BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

3) Dans le cadre de la coopération internationale :

Coopération Policière :

- messages urgents à l'attention des services de police compétents sur les lieux de virements,
- échanges de renseignements avec services de police locaux (enquête miroirs),
- coordination internationale via EUROPOL et INTERPOL,
- consultation de TRACFIN mais aussi des cellules de renseignements financiers étrangères.

Coopération Judiciaire :

- demandes d'entraide pénale internationale ou Commission Rogatoire Internationale,
- formalisation, actualisation et suivi des demandes,
- coordination judiciaire internationale via EUROJUST,
- déplacements à l'étranger des magistrats et enquêteurs.

BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

4) Exploitation des résultats obtenus et difficultés rencontrées :

Exploitation des résultats :

- en vue de la matérialisation de l'infraction, démonstration de la bande organisée, identification des schémas de blanchiment,
- de la poursuite des investigations, en France et à l'étranger,
- de l'identification et la localisation des auteurs.

Difficultés rencontrées :

- délais d'exécutions des demandes et pertinence des réponses,
- échelle d'intervention, volume et prescription des données, volatilité et vélocité des fonds, mobilité des escrocs et échelle d'action (cyberespace, paradis fiscaux et pays non-coopératifs),
- surenchère des moyens mis en œuvre par les escrocs (matériels mais aussi intellectuels).
- blanchiment dans la sphère économique légale.

BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

5) Bilan actualisé :

Des points négatifs :

- un arsenal juridique perfectible, mais surtout qui devrait être plus dissuasif,
- les escroqueries perdurent malgré les fréquentes sensibilisations,
- elles se complexifient, notamment les schémas de blanchiment,
- un coût financier et social, important, supporté par les sociétés victimes,
- le coût croissant des investigations.

Des points positifs :

- interruption des virements,
- la récupération ou le gel des fonds à l'étranger,
- identifications, interpellations et mises en examen des auteurs,
- amélioration de la coopération judiciaire et policière internationale et interpellations,
- saisies d'avoirs criminels.

LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

La géopolitique des cybermenaces la relation entre cyberattaques

Jean-François THONY

« En fait, Internet est foncièrement « dual ». Il est un moyen, un outil d'influence et d'action au profit des acteurs de la mondialisation. Mais il est aussi un espace où se déploient les stratégies de puissance, de croissance, de prédation ou de (re)positionnement de ces acteurs.

Donc un « territoire » au sens de l'analyse géopolitique, à savoir un « espace habité [même virtuellement, mais en tout cas occupé] par les hommes, un terrain "magique", signifiant, chargé de symboles et de mémoires concurrentes »

(Note d'analyse géopolitique CLES de Grenoble Ecole de management, n°154, 05/03/15 Internet un espace de jeu politique, Olivier Zajec, Introduction à l'analyse géopolitique, Argos, 2013).

LES PRINCIPALES CYBERMENACES

- La cyberguerre
- La cybercriminalité
- Le cyberactivisme
- Le cyberterrorisme
- Les cybercasseurs

- Toutes transnationales

LES PRINCIPALES CYBERMENACES:

La cyberguerre

- Renseignement
  - Militaire
  - Diplomatique
  - économique
- Guerre économique
- Rétorsion
- Déstabilisation/désorganisation
- Destruction des infrastructures

LES PRINCIPALES CYBERMENACES:

Cyberguerre en temps de paix et en temps de guerre

- La notion de guerre et de paix s'estompe dans le cyberespace
- Comme la notion de souveraineté
- Et la notion d'agression

LES PRINCIPALES CYBERMENACES:

La cybercriminalité

- Finalité unique = profit
- Vise les particuliers, les entreprises, les établissements financiers
- Palette d'infractions variée: vol, escroquerie, abus de confiance, extorsion (menaces), recel, contrefaçon, blanchiment
- Exception des infractions à caractère sexuel
  - Peuvent viser le profit
  - Ou simplement la prédation sexuelle

LES PRINCIPALES CYBERMENACES:

La cybercriminalité

- Modalités variées:
  - Haute technologie (hacking, etc.)
  - Utilisation basique des ressources informatiques (messagerie électronique)
  - Support de médias sociaux ou de sites marchands existants

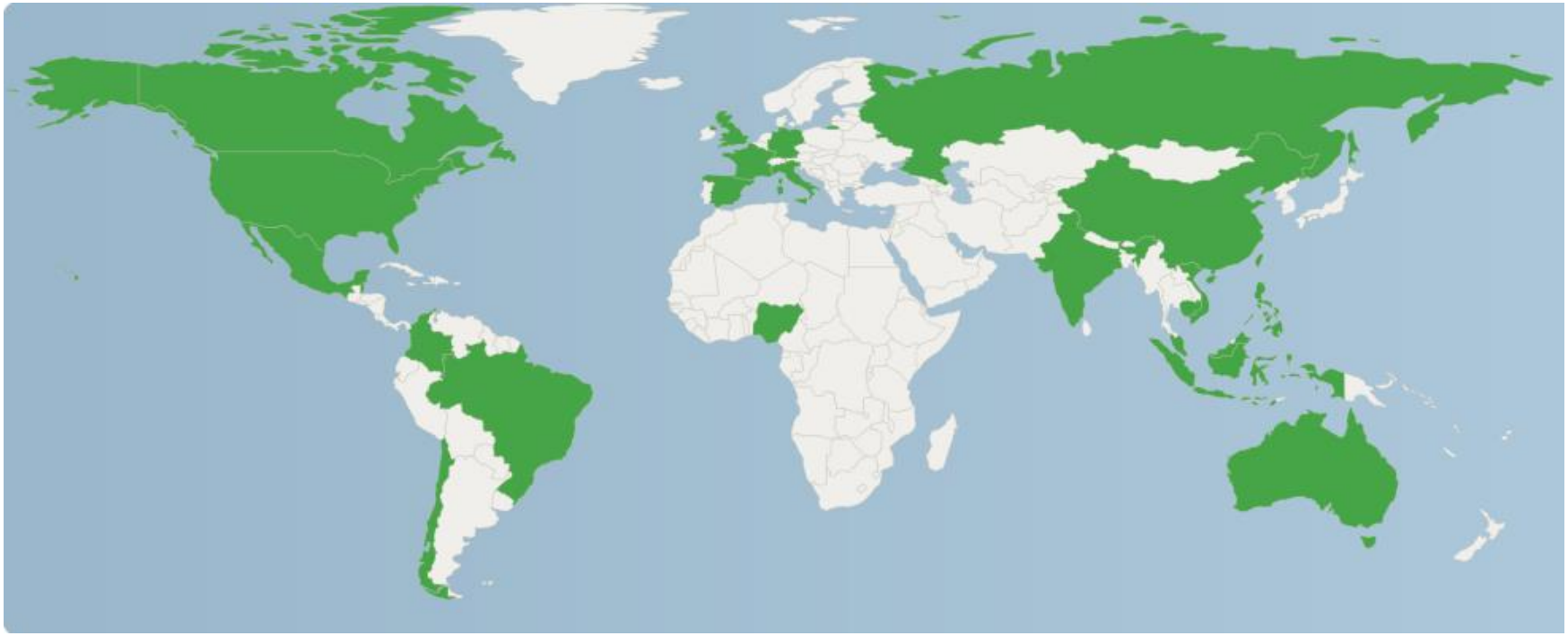
CYBERCRIMINALITÉ ET CRIME ORGANISÉ

- **La dématérialisation des marchés criminels existants**
  - Le vol de voitures
  - La contrefaçon
  - Les escroqueries

- **La création de nouveaux marchés criminels**
  - Les nouveaux « produits »
  - Un marché parallèle structuré

- **L'émergence de nouvelles organisations criminelles**
  - Cybercriminalité de basse technologie: organisations traditionnelles
  - Cybercriminalité de haute technologie: nouveaux schémas

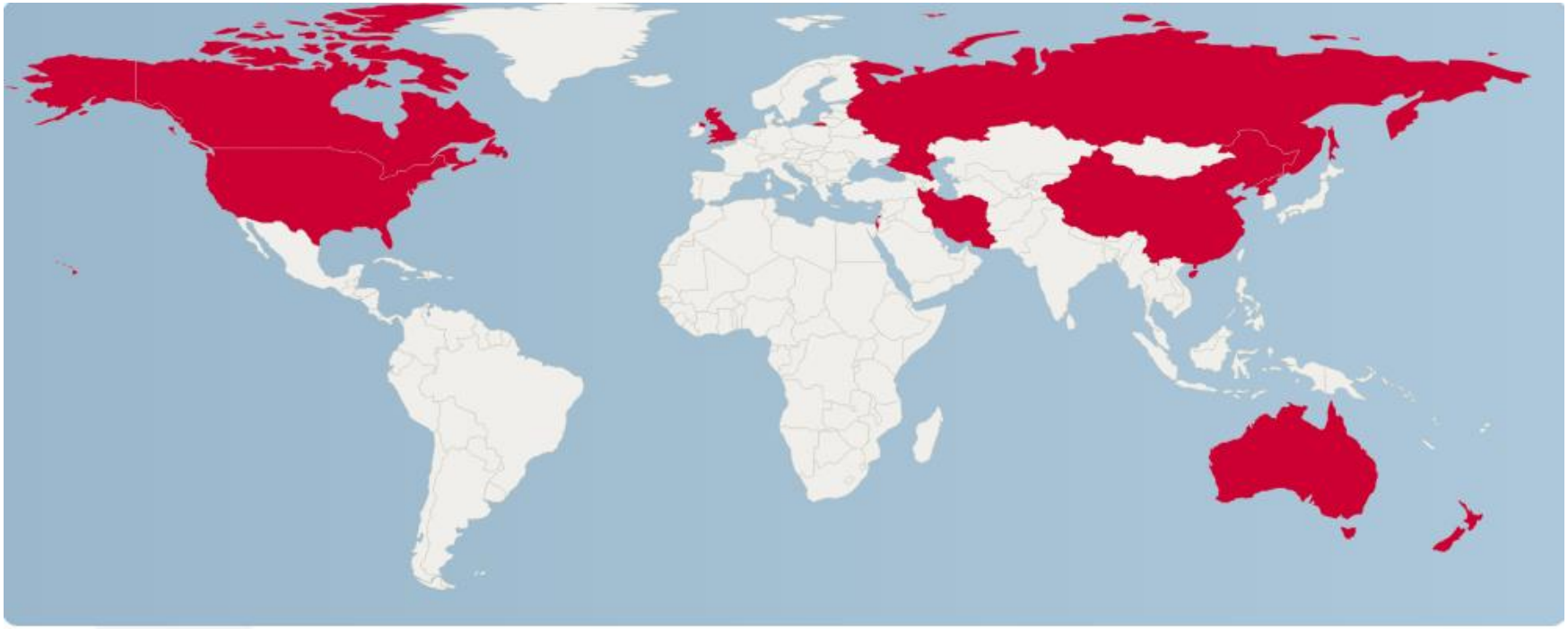
LA CYBERCRIMINALITÉ ET LE RÔLE DU CRIME ORGANISÉ



Représentation géographique des faits de cybercriminalité entre 2015 et 2016

Sources : rapport annuel d'Europol 2016, articles

LA GÉOGRAPHIE DE LA CYBERGUERRE



Principaux Etats à l'origine de cyberattaques entre 2010 et 2016

III. LES CYBERATTAQUES ET LE CRIME ORGANISÉ

Les rapports de pouvoir sur le territoire du cyberespace

- **Une relation ambiguë entre le crime organisé et les Etats**
  - Les Etats recrutent parmi les membres du crime organisé
  - Les Etats alimentent les rangs du crime organisé

- **Le crime organisé et les autres acteurs du cyberespace**
  - Affrontement entre les Zetas et les Anonymous

CONCLUSION

- **Le cyberespace a besoin d'une réglementation internationale**
  - Impulsée par des nations puissantes, elles-mêmes actrices du cyberespace
- **La réglementation devra s'appliquer à tous les acteurs**
  - Étatiques
  - Non-étatiques

LA CYBERCRIMINALITÉ :
UN BUSINESS LUCRATIF

QUESTIONS
RÉPONSES

9ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

… POURTANT DES SOLUTIONS EXISTENT

Démonstration d'attaque par rançongiciel

- **Julien GAMBA, Nicolas RENARD, Vinh LUONG**

  Etudiants en Master 2 - Réseaux informatiques et systèmes embarqués à l'Université de Strasbourg

- **Benjamin CHETIOUI**

  Etudiant en Master 2 - Ingénierie du Logiciel et des Connaissances à l'Université de Strasbourg

PLAN DE LA CONFERENCE

4 points-clés

Définition

Qu'est-ce qu'un ransomware ?
Beaucoup d'entreprises touchées ?

Bonnes pratiques

Que faut-il faire pour se prévenir de ce type d'attaque ?
Que faire quand son ordinateur est touché ?

Démonstration

En direct sur un PC.

Analyse

Les limites de la démonstration.

LES MALWARES

Les logiciels malveillants – Les différences

Virus			Logiciel espion (Spyware)
Ver (Worm)			Keylogger
Cheval de Troie (Trojan)			Rançongiciel (Ransomware)
Une porte dérobée (Backdoor)			Et bien d'autres encore…

LES RANSOMWARES

Les rançongiciels – Définition

Logiciels malveillants qui prennent en otage les données personnelles. Les rançongiciels chiffrent les données puis demandent à leur propriétaire d'envoyer de l'argent afin d'obtenir la clef qui permet de les déchiffrer.

LES RANSOMWARES

Les rançongiciels – Les différents types

Chiffre les données	Verrouille l'ordinateur	Chiffre le MBR	Chiffre les Web servers	Pour Android
Chiffre toutes les données de l'ordinateur	Verrouille l'écran	Chiffre uniquement le MBR, l'ordinateur ne peut plus démarrer normalement	Vise les serveurs webs et crypte les fichiers dessus	Spécialement développé pour Android

LES RANSOMWARES

Les rançongiciels – Histoire

1986
Premier ransomware connu sous le nom de “PC Cyborg”

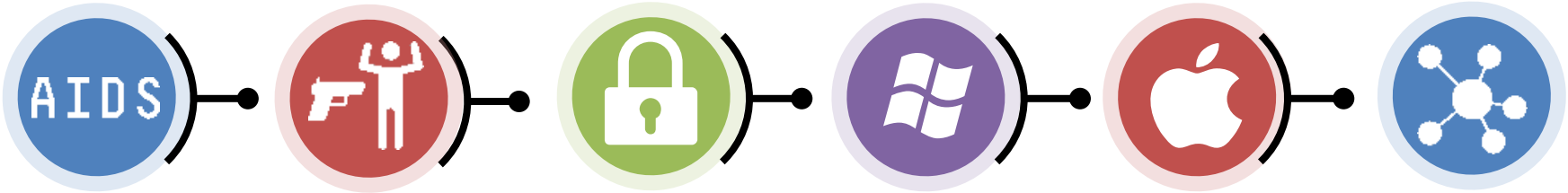
2005
Les premiers ransomwares d’extortion apparaissent

2006
Ransomware avec des clefs RSA encore plus compliquées

2011
Un ver ransomware imite l’activation Windows

2013
Le premier ransomware pour ordinateur de la marque Apple apparaît

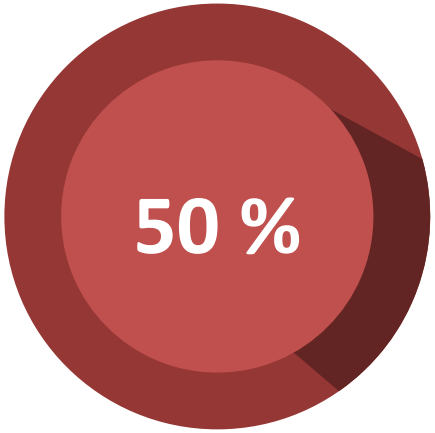
2015
Des ransomwares sur plusieurs plateformes



LES RANSOMWARES

Les rançongiciels – Quelques chiffres

Menaces pour les entreprises en 2016



Des entreprises paient la rançon

Montant moyen de la rançon demandée

LES RANSOMWARES

Les rançongiciels – Prévention

- Sauvegarder
- Ne faire confiance à personne
- Mettre en place un bon antivirus
- Activer l'option "Afficher les extensions" dans les paramètres Windows
- Effectuer les mises à jour
- Déconnecter la machine d'Internet si programme suspect et ne pas éteindre l'ordinateur

LES RANSOMWARES

Les rançongiciels – Pourquoi il ne faut pas payer ?

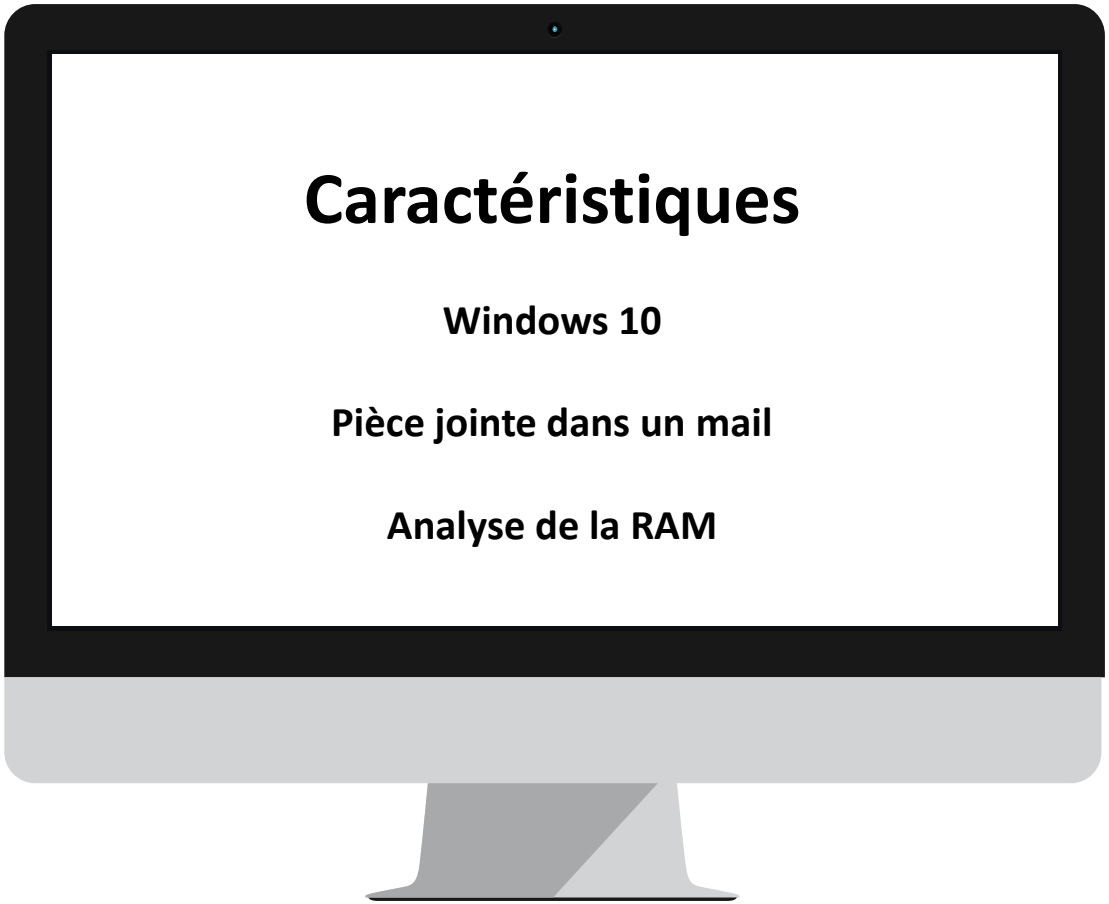
Aucune garantie

Déchiffrement mal implémenté

Incite les criminels à continuer

LES RANSOMWARES

Démonstration en live



LES RANSOMWARES

Démonstration – Les limites

Clef simple

Chiffrement symétrique et non asymétrique

Un dossier chiffré uniquement

Un seul dossier a été chiffré et non tout le disque dur

Pièce jointe facilement détectable

L'extension du fichier laisse facilement deviner que c'est un malware

TABLE RONDE 2

… pourtant des solutions existent

… POURTANT DES SOLUTIONS EXISTENT

- **Ludovic HAYE**

  Consultant IT à l'international

  Délégué Régional de l'Anaj-IHEDN (Alsace)

  Chef d'Escadron (RC) de la Région de Gendarmerie nationale.

- **Daniel GUINIER**

  Expert près de la Cour pénale internationale de la Haye

  Colonel (RC) de la Gendarmerie nationale

- **Laurent SCHMERBER**

  Président 3MA Group

  Chef d'escadron (RC) de la Gendarmerie nationale

… POURTANT DES SOLUTIONS EXISTENT

La signature électronique : une solution contre la fraude

Ludovic HAYE

LE PARADIGNE DE SIGNATURE ELECTRONIQUE

- N’est pas un concept nouveau
- Réponse technique à la gestion de la preuve numérique
- Considérée comme plus sûre que la signature manuscrite

LE CONTEXTE

- **L'explosion du phénomène de fraude externe**

77% des entreprises (Etude effectuée par Euler et la DFCG)

-> C'est + 51% (38% dans le reste du monde).

- **La fraude est devenue un phénomène de masse qui touche toutes les structures économiques**

Du grand groupe en passant par l'ETI, jusqu'à la PME

- **La fraude externe n'est pas la seule à battre des records. (60% des cas de fraude interne)**

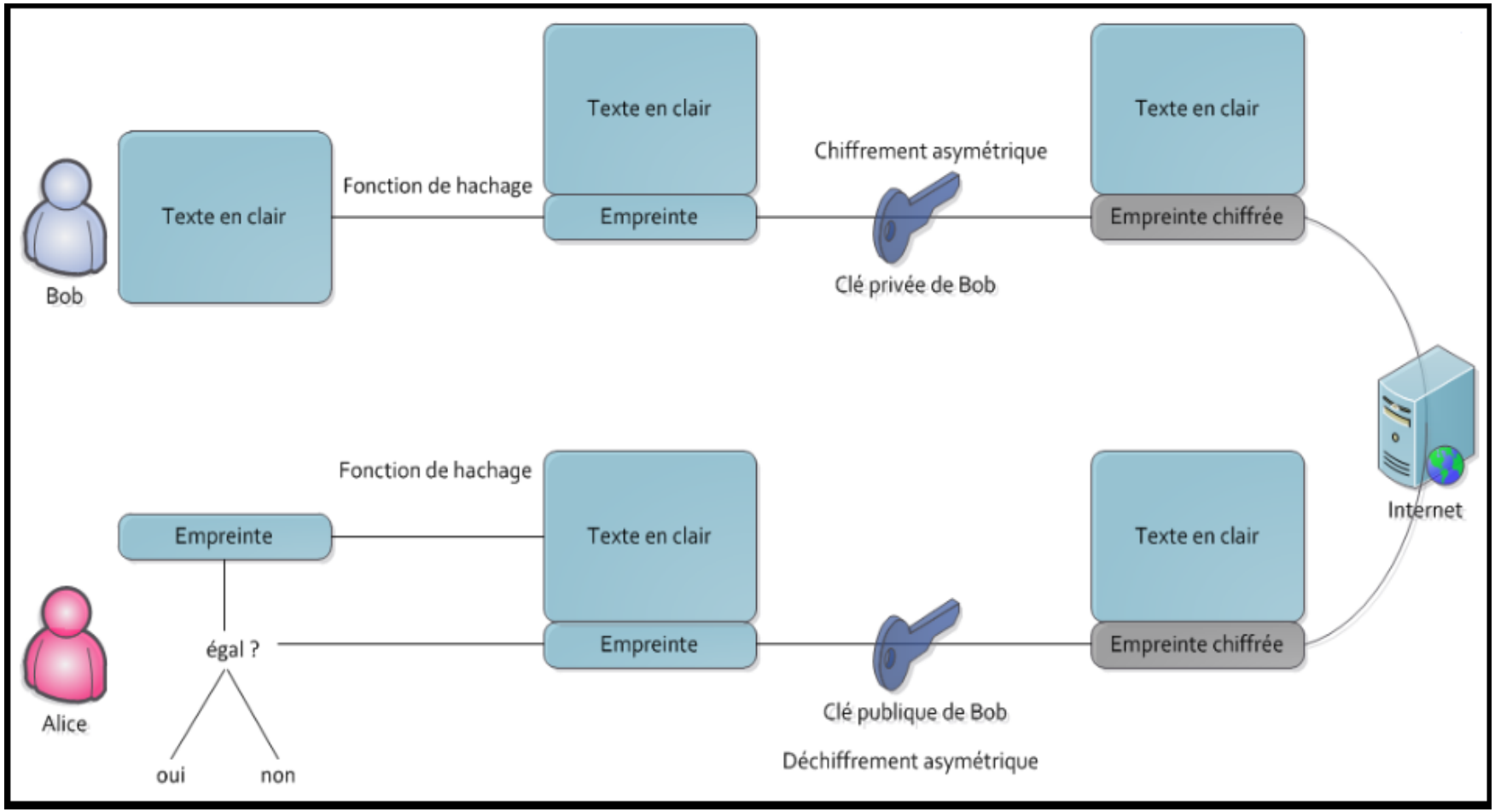
- **250 millions d'euros de préjudices liés à la fraude**

ATTENTION

La signature électronique n'est pas simplement l'apposition d'une image numérisée de la signature manuscrite, sur un document numérique, elle consiste en l'usage de procédés cryptographiques, permettant de **faire le lien entre l'identité du signataire et le contenu du document** et de le rendre intègre, pour interdire sa falsification ultérieure.

A ne pas confondre avec la signature manuscrite sur tablette numérique qui tient compte de la pression appliquée au stylet et de la vitesse d'écriture.

PRINCIPE DE FONCTIONNEMENT



A RETENIR

Pour faire le lien entre l'identité du signataire et le contenu du document, et rendre le tout intègre pour interdire sa falsification ultérieure, la seule technique existante à ce jour consiste en l'utilisation de deux outils informatiques : **le certificat électronique** délivré par une « autorité de certification », et l'**application de signature électronique**.

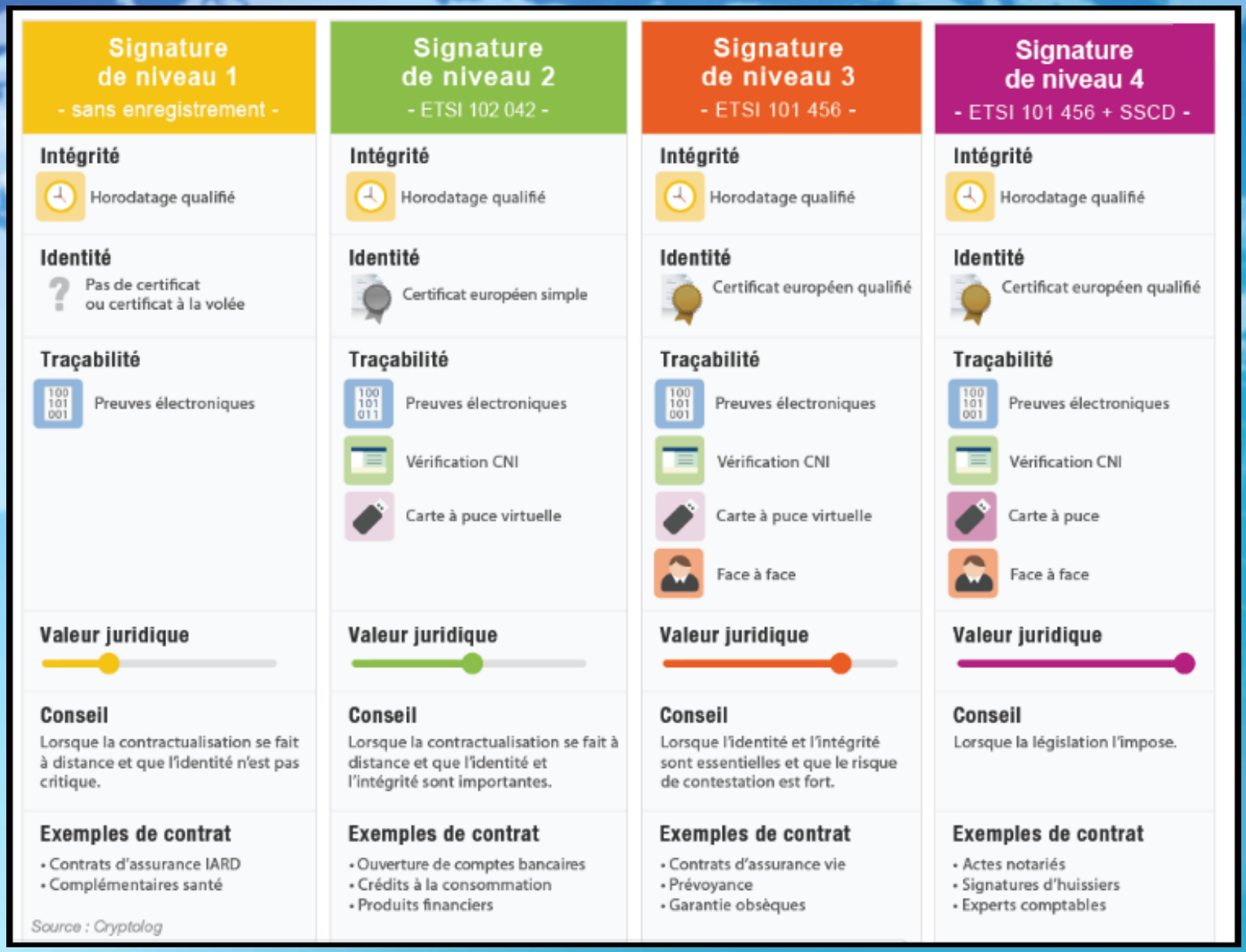
Document à signer

Certificat électronique

Application de signature électronique

Signature électronique

DES NIVEAUX DE SECURITE VARIABLES



LA VALEUR LEGALE DE LA SIGNATURE ELECTRONIQUE

LA SIGNATURE ELECTRONIQUE DANS LES ENQUETES

- **L'identité et l'authenticité** du signataire
- **L'intégrité** du document signé (cohérence entre les données envoyées et celles reçues**)**
- **La non-répudiation** (preuve fiable prouvant l'envoi des données par l'expéditeur)
- Complément possible par **l'horodatage électronique**

LES PRINCIPAUX BÉNÉFICES DE LA SIGNATURE ÉLECTRONIQUE ?

- La possibilité **de signer un document sans l'imprimer** (économie de papier)
- La possibilité **d'envoyer le document par e-mail** (économie d'impression, affranchissement, traitement du papier)
- La possibilité **de signer un document sans se rencontrer** (réduction des déplacements, gain en productivité et en fluidité)
- La possibilité **de conserver le document au format numérique** (simplification et suppression de l'archivage papier)
- Les formulaires électroniques téléchargés sur Internet sont pré-remplis et réutilisables (gain de temps)
- Une image moderne et des opportunités d'échanges à l'international

LES APPLICATIONS DANS LA LUTTE CONTRE LA FRAUDE

- Usurpation d'identité (Fraude au Président, la fraude au fournisseur, aux loyers, aux coordonnées bancaires, le Social Engineering (AMF)...
- Falsification de documents officiels.
- Sécurise les moyens de paiement
- Tout paiement peut faire l'objet d'une signature électronique : virements domestiques (paye, notes de frais, règlements fournisseurs), virements internationaux, virements de trésorerie, prélèvements clients, etc.
- La fin de la validation des virements par Fax.
- (La fin du fax de confirmation des paiements en EBICS TS* est annoncée fin 2016)

* Electronic Banking Internet Communication Standard Transport & Signature

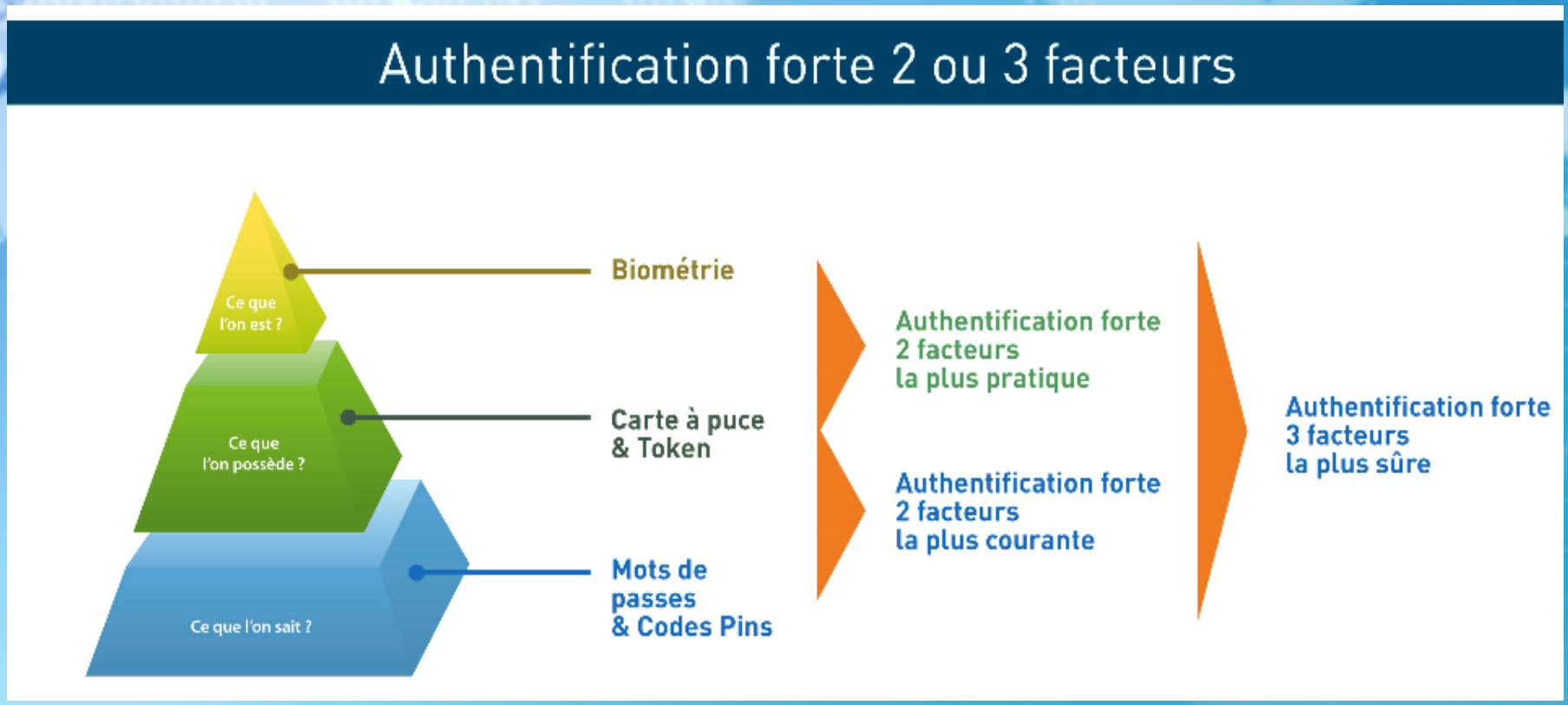
LE FUTUR

- **Les caractéristiques biométriques des signatures renforcent l'authenticité d'un cran** – L'identité du signataire peut être confirmée par des données biométriques propres à une signature, comme la vitesse d'écriture et les niveaux de pression

- Avec une croissance annuelle de 50% selon Gartner, la dématérialisation est au cœur de l'économie numérique

- L'explosion du marché des tablettes ne va faire qu'accélérer ce phénomène

L'AUTHENTIFICATION

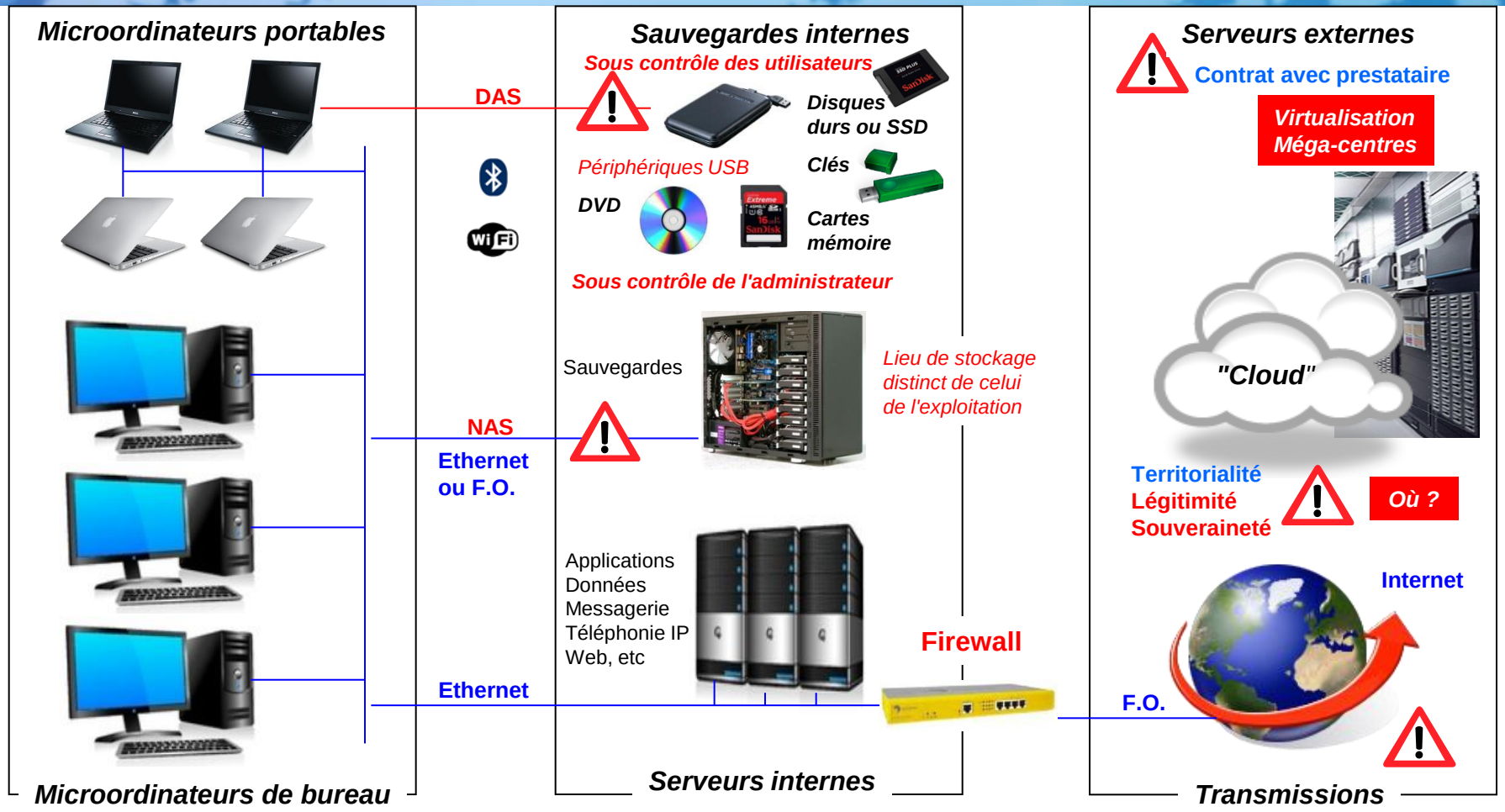


… POURTANT DES SOLUTIONS EXISTENT

Protection des données : caractéristiques et planification des sauvegardes

Daniel GUINIER

L'INFORMATIQUE DE L'ENTREPRISE



Les sauvegardes devront être administrées et contrôlées de façon centralisée.

DAS (Direct Attached Storage) ou unité de stockage en connexion directe ; **NAS** (Network Attached Storage) ou unité de stockage connecté en réseau.

ELEMENTS A PRENDRE EN COMPTE

Serveurs

Attention aux médias de sauvegarde connectés !

Microordinateurs portables unités centrales et autres objets

En interne

Lieux différents distants
Sécurité physique
Sécurité logique

Dispositif automatique
Supervision et contrôle
Qualité de service (SLA)
Garantie pour le PRA

Externalisation

Contrat

Serveurs data-centres

"Cloud"

Souveraineté
Territorialité

Les sauvegardes des postes de travail et des serveurs devront être planifiées et répertoriées, l'intégrité formellement vérifiée et la sécurité CID maintenue.

TECHNOLOGIES VERSUS DEFAILLANCES

- **Haute disponibilité - redondance et sauvegardes**
  - Systèmes tolérants aux pannes
  - Réplication : unités de stockage et canaux fibre optique (F.O.)
  - Sauvegardes classiques, robotisées ou *"cloud"*

RAID	Synchrone	Asynch.	Sauvegarde	Type de défaillance
Oui	Oui	Oui	Oui	Panne matérielle
	Oui	Oui	Oui	Sinistre physique
		Oui	Oui	Dysfonctionnement logique
		Oui	Oui	Erreurs opératoires
			Oui	Sinistre logique
			Oui	Pollution de données, virus, ransomware

Ces technologies jouent un rôle complémentaire en répondant à des objectifs différents.

SAUVEGARDES : L'ESSENTIEL…

- **Utilité des sauvegardes**
  - Restaurer des fichiers et des dossiers supprimés ou corrompus
  - Restaurer un système corrompu ou ne pouvant plus démarrer
  - Permettre la reprise d'activité après sinistre dans le **cadre d'un PRA**
- **Sauvegardes physiques** ***- secteur par secteur***
  - Sauvegarde de partitions, *pouvant exclure les secteurs non alloués*
  - Image exacte de l'intégralité du disque, *dénommée "clone"*
- **Sauvegardes logiques** ***- fichiers et arborescence***
  - Sauvegardes complètes
  - Sauvegardes différentielles
  - Sauvegardes incrémentales

Les sauvegardes peuvent être compressées et chiffrées, mais avant tout, elles doivent être planifiées et validées pour être utilisables.

SAUVEGARDES LOGIQUES

- **Sauvegardes complètes**
  Tous les fichiers
  présents à la création de cette sauvegarde

- **Sauvegardes différentielles**
  Fichiers modifiés
  depuis la **dernière sauvegarde complète**

- **Sauvegardes incrémentales**
  Fichiers modifiés
  depuis la **dernière sauvegarde**

Une sauvegarde différentielle requiert moins de temps et d'espace qu'une sauvegarde complète mais plus qu'une sauvegarde incrémentale.

PLANIFICATION DES SAUVEGARDES

- **Sauvegardes journalières** **J**

  chaque jour ouvré à l'horaire prévu sauf vendredi

- **Sauvegardes hebdomadaires** **H**

  le vendredi sauf celui de la sauvegarde mensuelle

- **Sauvegardes mensuelles** **M**

  le dernier vendredi de chaque mois

- **Sauvegardes sur événement**

  lors d'un évènement prévu et d'un incident

Vendredi pour les sauvegardes **H**ebdomadaires et **M**ensuelles
Périodes de rétention personnalisées pour chaque type de sauvegarde

Echantillon sur un mois

Lu	Ma	Me	Je	Ve
J	J	J	J	H
J	J	J	J	H
J	J	J	J	H
J	J	J	J	M

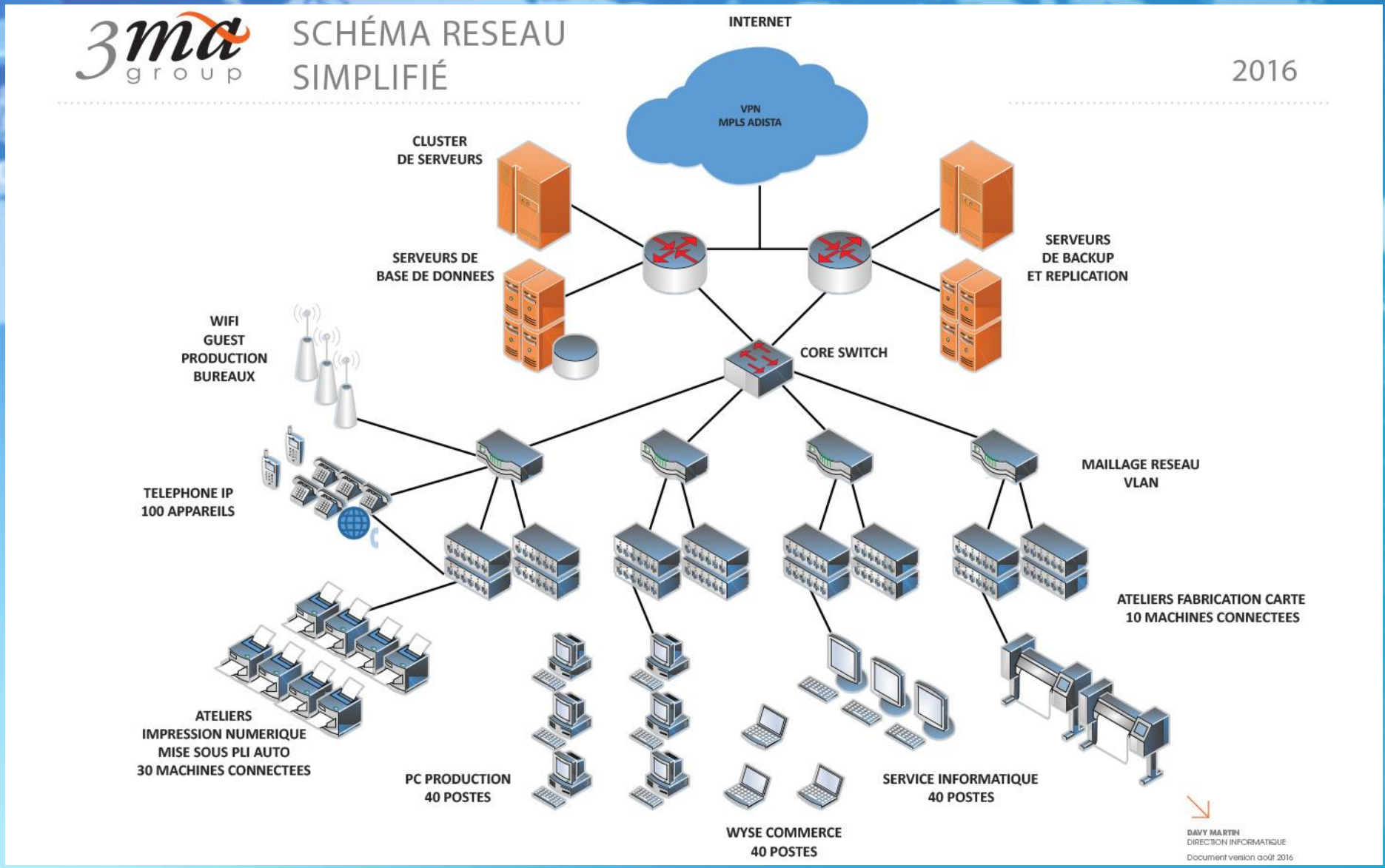
12 sauvegardes mensuelles permettront de couvrir une année complète, avec 4 journalières et 3 hebdomadaires en plus.

… POURTANT DES SOLUTIONS EXISTENT

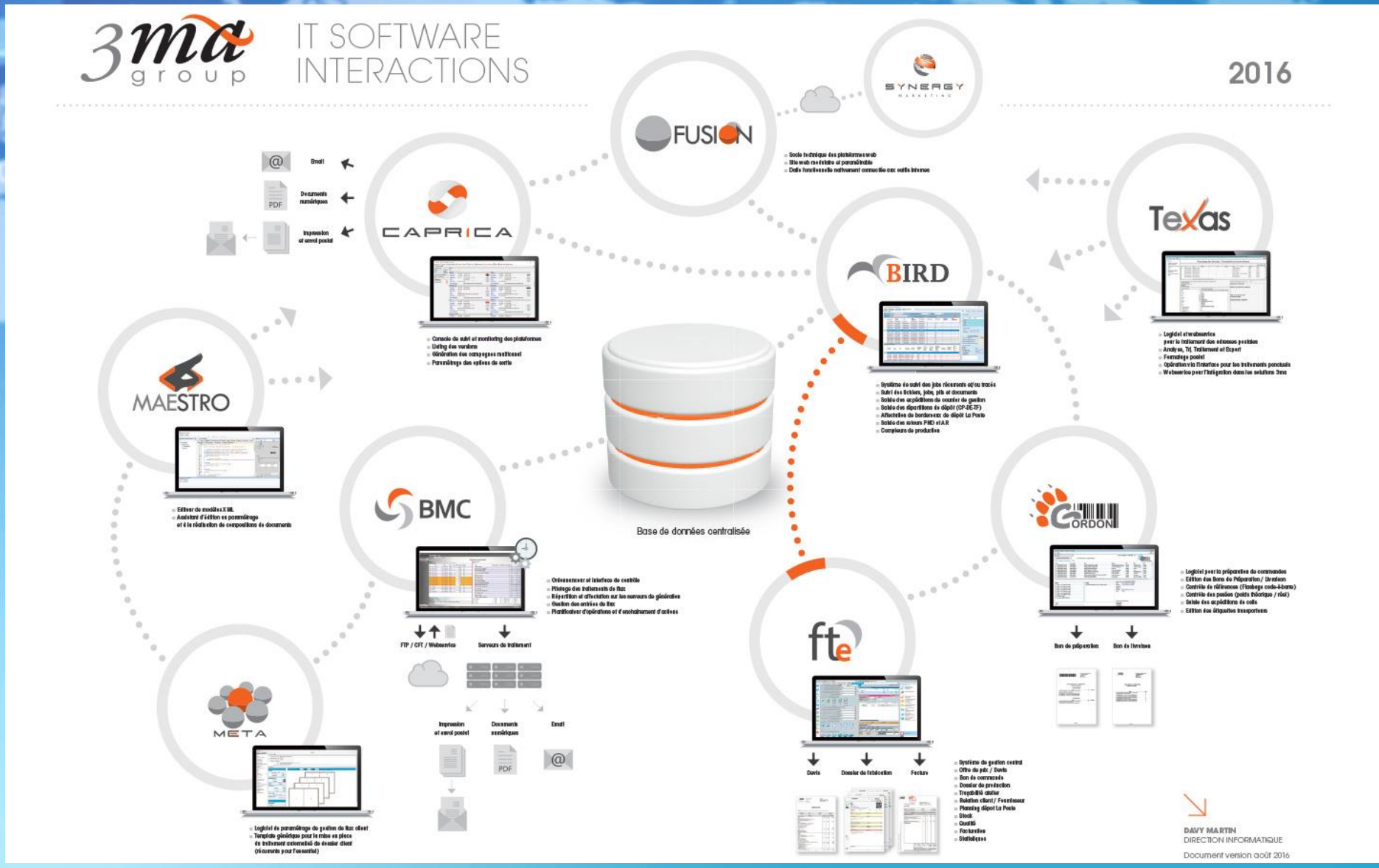
Tentative d'intrusion et de blocage d'une entreprise par un « Ransomware »

Laurent SCHMERBER

INFRASTRUCTURE INFORMATIQUE



SYSTÈME D'INFORMATION



L'ATTAQUE DE LOCKY

- 24/02/2016 **13h30 – Ralentissements**
  - Le service infra est alerté de gènes par les utilisateurs
  - L'équipe développement est informée et observe des anomalies fichiers
  - Les deux équipes identifient et ciblent le problème : Locky
- 24/02/2016 **14h00 – Périmètre impacté**
  - Information de la direction générale
  - Mise en place immédiate du Plan de Sécurité
  - Mise hors réseau préventive **SANS** éteindre les serveurs / machines
- 24/02/2016 **14h30 – Consultation Expert**
  - Information à la Gendarmerie et échange avec Daniel Guinier
  - Décision de couper l'intégralité des liaisons entre serveurs
  - Etablissement du bilan des atteintes et des sauvegardes sûres
- 24/02/2016 **15h00 – La source**
  - Identification et confirmation de l'origine de l'attaque
- 24/02/2016 **16h00 – Société à l'arrêt**
  - Information d'interruption de service à la clientèle
  - Mise en congé des personnels

LA REPONSE

- 24/02/2016 **17h00 – La rançon**
  - Visite de la Brigade de Rouffach (ADJ Kuster)
  - Information au N-Tech qui confirme les bonnes pratiques appliquées
  - Rançon demandée de 10 bitcoins -> Plus de 5 000 Euros
- 24/02/2016 **19h00 – Etat des lieux**
  - Fin des test de sauvegardes
  - Analyses des matériels
- 25/02/2016 **0h00 – Restauration**
  - Le service infra débute les réinstallations
- 25/02/2016 **7h00 – Contrôles et Patience**
  - 80% des serveurs sont opérationnels et recettés
- 25/02/2016 **9h30 – Succès**
  - 100% des serveurs sont opérationnels et recettés
  - Victoire des équipes informatique au détriment de la rançon

… POURTANT DES SOLUTIONS EXISTENT

QUESTIONS
RÉPONSES

CONFÉRENCE DE CLÔTURE

- **Marc WATIN AUGOUARD**

  Ancien inspecteur général des armées

  Directeur du centre de recherche de l'école des Officiers de la Gendarmerie Nationale

LE SALON EUROPÉEN DE LA CONFIANCE NUMÉRIQUE

9ème Forum International de la Cybersécurité – FIC 2017

Smarter security for future technologies

Le 24 et 25 janvier 2017

REMERCIEMENTS

L’association AD HONORES Réseau Alsace

REMERCIEMENTS : L'ÉQUIPE

LT Nadia BOUGHANI

CL Patrick DA COSTA

CDT Catherine DELASALLE

Emmanuelle HAASER

Perle KREBS

Daniel GUINIER

Ludovic HAYE

Johan MOREAU

Didier SCHERRER

Laurent SCHMERBER

Véronique WADEL

Jonathan WEBER

REMERCIEMENTS

- **L'équipe de l'INEDIT THEATRE**

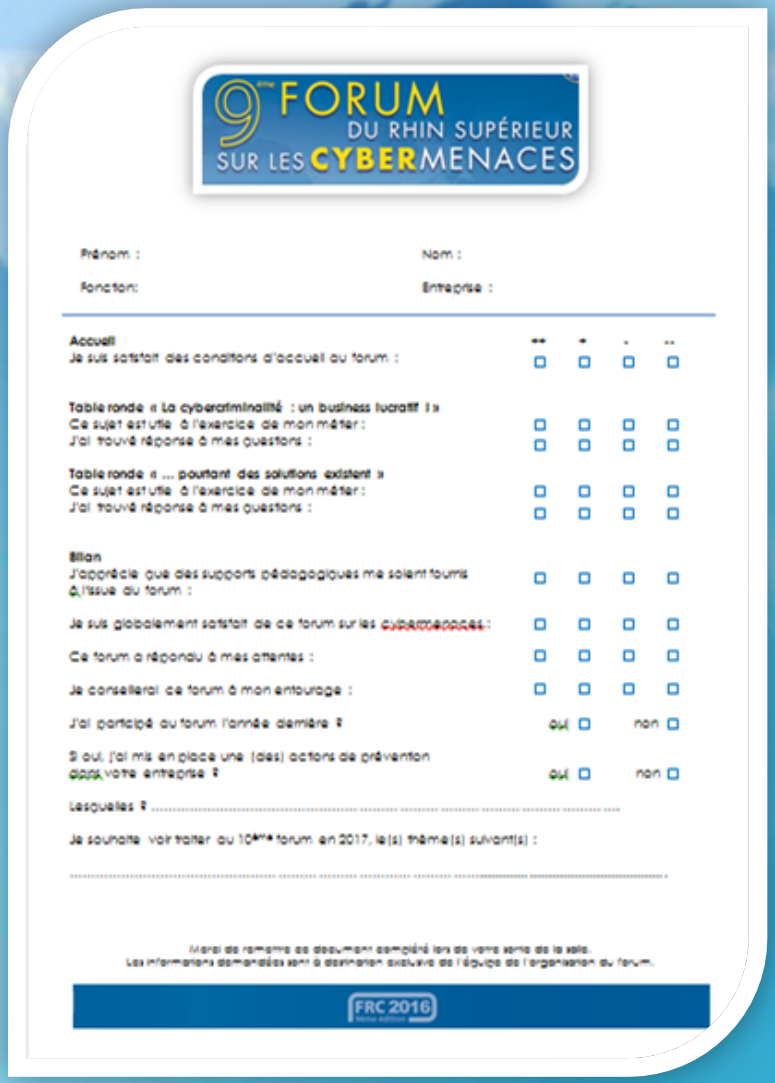
  Camille COMPARON

  Marko MEYERL

- **L'illustrateur**

  Laurent SALLES

FICHE D'EVALUATION



9ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Prénom : Nom :

Fonction: Entreprise :

	**	*	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « La cybercriminalité : un business lucratif ! »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « ... pourtant des solutions existent »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Bilan				
J'apprécie que des supports pédagogiques me soient fournis à l'issue du forum :	☐	☐	☐	☐
Je suis globalement satisfait de ce forum sur les cybermenaces :	☐	☐	☐	☐
Ce forum a répondu à mes attentes :	☐	☐	☐	☐
Je conseillerai ce forum à mon entourage :	☐	☐	☐	☐

J'ai participé au forum l'année dernière ? oui ☐ non ☐

Si oui, j'ai mis en place une (des) actions de prévention dans votre entreprise ? oui ☐ non ☐

Lesquelles ? .....

Je souhaite voir traiter au 10ème forum en 2017, le(s) thème(s) suivant(s) :

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

FRC 2016

DOCUMENTS A VOTRE DISPOSITION

RENDEZ-VOUS

10ème Forum du Rhin Supérieur sur les Cybermenaces

7 novembre 2017

www.frc.alsace

@cybermenaces

« Le succès n’est pas final

L’échec n’est pas fatal

C’est le courage de continuer qui compte »

Winston Churchill