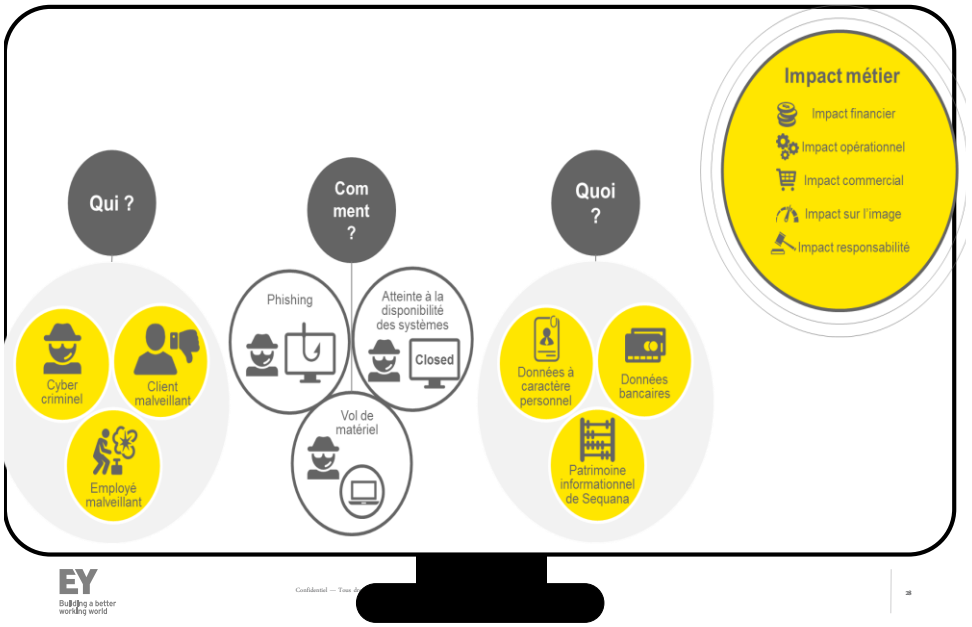
Comment s'en prémunir ?

Appliquer les bonnes pratiques

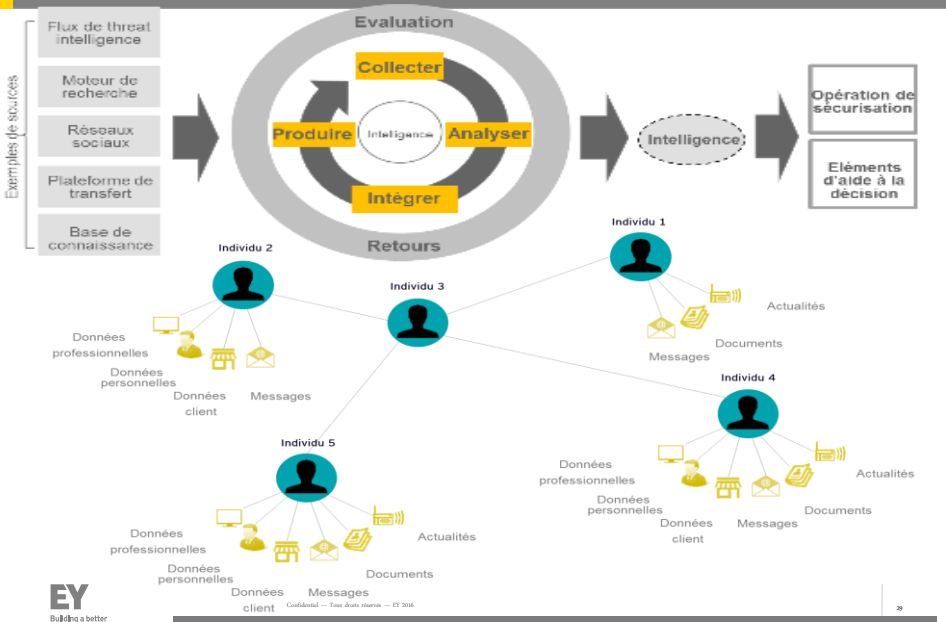
ISO 27001

Olivier Patole – Senior manager - EY

La Cyber Intelligence pour doper votre capacité à anticiper

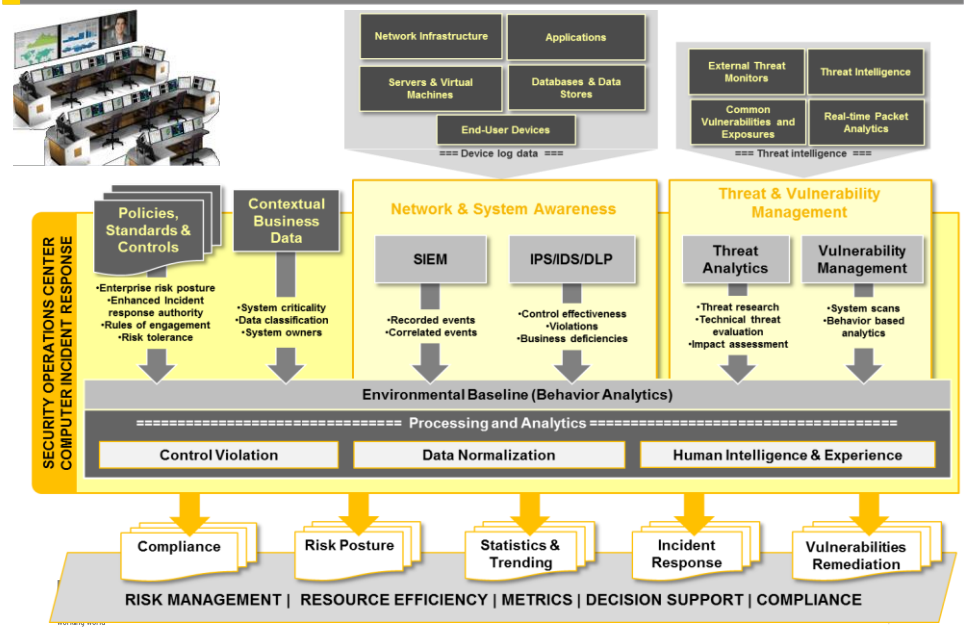


La Cyber Intelligence devient indispensable



Olivier Patole – Senior manager - EY

Le SOC, un élément indispensable de votre stratégie de protection



ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

EPITECH.
L'ECOLE DE L'INNOVATION ET DE L'EXPERTISE INFORMATIQUE

Découvrir le Darknet

Ecole EPITECH de Lille et son association de Cyber sécurité

5-9, rue du Palais Rihour
59000 Lille - Tél : 01 44 08 00 10

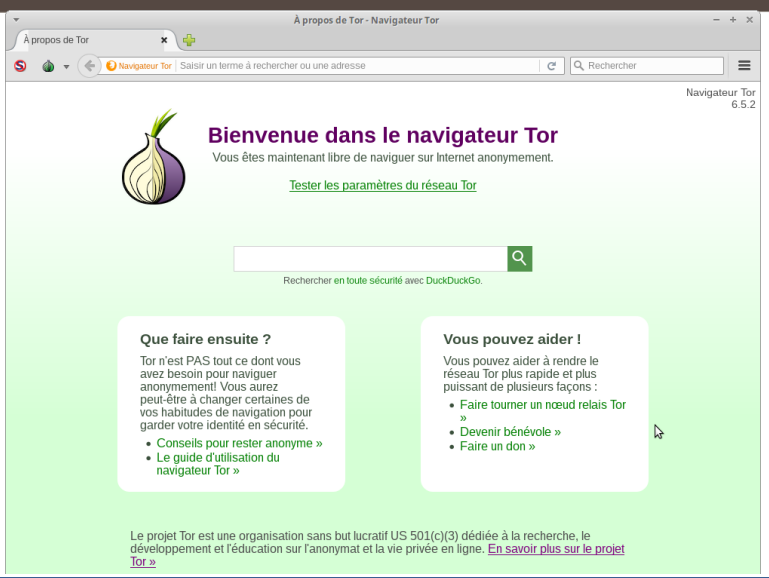
L'IFACI est affilié à The Institute of Internal Auditors

ifaci
institut français de l'audit et du contrôle internes

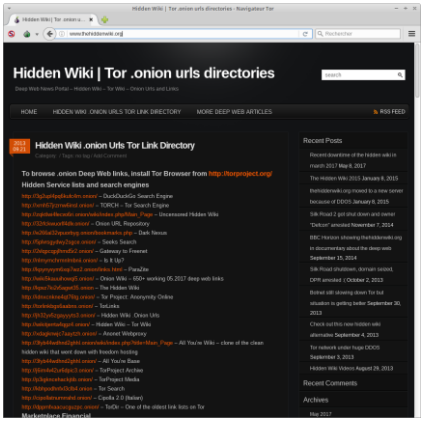
FIC 2017

Qu'est-ce que le darknet ?

Comment l'utiliser ?



Comment l'utiliser ?

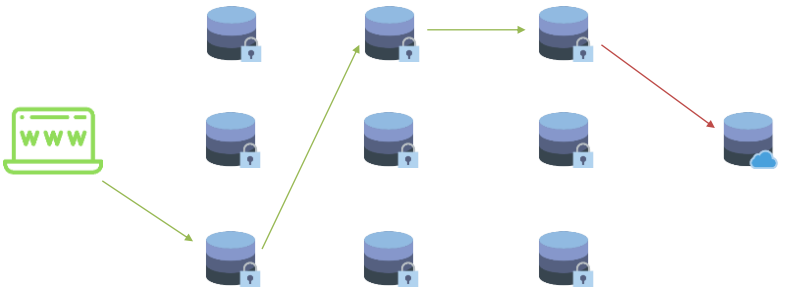


Comment ça marche ?

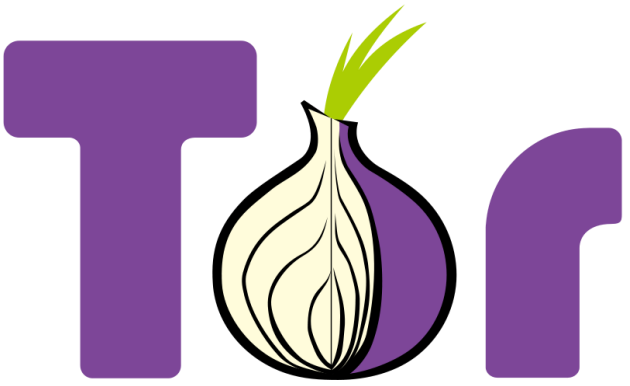
Comment ça marche ?

Comment ça marche ?

Comment ça marche ?



Démonstration



AVEZ-VOUS DES QUESTIONS ?

EPITECH.
L'ECOLE DE L'INNOVATION ET DE L'EXPERTISE INFORMATIQUE

ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

ETI et risque Cyber

Christophe CAPON
Directeur des Systèmes d'Information (DSI) de Vilogia

christophe.capon@vilogia.fr

Vilogia
Bien dans ma ville

ETI et risque Cyber
Le contexte VILOGIA

- La taille et les moyens d'une ETI…mais les ennuis potentiels d'un grand groupe
  - Système riche et multi métiers
  - Très intégré en interne et vers le monde extérieur
- Menaces
  - Externes ou internes
  - Qui ne ciblent pas que le SI Finances !

ETI et risque Cyber
Craintes actuelles

- La perte/le vol de données
- L'altération des circuits financiers
- L'indisponibilité opérationnelle

ETI et risque Cyber
Organisation et processus

- Audit sécurité : test d'intrusion régulier
- Les difficultés
- Pas de RSSI : un problème ?

- Les autres acteurs
  - Audit interne et comité d'audit
  - Corresponsant Informatique et Libertés

ETI et risque Cyber
La réponse RH

- DSI
  - Formation des équipes
  - Compétences des développeurs
  - Architecte technique

- Collaborateurs
  - Sensibilisation

ETI et risque Cyber
Réponse technologique

- Préventif
  - Firewall
  - Antispam externalisé
  - DMZ
  - Antivirus
- Curatif
  - PRA
  - Backups

ETI et risque Cyber

- Questions ?

ifaci
institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

GUIDE D'HYGIÈNE INFORMATIQUE

RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

ANSSI
Autorité Nationale de défense et de Sécurité des Systèmes d'Informations

Olivier SIEROCKI
Référent ANSSI Hauts-de-France
SGDSN/ANSSI/RELEC/COT

Hauts-de-france@ssi.gouv.fr

ifaci
institut français de l'audit et du contrôle internes

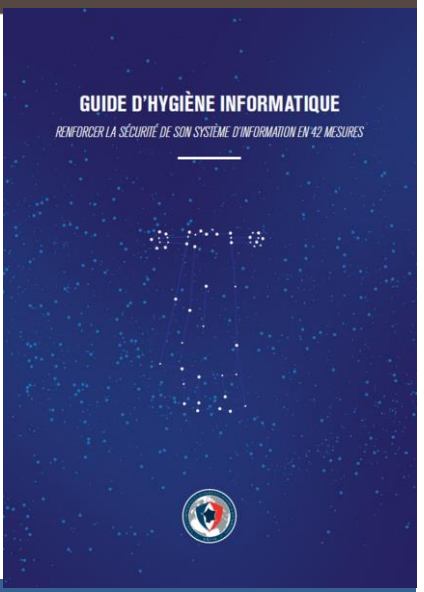
GUIDE D'HYGIÈNE INFORMATIQUE
RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

Le guide d'hygiène informatique version 2 de janvier 2017

Les changements :
- 42 règles (40 dans la version 1)
- 10 chapitres (13 dans la version 1)

Concrètement :
- Une approche **plus pragmatique**,
- Une rédaction **plus compréhensible**,
- Une cible plus large,

Mais à destination des familiers de la technique.



GUIDE D'HYGIÈNE INFORMATIQUE

RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

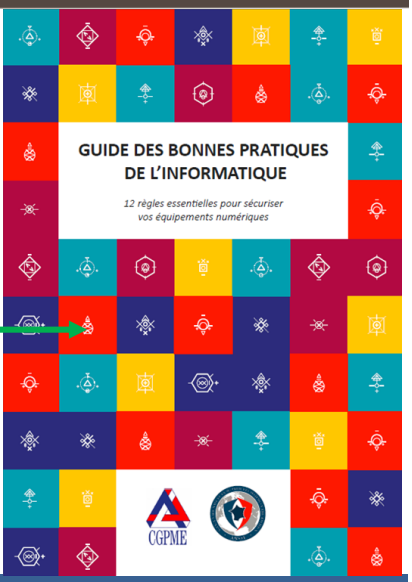
Question: une réponse uniquement pour les PME?

A l'approche basée sur la taille de la structure (startup, TPE, PME, ETI) on doit préférer l'approche sur la **maturité** de la structure.

Un guide simplifié, **plus compréhensible** par un plus grand nombre : le ***Guide des bonnes pratiques de l'informatique – 12 règles essentielles pour sécuriser vos équipements numériques***

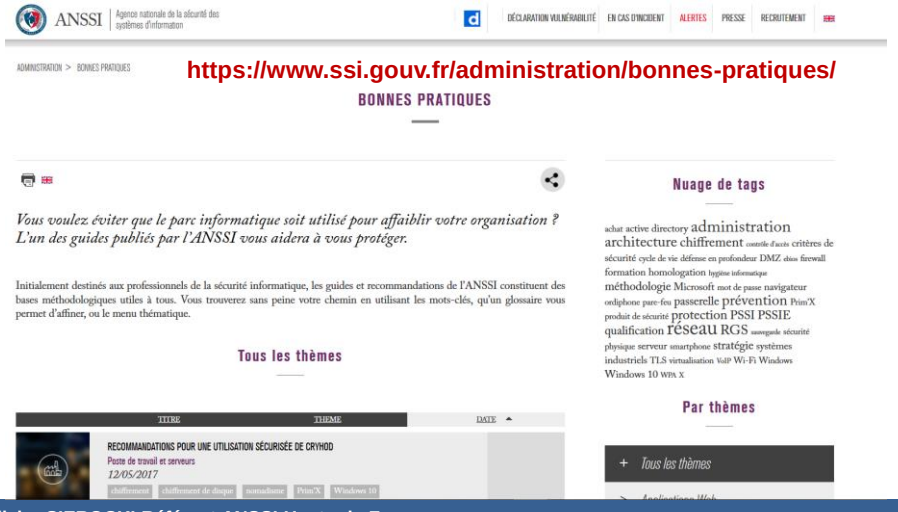
Une **base** pour établir un plan d'action de cybersécurité.

Un guide qui conserve des **limites**.

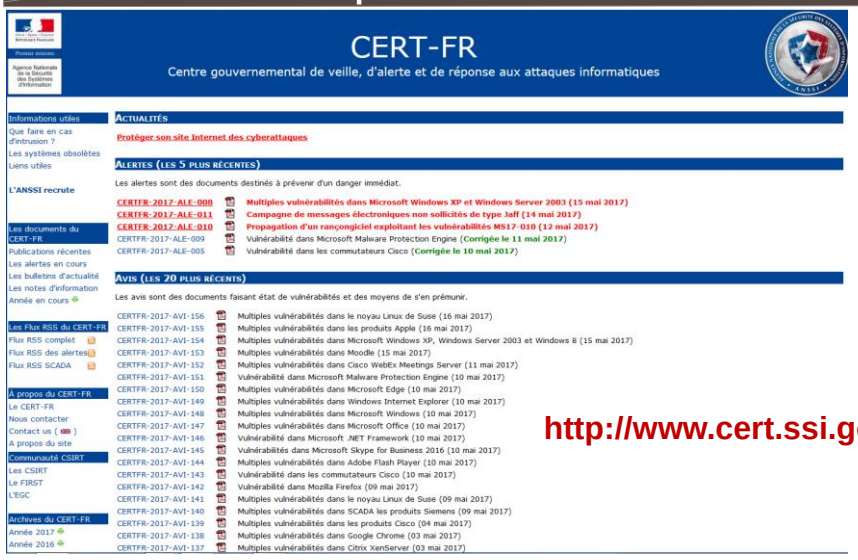


Pour aller plus loin... Une des premières étapes vers les autres guides de l'ANSSI, plus techniques et plus détaillés.

Si besoin , ne pas hésiter à **revenir aux fondamentaux**, plus simples, que constituent le Guide des Bonnes Pratiques, le Passeport Voyageurs, etc.



Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques à votre disposition



http://www.cert.ssi.gouv.fr/

institut français de l'audit et du contrôle internes

Antenne Hauts de France

16 Mai 2017

Questions / Réponses

Conclusion (synthèse de l'ensemble avec Carole Dessaint d'EY)

L'IFACI est affilié à The Institute of Internal Auditors

Vif merci

Un grand Merci aux étudiants du MS Expert Contrôle de Gestion SI de Skema et à toute l'équipe dEY

De la part de tous nos partenaires:

Save The Date et recherche de témoins en région

MAZARS DARROIS VILLEY MAILLOT BROCHIER

Conférence débat

Jeudi 15 Juin 2017 à l'IAE de Lille à 18h

Loi Sapin 2 anticorruption, lancement d'alerte : des méthodes pour rester serein ?

Premiers Intervenants et témoins

> **Carine DUPEYRON**, Avocat au barreau de Paris, Darrois Villey Maillot Brochier
> **François NOGARET**, Associé, Mazars
> **Pierre Alain AUBIN**, Directeur de l'audit interne et des risques, Eurazeo

eurazeo

Nous recherchons un témoin dans la région pour présenter au choix:

- **Son dispositif Sapin 2**
- **Son projet de migration de ses dispositifs UK BA et FCPA vers Sapin 2**
- **… selon l'avancement pour identifier les difficultés rencontrées au titre de retour d'expérience.**

ifaci
institut français de l'audit et du contrôle internes

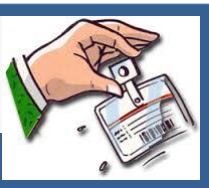
Antenne Hauts de France

16 Mai 2017

merci

En partenariat avec :

Le Geste Citoyen



Cocktail à l'initiative d'EY

L'IFACI est affilié à
The Institute of Internal Auditors

EY Building a better working world