LA SÉCURITÉ DES SYSTÈMES D'INFORMATION NUMÉRIQUE DES COLLECTIVITÉS LOCALES

Conférence :
Centre de Formation des Maires et des Elus Locaux de l'Hérault
Janvier 2018

Par Thierry ROLLAND
Directeur général des services d'une commune touristique
Directeur délégué d'un office de tourisme
Chargé d'enseignement Université de Montpellier
Conférencier Université de Lyon
IHEDN

LE CONTEXTE JURIDIQUE

Les collectivités locales sont tenues d'assurer la continuité du service public

Compte tenu de leur importance stratégique les collectivités doivent soit mettre en œuvre

- soit un plan de continuité d'activité,
- soit un plan de reprise d'activité

LE CONTEXTE JURIDIQUE

Le code de la sécurité intérieure dispose que :

« la sécurité est un droit fondamental des libertés individuelles et collectives.

L'Etat a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect de lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens.

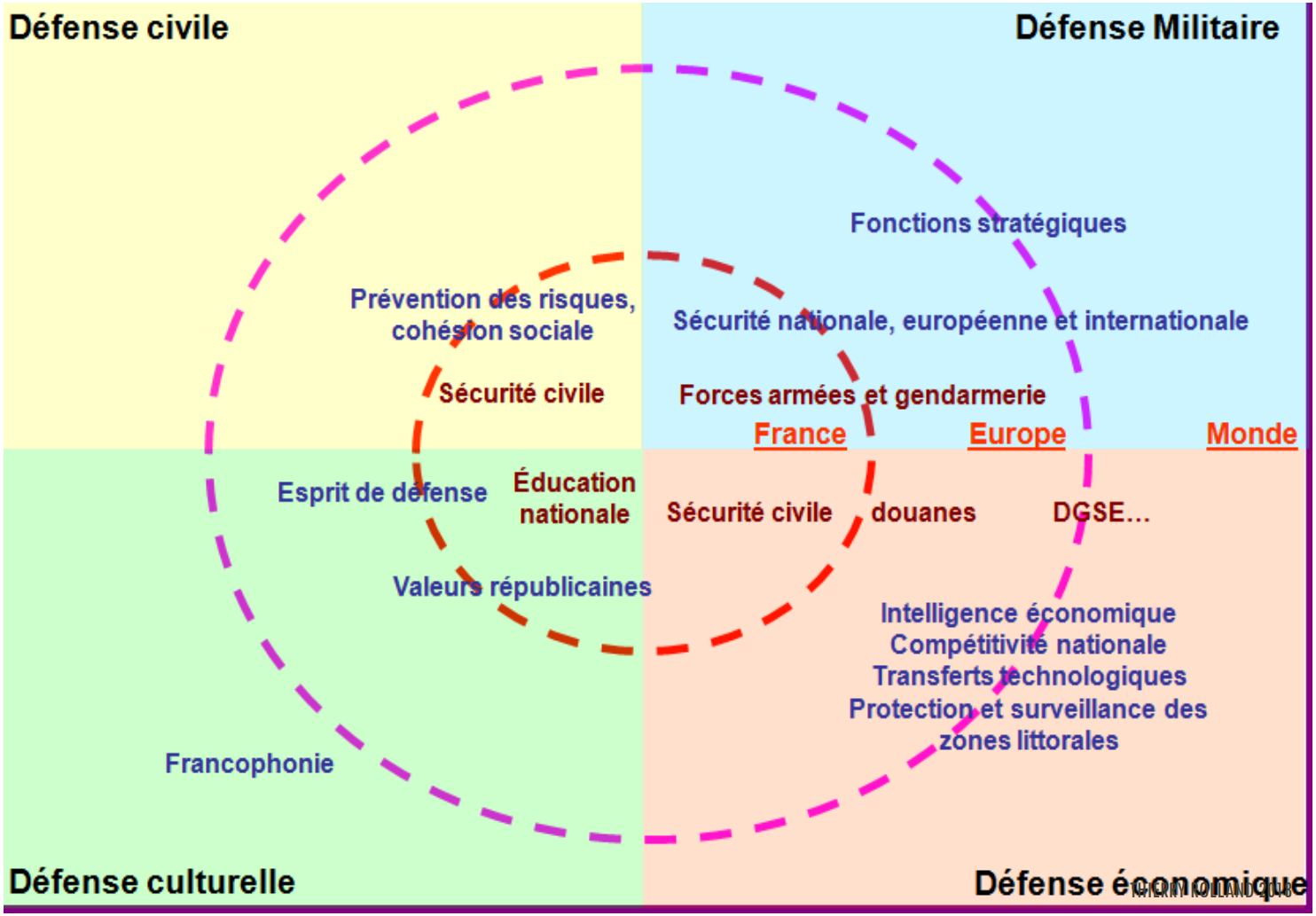
Il associe à la politique de sécurité (…) les collectivités territoriales (…)

LE CONTEXTE JURIDIQUE

La sécurité des personnes et des biens est une préoccupation ancienne et permanente de l'Etat et des acteurs publics.

S'inscrivant dans le concept de défense globale, une déclinaison territoriale est celle des risques urbains.

LE CONTEXTE JURIDIQUE



LE CONTEXTE JURIDIQUE

Un environnement juridique méconnu

La sécurité n'est pas seulement une affaire de voie publique. Des menaces pèsent aujourd'hui sur les communications et les échanges de données des administrations et entreprises des pays développés. La lutte contre la cyber criminalité, est prise très au sérieux par les autorités.

Elle doit être mise en œuvre au niveau local

LE CONTEXTE JURIDIQUE

Un risque complexe issu d'aléas directs et indirects

Aléas naturels ayant des conséquences sur l'électricité, les télécommunications…

Aléas industriels sur les moyens de télécommunications…

Aléas anthropiques internes et externes : mauvaises pratiques et malveillance…

UNE RÉGLEMENTATION MÉCONNUE

Sensibilité	Textes	Entités concernées
Informations secret de la défense nationale	IGI 1300 IGI 2100 / 2102 II 920 II 300	Entités privées ou publiques concernées par la gestion d'information liée au secret de la défense nationale
Informations Diffusion restreinte	Instruction n°901 sur la protection des SI sensibles (partie 1 + partie 2)	Entités publiques ou privées qui traitent des informations de mention « Diffusion Restreinte » Entités mettant en oeuvre des zones à régime restrictif (ZRR) et concernées par les spécialités les plus sensibles dans le cadre du dispositif relatif à la protection du potentiel scientifique et technique de la Nation
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
	II 300 – Annexe 2	Entités publiques ou privées qui traitent des informations de mention

UNE RÉGLEMENTATION MÉCONNUE

Informations sensibles	Instruction n°901 sur la protection des SI sensibles (partie 1)	Entités publiques ou privées soumises à la réglementation relative à la PPST pour leurs SI liés à une ZRR.
	PSSIE	Administrations de l'État
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
	II 300 – Annexe 2	Administrations de l'État
Informations peu sensibles	PSSIE	Administrations de l'État
	RGS	Autorités administratives échangeant des informations avec les usagers et entre autorités administratives
Informations liées à une réglementation spécifique	Exemples :Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation	En fonction du texte

UNE RÉGLEMENTATION MÉCONNUE

Le référentiel général de sécurité (RGS) est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.

Autorité administrative demanderesse	Service	Lien vers de certificat validé	Type de certificat	Niveau de sécurité	Prestataire de service de certification électronique	Autorité de certification	Date de validation
Commission nationale de linformatique et des libertés (CNIL)	Service de dépôt de plainte en ligne	https://www.plaintes.cnil.fr/plaintes/plainte.action↗	Authentification serveur	*	Certinomis	Certinomis Serveur Authentification OID : 1.2.250.1.86.2.2.2.20.1	22/02/12

UNE RÉGLEMENTATION MÉCONNUE

Plan de maintien d'activité

Plan de reprise d'activité

Le choix stratégique dépend de **l'activité exercée** et du **choix coût / avantage** de la solution

Exemple : chute du serveur - été 2011 à 13h

la paye avait été faite à 11h

UNE SITUATION BIEN CONNUE ?

Une appréciation relative de la situation

J'ai tout sous contrôle !

Antivirus

Pare-feu

Enjeux réduits

Vulnérabilité maîtrisée

Risques minimes

Une réalité plus complexe

Aléas / enjeux / vulnérabilités /risques

- Comptabilité et RH
- Service social
- Etat-civil
- Administration générale
- Vidéo-protection
- Alarmes
- Télésurveillance
- Distribution d'eau et d'énergies
- Communication
- Entretien des véhicules
- Téléphonie : voix sur IP
- Réseaux sans fil
- Contrôle d'accès des personnes physiques
- Télé-opération de surveillance personnes vulnérables
- Applicatifs métiers

IDENTIFIER LES MENACES

Hameçonnage & ingénierie sociale
Fraude interne
Intrusion informatique
Virus informatique
Déni de service

Cryptolocker

Virus

Pourriels (SPAM)

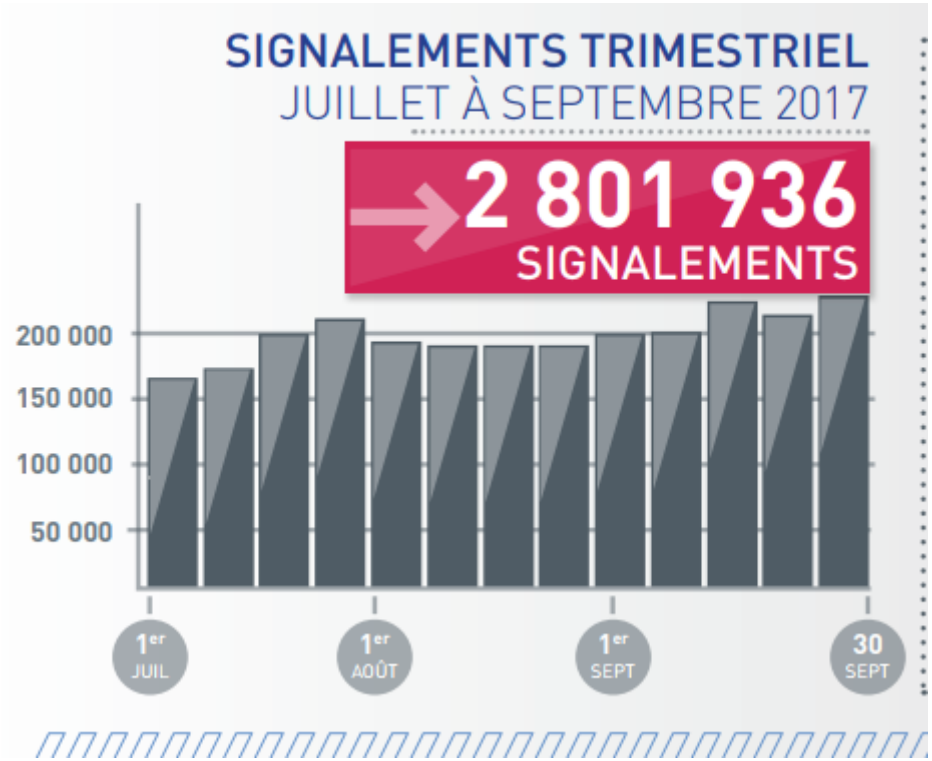
Publicités

Défaillances de programmes

Arnaque au président (ingénierie sociale)

IDENTIFIER LES MENACES
LES SPAM OU POURRIELS

Quelques chiffres

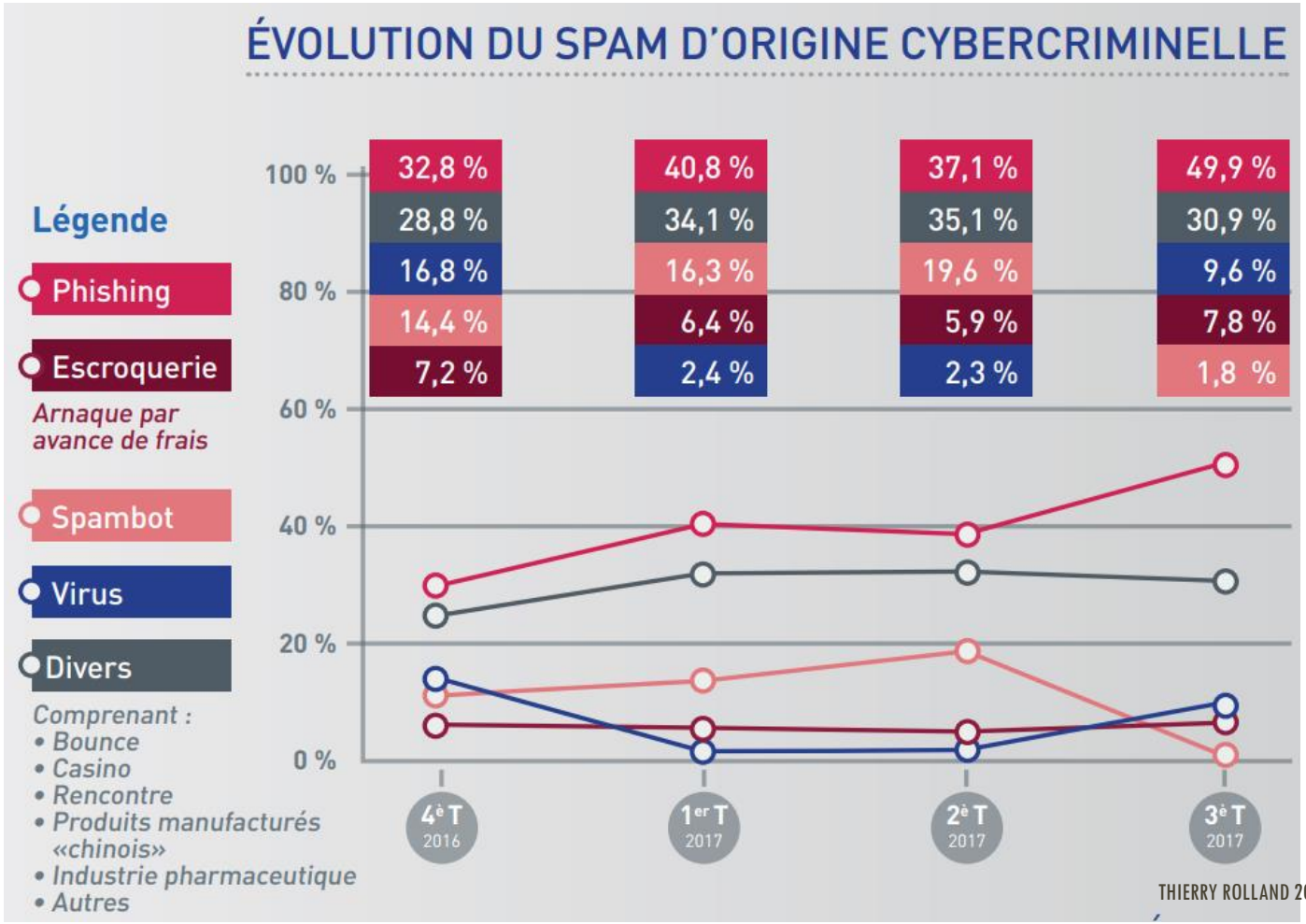


LE TOP 10 DES OBJETS

n°	Objet
1	1 commande d'encre = 1 casque de réalité virtuelle offert
2	Loi (*nom*) : Isoler votre maison pour 1 euro
3	Bénéficiez de l'aide de l'État pour payer vos impots
4	(*Assureur*) vous fait decouvrir la Convention Obseques
5	Estimation et vente rapide de votre auto
6	Surprenez ceux qui vous entourent, maigrissez sans effort
7	Regardez comment bien dormir
8	Votre adoucisseur d'eau livré et posé gratuitement
9	Investissez avec nous
10	Découvrez nos PROMOS à durée limitée

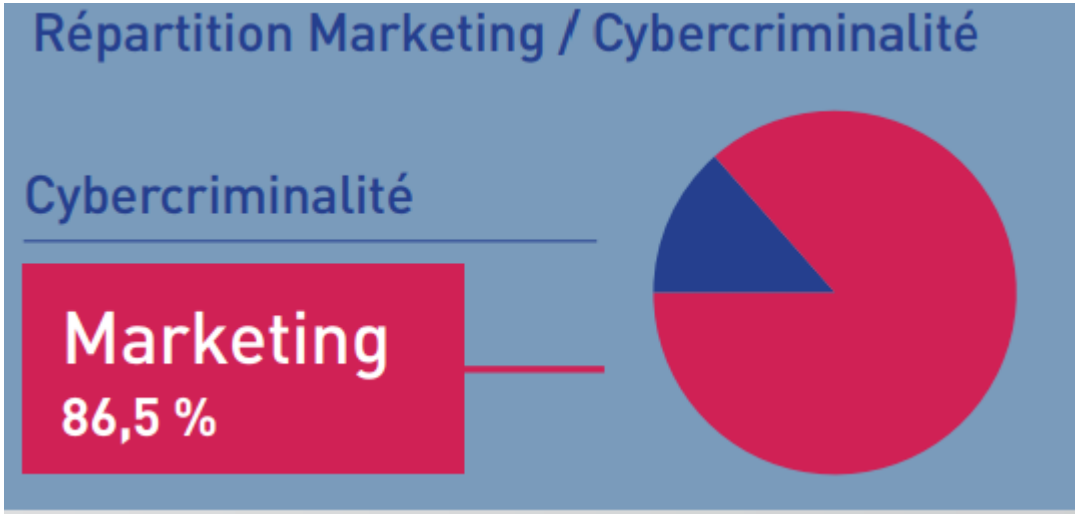
IDENTIFIER LES MENACES
LES SPAM OU POURRIELS

Quelques chiffres



IDENTIFIER LES MENACES
LES SPAM OU POURRIELS

Quelques chiffres



EXEMPLE RÉCENT N°1

Vulnérabilit

Adobe Flash Player

Adobe Flash Player est un contrôle ActiveX, un plugin ou un lecteur multimédia autonome utilisant la technique Flash. La première version de la branche 10 est sortie en octobre 2008, peu après la sortie de la suite CS4 des logiciels Adobe.

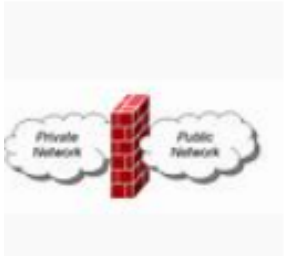
Référence	CERTFR-2016-ALE-004
Titre	Vulnérabilité dans Adobe Flash Player
Date de la première version	15 juin 2016
Date de la dernière version	16 juin 2016
Source(s)	Bulletin de sécurité Adobe apsa16-03 du 14 juin 2016
Pièce(s) jointe(s)	Aucune

Une vulnérabilité a été découverte dans *Adobe Flash Player*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Dans son bulletin d'alerte APSA16-03 (cf. Section Documentation), Adobe annonce qu'une vulnérabilité jugée critique affecte les versions 21.0.0.242 et antérieures de son Flash Player, et ce sur toutes les plateformes.

Adobe prévient également que cette vulnérabilité est activement exploitée dans le cadre d'attaques ciblées.

EXEMPLE RÉCENT N°2

Vulnérabilité pare-feu CISCO : **objet SYSTEME**



Un pare-feu, est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention … +

Référence	CERTFR-2016-ALE-005
Titre	Multiples vulnérabilités dans les pare-feux Cisco
Date de la première version	18 août 2016
Date de la dernière version	5 septembre 2016
Source(s)	Bulletin de sécurité cisco-sa-20160817-asa-snmp Cisco du 17 août 2016 Bulletin de sécurité cisco-sa-20160817-asa-cli Cisco du 17 août 2016
Pièce(s) jointe(s)	Aucune

Le samedi 13 août, des attaquants se faisant appeler les Shadow Brokers ont publiquement révélé des outils offensifs, qu'ils affirment provenir d'Equation, un groupe d'élite lié à la NSA.
Parmi ces outils se trouve du code malveillant dont la fonction est d'exploiter des vulnérabilités dans les pare-feux Cisco afin d'en prendre le contrôle.
Dans ses bulletins de sécurité cisco-sa-20160817-asa-snmp et cisco-sa-20160817-asa-cli (cf. Section Documentation), l'équipementier énumère la liste de produits pour lesquels un correctif est disponible.
Le CERT-FR recommande de durcir ses équipements tout en respectant les bonnes pratiques (cf. Section Documentation).
Des règles de détection réseau sont également disponibles, soit de manière payante (Cisco, cf. Section Documentation), soit à titre gratuit (Emerging Threats, cf. Section Documentation).

EXEMPLE RÉCENT N°3

Vulnérabi Joomla!

Joomla! est un système de gestion de contenu libre, open source et gratuit. Il est écrit en PHP et utilise une base de données MySQL. Joomla! inclut des fonctionnalités telles que des flux RSS, des news, une version imprimable des pages… +

Une vulnérabilité a été découverte dans *Joomla!*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

Une mise à jour de sécurité a été publiée aujourd'hui sur le site officiel de *Joomla!*.

Cependant, une société de sécurité informatique précise qu'une vague d'attaques provenant des adresses IP 146.0.72.83, 74.3.170.33, 93.179.68.167, 199.182.234.132, 185.15.185.17, 37.61.232.173 et 194.28.174.106 avait débuté avant la mise en ligne du correctif. En plus de ces adresses IP, des marqueurs de détection dans les fichiers de log sont fournis : la présence de la chaîne "JDatabaseDriverMysqli" ou de la chaîne "O:" dans l'entête HTTP User-Agent.

Le CERT-FR recommande, pour les utilisateurs de *Joomla!*, la mise à jour immédiate vers la version 3.4.6 ainsi que la recherche de la chaîne "JDatabaseDriverMysqli" dans le fichier de log ainsi que des connexions depuis les adresses IP 146.0.72.83, 74.3.170.33, 93.179.68.167, 199.182.234.132, 185.15.185.17, 37.61.232.173 ou 194.28.174.106.

EXEMPLE RÉCENT N°4

Vulnérabili

Mozilla Firefox

Mozilla Firefox est un navigateur web libre et gratuit, développé et distribué par la Mozilla Foundation avec l'aide de milliers de bénévoles grâce aux méthodes de développement du logiciel libre/open source et à la liberté du code source.

Référence	CERTFR-2016-AVI-355
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	21 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla mfsa2016-87 du 20 octobre 2016
Pièce(s) jointe(s)	Aucune

De multiples vulnérabilités ont été corrigées dans *Mozilla Firefox*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données.

EXEMPLE RÉCENT N°5

Vulnérabilité Oracle MySQL :

objet : base de données compta – RH – urbanisme – état civil

Référence	CERTFR-2016-AVI-351
Titre	Multiples vulnérabilités dans Oracle MySQL
Date de la première version	19 octobre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuoct2016-2881722 du 18 octobre 2016 Bulletin de sécurité Oracle cpuoct2016verbose-2881725 du 18 octobre 2016
Pièce(s) jointe(s)	Aucune

De multiples vulnérabilités ont été corrigées dans *Oracle MySQL*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et une atteinte à l'intégrité des données.

EXEMPLE RÉCENT N°6

Vulnérabilité CRYPTOLOCKER

objet : tous les fichiers

EXEMPLE RÉCENT N°7

Cela n'arrive pas qu'aux autres !

Répondre Répondre à tous Transférer

mer. 16/03/2016 09:32

info@palavaslesflots.com de la part de info@

Image transférée de: 0049203579

À thierry ROLLAND

Nous avons supprimé les sauts de ligne en surnombre dans ce message.

Message dgs@palavaslesflots.com_20160316_4443.zip (3 Ko)

Répondre à: info@palavaslesflots.com <info@palavaslesflots.com> Nom du périphérique: TRD Modèle de périphérique: MX-3114N
Emplacement: Non établi

Format de fichier: PDF MMR(G4)
Résolution: 204dpi x 196dpi

Le fichier joint est une image numérisée au format PDF.
Utilisez Acrobat(R)Reader(R) ou Adobe(R)Reader(R) d'Adobe Systems Incorporated pour visualiser le document.
Il est possible de télécharger Adobe(R)Reader(R) de l'adresse suivante:
Adobe, le logo Adobe, Acrobat, le logo Adobe PDF et Reader sont des marques déposées ou des marques commerciales d'Adobe Systems Incorporated aux Etas-Unis et dans les autres pays.

http://www.adobe.com/

AUTRES EXEMPLES

Répondre Répondre à tous Transférer

Votre Assurance Maladie <contact@exegesis.com.br> assure.ameli.fr 26/12/2017

Suivi remboursements ✓

Ce message a été envoyé avec l'importance Faible.
En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.
Cliquez ici pour télécharger des images. Pour protéger la confidentialité, Outlook a empêché le téléchargement automatique de certaines images dans ce message.

Sécurité sociale
L'Assurance Maladie

Bonjour ,

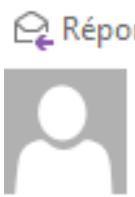
Apres les derniers calculs de votre assurance maladie , nous avons determine que vous etes admissible a recevoir un remboursement.

Consulter les demarches a suivre en : Formulaire de remboursement electronique

Consultez des maintenant la messagerie de votre compte ameli.

Avec toute mon attention,
votre correspondant de l'Assurance Maladie.

AUTRES EXEMPLES



Répondre Répondre à tous Transférer

réf.illimité <thiolieres.mairie@orange.fr> 0

Cher(e) abonné(e)

En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.

Bonjour,

Le numéro 0684111203 vous a laissé un message le 29/11/2017 à 17:15.
Pour le consulter, cliquez ici ou composez le 3103 depuis votre poste téléphonique.

.
Bien cordialement,
TEL:068548000
0384591265

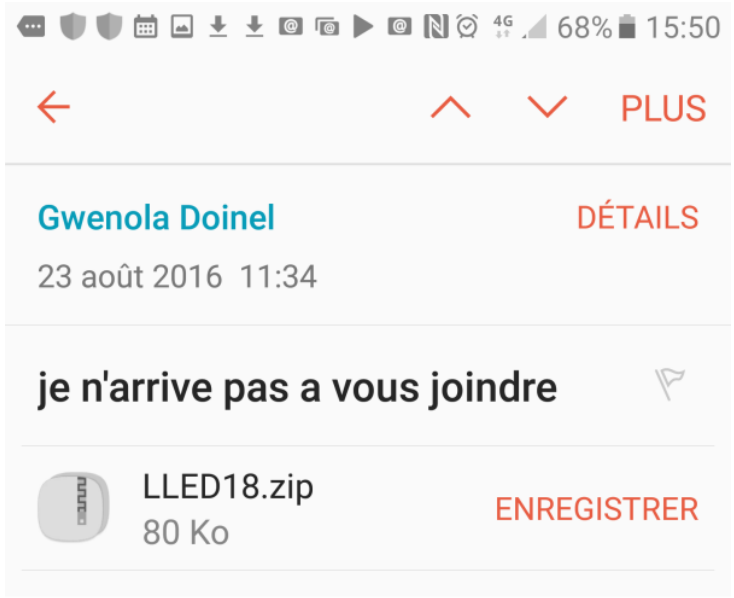
 # Adresse mairie :
Le bourg,
63600 Thiolières

 # Téléphone :
Tel : 0473823680
Fax : 0473823680

 # Courriels :
Secrétariat : thiolieres.mairie @ wanadoo.fr
webmaster : mairie.thiolieres @ gmail.com

AUTRES EXEMPLES

Cela n'arrive pas qu'aux autres !



Bonjour Thierry Rolland !

Toutes les modifications nécessaires ont été reportées sur le document. Les chiffres ont été corrigés.
Malheureusement, je n'arrive pas à vous joindre au numéro de téléphone suivant : 0467077314.
Vous trouverez le fichier en pièce jointe.
Veuillez s'il vous plaît en prendre connaissance.

Cordialement.

EXEMPLE RÉCENT N°8 (INGÉNIERIE SOCIALE)

PARKEON SAS- RIB 2017.pdf

Taille : 708 Ko

Dernière modification : lundi 12 juin 2017

Message PARKEON SAS- RIB 2017.pdf (708 Ko)

PARKEON

ST17110**0500249**

ORIGINAL :

08 JUIN 2017

COPIE :

Commune de Palavas-les –Flots
16 boulevard Maréchal Joffre
34250 Palavas-les-Flots

Attestation Changement de RIB

Intitulé : Fourniture, pose et maintenance d'horodateurs solaires pour la Commune de Palavas-les-Flots.

Référence :**16DST36**

EXEMPLE RÉCENT N°8 (INGÉNIERIE SOCIALE)

PARKEON SAS- RIB 2017.pdf

Taille : 708 Ko

Dernière modification : lundi 12 juin 2017

Message PARKEON SAS- RIB 2017.pdf (708 Ko)

Bonjour,

Je vous atteste par la présente du changement de coordonnées bancaires afin d'effectuer vos prochains paiements.

Veuillez trouver ci-dessous notre RIB pour enregistrement.

Pour tout complément d'information, veuillez nous contacter par mail à l'adresse suivante: **j.legrand@parkeon-finances.fr** ou par téléphone au **08 20 48 81 77**.

Cordialement,

Thierry Gonnet
Directeur Financier

Bertrand Barthelemy
PDG PARKEON SAS

PARKEON SAS au capital de 30.382.146 euros - Siège social 100 Avenue de Suffren, 75015 Paris – France
SIREN : 444 719 272 RCS PARIS.

EXEMPLE RÉCENT N°8 (INGÉNIERIE SOCIALE)

BNP PARIBAS

L'utilisation de ce relevé permet d'éviter les erreurs ou retards qui pourraient résulter d'indications incorrectes dans la transmission de vos références bancaires.

RELEVE D'IDENTITE BANCAIRE / IBAN

Partie reservée au destinataire du relevé

Titulaire du compte: **ASTORIA INVEST PARKEON SAS**

100 Avenue de Suffren
75015 Paris France

Domiciliation banque : **BNP PARIBAS**

3 Rue Sawa
02 670 VARSOVIE
POLOGNE

IBAN (International Bank Account Number) :	PL28 1600 1127 1838 9037 8000 0002
Code BIC (Bank Identifier Code) :	PPABPLPKXXX

ENJEUX

DESTABILISATION : enjeu économique

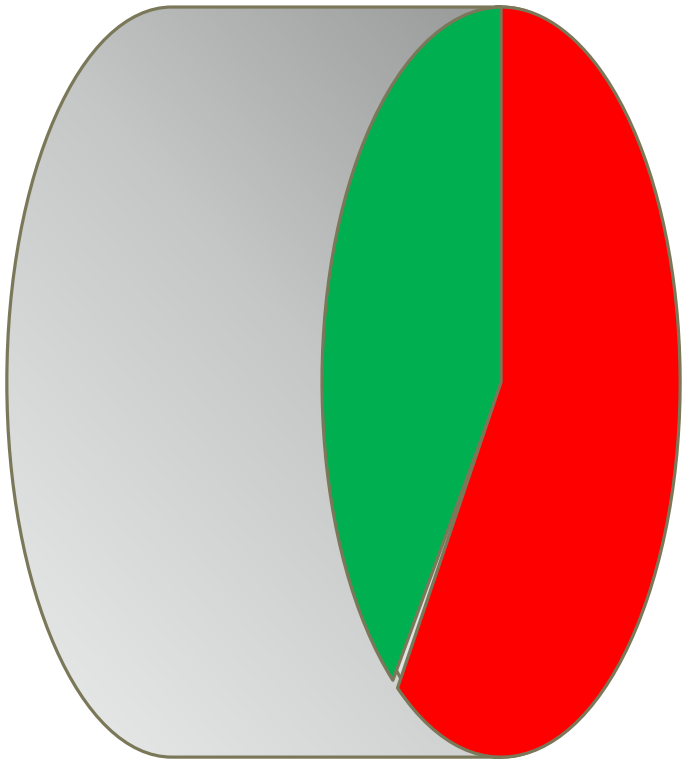
ESPIONNAGE : enjeu stratégique

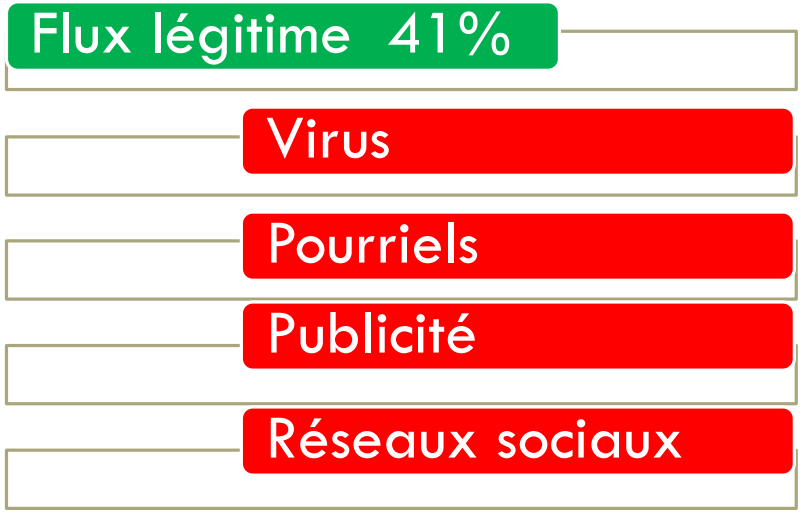
SABOTAGE : enjeu organisationnel

CYBERCRIMINALITE : enjeu financier

ENJEUX

BLOCAGE DU FLUX : enjeu économique





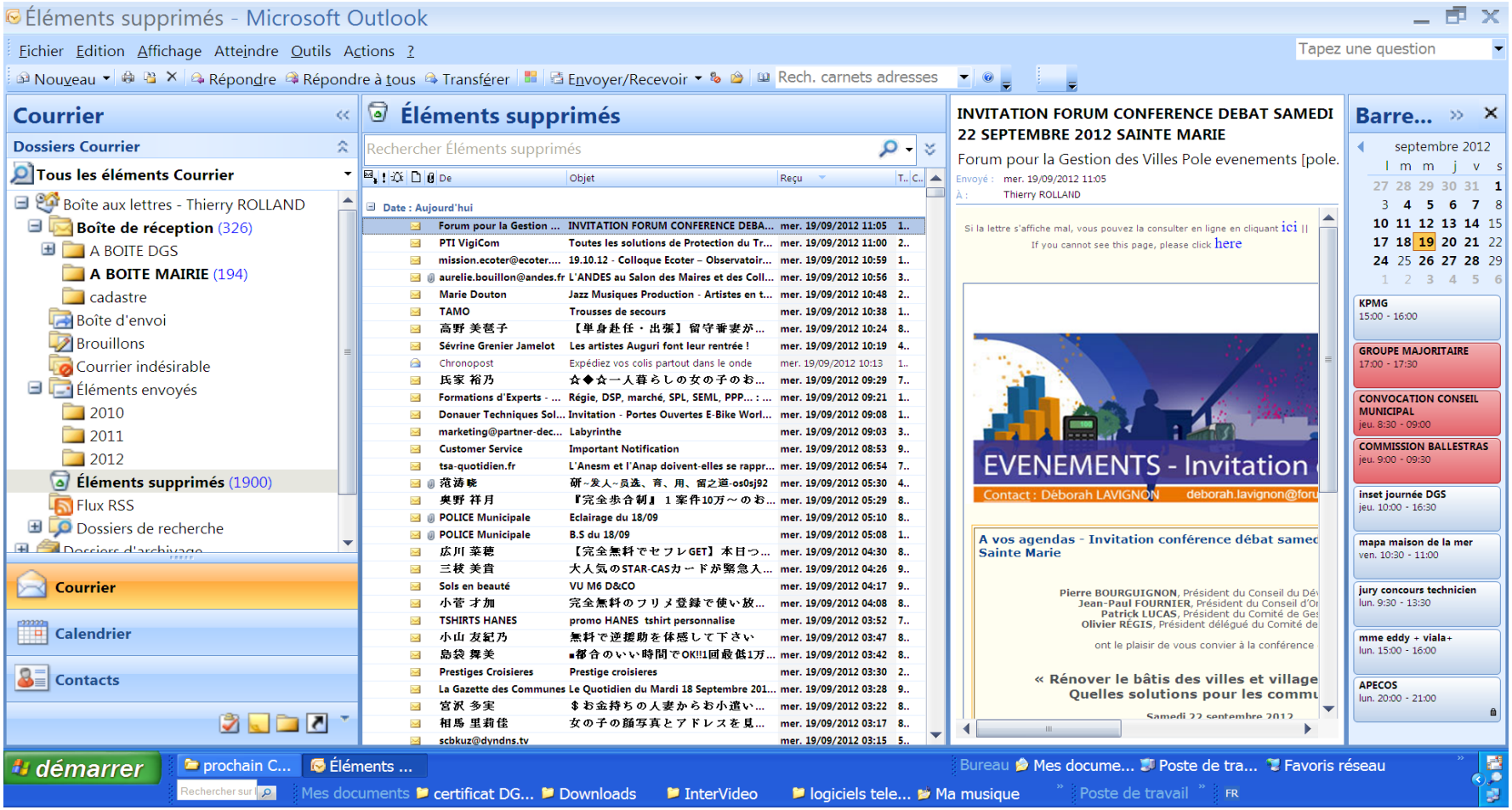
En 6 mois (mi avril – mi octobre 2016) :
30 551virus et 24 028 pourriels bloqués par *VADERETRO*.

En 1 an (2017) :
24 425 messages légitimes / 34 960 messages illégitimes

Débit internet utilisé à 59% pour des usages illégitimes.

ENJEUX

POURRIELS = perte de temps



Les pourriels bloqués permettent d'optimiser son temps

UN ACTEUR SUPPORT DE RÉFÉRENCE

L' ANSSI

Comme le précise la loi n°2013-1168 du 18 décembre 2013, « le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information », l'ANSSI, rattachée au secrétaire général de la défense et de la sécurité nationale.

UN GUIDE À TÉLÉCHARGER SUR LE SITE

SGDSN

VIGIPIRATE

PARTIE PUBLIQUE

OBJECTIFS DE CYBERSÉCURITÉ

UN GUIDE À TÉLÉCHARGER SUR LE SITE

GUIDE D'HYGIÈNE INFORMATIQUE

LES RÈGLES DE SÉCURITÉ

Définir une politique de sécurité

Définir une homologation de sécurité

Établir une cartographie des risques

Maintenir en conditions de sécurité

Respecter la journalisation

Réagir lors de la détection

Traiter les incidents

Traiter les alertes

Gérer les crises

Gérer les identités et accès

Administrer

Défendre en profondeur

Suivre des indicateurs

ADOPTER DE BONNES PRATIQUES

Réglementer les pratiques simples

Former les collaborateurs

Sensibiliser en permanence

Alerter

ADOPTER DE BONNES PRATIQUES

Réglementer les pratiques simples

Former les collaborateurs

Sensibiliser en permanence

Alerter

ADOPTER DE BONNES PRATIQUES

Réglementer les pratiques simples

Le comité technique a adopté une réglementation interne arrêtée par le maire et diffusée à tous les agents et les élus.

ADOPTER DE BONNES PRATIQUES

« Il est rappelé à l'ensemble du personnel que le matériel informatique mis à sa disposition n'a qu'une **finalité professionnelle**. Par conséquent**, l'usage privé** est strictement prohibé.

Il convient également de réglementer des **pratiques** professionnelles visant à **garantir la sécurité** du **réseau** et la **protection** des **données** professionnelles.

Il est rappelé que les **sites internets** ne sont pas toujours garantis ni dans leur **contenu** ni dans leur **forme,** que les **utilisateurs** doivent être **vigilants** sur ces points.

ADOPTER DE BONNES PRATIQUES

L'utilisation de matériels périphériques tels que les disques durs externes ou clés à mémoire flash (tel que clé USB, carte mémoire etc.) qui ne seraient pas fournis par la collectivité est strictement interdite. A fortiori, l'utilisation de **clé USB publicitaires** gratuitement offertes par un quelconque prestataire est rigoureusement prohibée.

Il est également interdit d'utiliser le matériel fourni par la ville pour **exploiter des données** ou **fichiers personnels** (photos, fichiers, films…).

Il est strictement **interdit** au personnel **d'installer des logiciels sur les postes clients sans l'accord préalable de l'entreprise de maintenance informatique**. Le téléchargement de logiciel ne peut intervenir qu'avec l'accord effectif du prestataire informatique.

ADOPTER DE BONNES PRATIQUES

Aucune modification de **droit d'accès ou d'architecture du réseau** ne peut intervenir sans **l'accord hiérarchique** et la **validation du prestataire informatique.**

Il est interdit de **désactiver les antivirus, « fire-wall »** ainsi que toute configuration pré-requise du poste client.

La **messagerie professionnelle** n'est destinée qu'à un usage professionnel. Le courriel ou la télécopie ayant la **valeur juridique d'un acte sous-seing privé,** il est vivement recommandé de procéder, d'une part, à **l'enregistrement du courrier arrivé et départ,** à la **conservation des données comme moyen de preuve,** de **respecter les délégations consenties** par le maire et d'autre part, de respecter la mise en forme des courriels, c'est-à-dire, en veillant à inclure une formule de politesse. A cet égard, une note précisera les formules selon les correspondants.

ADOPTER DE BONNES PRATIQUES

La consultation de la **messagerie personnelle est strictement interdite** sur les postes professionnels même en dehors des heures de travail.

La consultation des sites internets de type « **peer to peer** » (P2P, connexion d'égal à égal), « **streaming** » (diffusion en mode continu) même sur les sites à distribution gratuite ou légale est interdite.

Il est rappelé que le **téléchargement de données audio et vidéo** est protégé par la loi.

La collectivité n'engage pas sa responsabilité pour tout manquement au présent règlement et est susceptible d'engager celle de l'agent. »

ADOPTER DE BONNES PRATIQUES
ALERTES INTERNES

De: thierry ROLLAND
Envoyé: mercredi 16 mars 2016 14:23
Cc: Assistance Informatique
Objet: alerte faux messages internet
Pièces jointes: image001.png; image002.png

IMPORTANT

Bonjour,

Pour compléter mes précédentes circulaires, je vous informe qu'il y a des faux messages utilisant le suffixe @palavaslesflots.com

Il convient d'être prudent et cas de doute, appliquez la procédure déjà définie par mes précédents messages.

1) Exemple de faux message : l'adresse info@palavaslesflots n'existe pas en interne.

ADOPTER DE BONNES PRATIQUES
ALERTES INTERNES

2) Les attaques de virus utilisent le plus souvent les formats ZIP pour passer sous la vigilance des anti-virus.

3) Si vous regardez bien le message, ma propre adresse mail est imitée mais aucune adresse mail de la ville n'existe sous ce format, car c'est incohérent à la fin.

4) Le lien vers ADOBE est aussi une entrée du virus ; il ne faut donc pas cliquer sur ce type de lien hypertexte.

ADOPTER DE BONNES PRATIQUES
ALERTES INTERNES

N° 2) Je vous rappelle les bonnes pratiques en matière informatique :

1) Ne jamais se rendre sur des sites internets non professionnels
2) Ne jamais télécharger de données, films, photos, documents pdf ou autre à partir d'un site non fiable particulièrement depuis les sites de streaming même pour écouter de la musique
3) Ne pas ouvrir ou transférer de mail « humoristiques » comprenant des pièces jointes comprenant textes, photos, vidéos ou lien hypertexte
4) Ne pas utiliser votre ordinateur professionnel pour votre messagerie personnelle ou vos réseaux sociaux
5) Ne jamais raccorder votre téléphone personnel ou professionnel sur votre ordinateur même pour recharger la batterie. Un smartphone est un ordinateur à part entière et il n'est pas doté d'antivirus ou d'antispam.
6) Ne pas utiliser de clé USB publicitaire ou offerte par un tiers

Concernant les courriels :

1) Ne jamais ouvrir les mails dont l'expéditeur ou l'objet n'est pas clairement identifié. L'ajouter alors aux courriers indésirables.
2) Ne pas ouvrir les pièces jointes d'un mail inconnu
3) Ne pas suivre un lien hypertexte inconnu

Concernant vos données :

1) Les données doivent être enregistrées sur le serveur
2) Ne pas enregistrer de données sur votre ordinateur en local

ADOPTER DE BONNES PRATIQUES
ALERTES INTERNES

Concernant certains de vos correspondants :

1) Ils peuvent faire l'objet d'un détournement de correspondance. Ainsi, l'adresse de courriel d'un correspondant connu peut être utilisée par un tiers. En cas de doute, supprimer le message et vider la corbeille. Contacter téléphoniquement votre correspondant pour vérifier l'information et l'alerter.
2) La dématérialisation des factures se fera au 1er janvier 2017 depuis un site sécurisé du ministère des finances « Chorus portail pro ». Aucune facture numérique n'est actuellement recevable directement par courriel sans être préalablement authentifiée comme valide.
3) Les messages d'appel au secours sur votre messagerie sont des faux ou des arnaques. Traitez-les en indésirables et ne pas y répondre.
4) La ville n'a pas de compte bancaire dans le secteur privé. Tous les messages provenant d'une banque vous signalant un problème sur la gestion des comptes est un faux. Traitez-le en indésirable.

ADOPTER DE BONNES PRATIQUES
ALERTES INTERNES

N°4) Si vous faites l'objet d'une attaque virale :

- Débrancher le câble réseau de votre poste informatique ;
- Prévenez immédiatement notre prestataire SAGES GROUPE et informez votre hiérarchie.

Les antivirus ou les antispam mis en œuvre ne sont pas toujours efficaces contre les virus cryptants de type cryptolocker.

La sécurité des systèmes d'information, c'est d'abord un comportement individuel responsable.

Merci de votre compréhension.

Bonne journée

ADOPTER DE BONNES PRATIQUES
ALERTES DU PRESTATAIRE

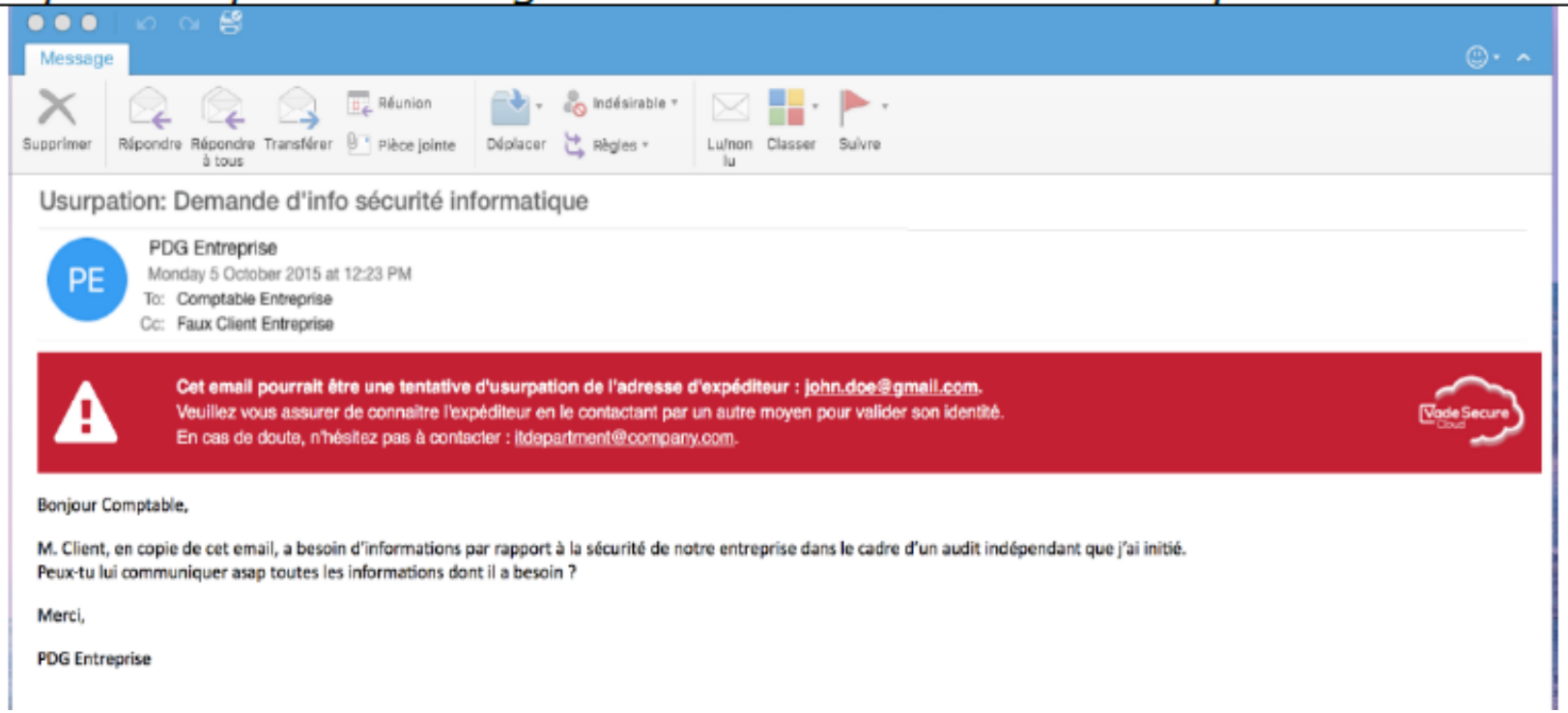
ALERTE : NOTE D'INFORMATION SUR VIRUS DANGEREUX

Un virus de type Cryptolocker, contre lequel les antivirus sont peu ou pas efficaces sévit depuis plusieurs mois. Il provoque au moyen d'un cryptage de fichiers, la **perte irréversible** de vos données, sauf à payer une rançon de

ADOPTER DE BONNES PRATIQUES
ALERTES DU PRESTATAIRE

- Une bannière peut signaler une usurpation d'identité

Exemple de Spear Phishing avec la bannière « imitation proche d'adresse »



ADOPTER DE BONNES PRATIQUES
ALERTES DU PRESTATAIRE

De : Vade Secure Cloud [noreply@vade-retro.com]
À : thierry ROLLAND
Cc :
Objet : Vade Secure Cloud Rapport de compte

ADOPTER DE BONNES PRATIQUES
ALERTES DU PRESTATAIRE

Figure 8 – Exemple de page de chargement lors du Time-of-Click

ADOPTER DE BONNES PRATIQUES
ALERTES DU PRESTATAIRE

Figure 10 – Exemple de page affichée en cas de délai d'analyse expiré

ADOPTER DE BONNES PRATIQUES
REMERCIER VOS COLLABORATEURS

Féliciter plutôt de sanctionner

Former plutôt qu'interdire

Associer plutôt qu'imposer

Etre plus efficace ensemble que vouloir tout régler tout seul

UTILISER DES PRODUITS DE SÉCURITÉ QUALIFIÉS

Pare-feu

Antivirus

Mobilité et accès sans fil

Contrôles d'accès

Poste de travail

Signature électronique

Technologie sans contact

BONNES PRATIQUES

Sécurité des mots de passe

Smartphones et PC

Réseaux sociaux

Internet

Téléchargements

Commandes en ligne

Liens dropbox

Cloud

SÉCURITÉ DES MOTS DE PASSE

Voici quelques recommandations :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne demandez jamais à un tiers de générer pour vous un mot de passe ;
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ;
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document Recommandations de sécurité relatives aux mots de passe.

Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

LES DIX COMMANDEMENTS

1. Utiliser des mots de passe de qualité. Le dictionnaire définit un mot de passe « comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé ». Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne.
2. Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc. La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.
3. Effectuer des sauvegardes régulières. Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de ses données est une condition de la continuité de votre activité.
4. Désactiver par défaut les composants ActiveX et JavaScript. Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.
5. Ne pas cliquer trop vite sur des liens. Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

LES DIX COMMANDEMENTS

6. Ne jamais utiliser un compte administrateur pour naviguer. L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'Internet. En limitant les droits d'un utilisateur, on limite aussi les risques d'infection ou de compromission de l'ordinateur.
7. Contrôler la diffusion d'informations personnelles. L'Internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…
8. Ne jamais relayer des canulars. Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.
9. Soyez prudent : l'Internet est une rue peuplée d'inconnus ! Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou toute autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.
10. Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants. Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme une pièce jointe appelée photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. À l'inverse, quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus « inerte » possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations.

PROSCRIRE LES COMPORTEMENTS À RISQUE

Utilisation des **réseaux sociaux** depuis son poste de travail : facebook, instagram…

Commandes sur sites internet : les courses en lignes

Téléchargement de films et musiques

Utilisation de **sites musicaux** : écouter la musique en travaillant

Jeux vidéos

Consultation de **sites licencieux** ou immoraux

Rechargement de son **smartphone** sur un ordinateur

Transfert de données du smartphone vers un ordinateur

Utilisation d'une clé **USB publicitaire** ou personnelle

LIMITER LES ACCÈS AU CLOUD

Les données du CLOUD ne vous appartiennent pas.

Elles sont accessibles à tous.

Elles ne sont pas localisables.

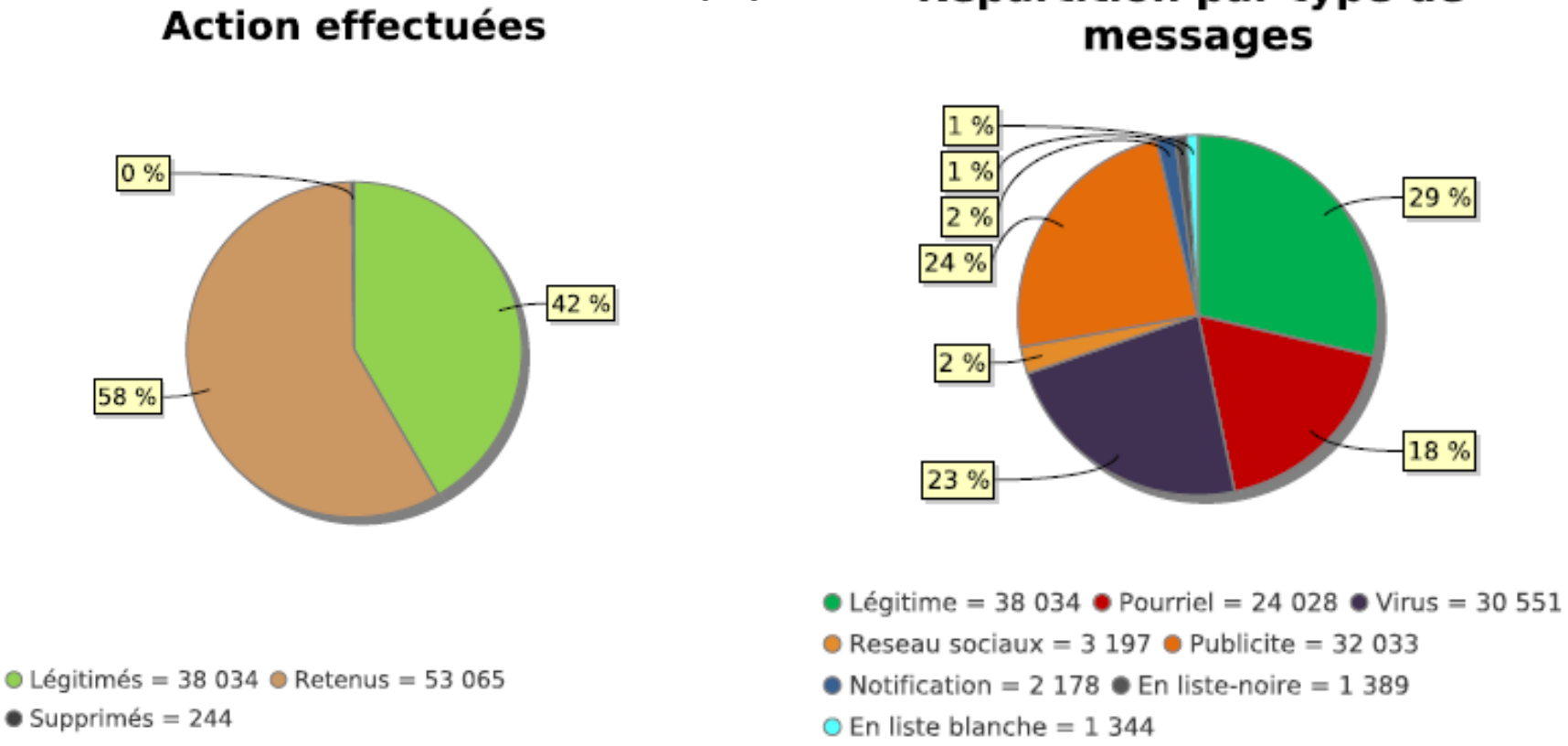
Elles peuvent faire l'objet d'un randsomware.

Les liens **dropbox** ne sont pas sûrs.

Les liens **doodle** ne sont pas sûrs.

ADOPTER DES OUTILS QUALIFIÉS

En 6 mois : d'avril à octobre 2016

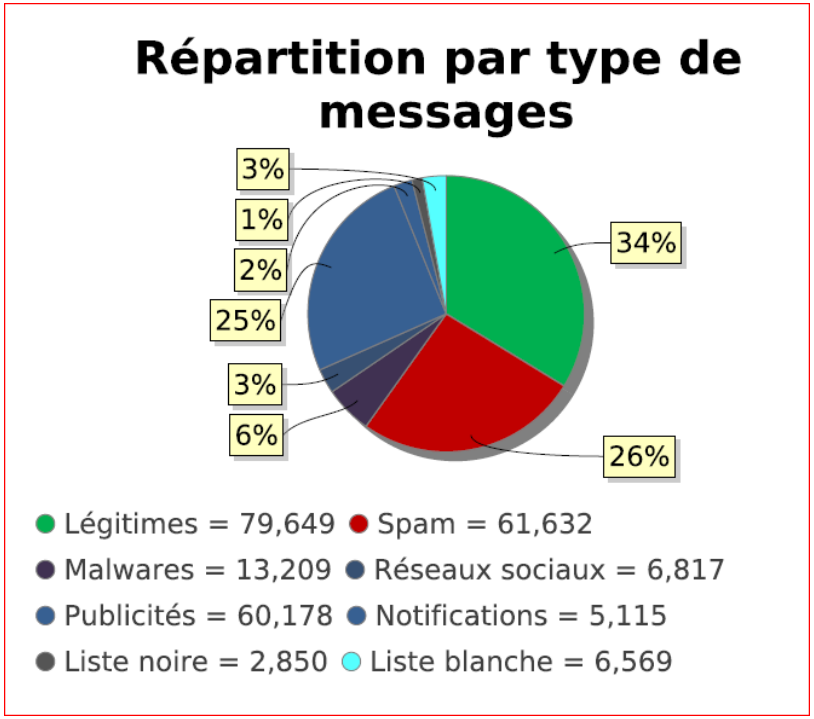


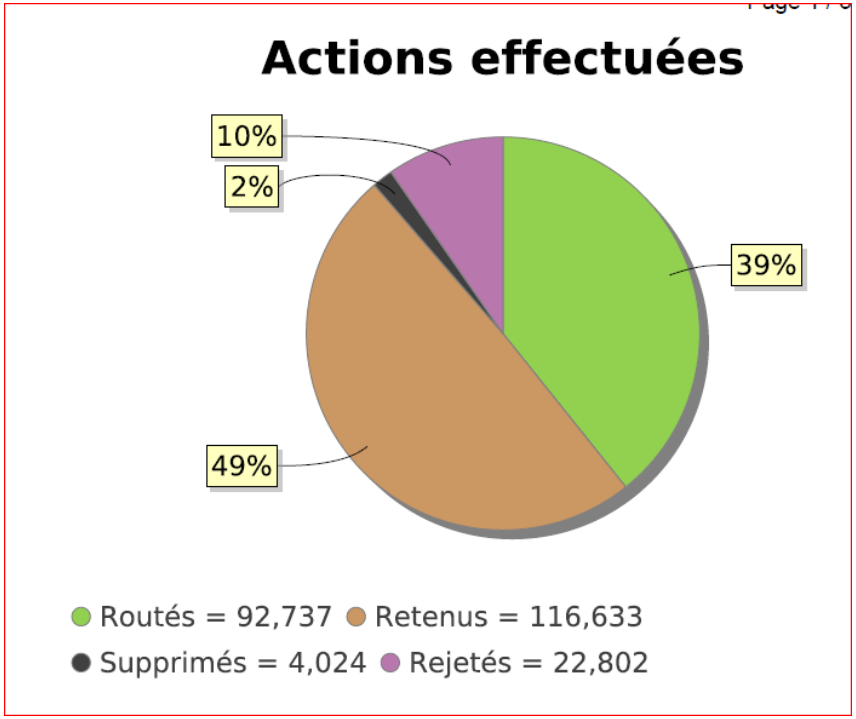
Resultats de l'analyse du flux entrant pour le site

EVOLUTION DANS LE TEMPS

Résultats de l'analyse du flux entrant pour le compte

01/12/2016 01:00 - 01/01/2018 00:59





PLAN DE REPRISE D'ACTIVITÉ OU PLAN DE MAINTIEN D'ACTIVITÉ

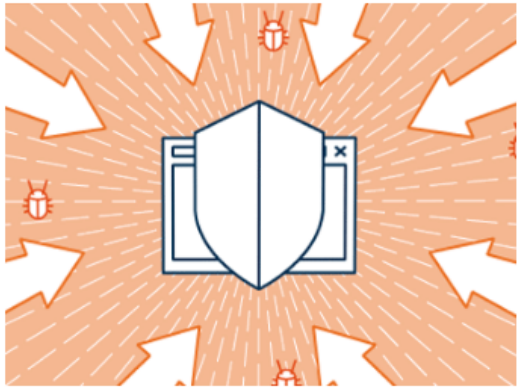
Le rôle clé des sauvegardes

L'adaptation de la mesure dans le ratio coût/avantage

Vers la nécessité d'un dispositif intégré ?

RESTER VIGILANT

L'actualité récente a entrainé un accroissement significatif du nombre d'attaques informatiques visant des sites Internet français. La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service** (DDoS) qui exploitent les failles de sécurité de sites vulnérables.*

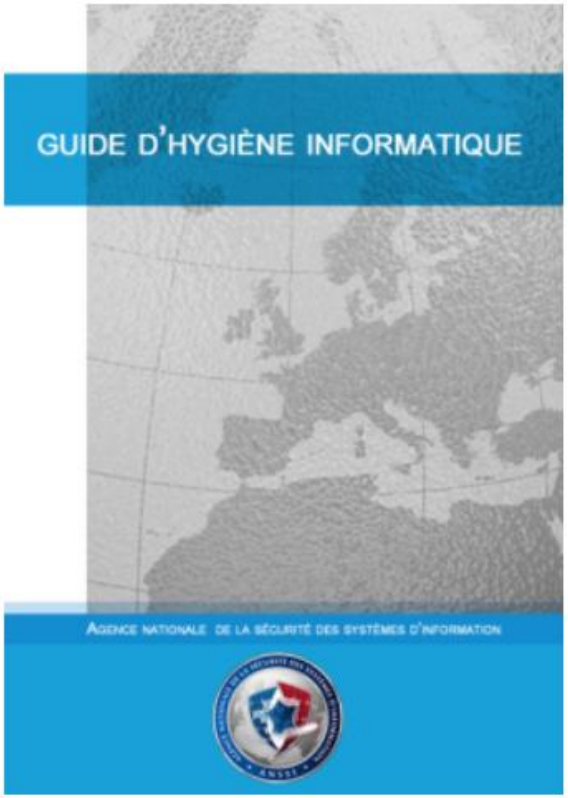


L'ANSSI rappelle qu'il est possible de se prémunir de ces types d'attaques en appliquant les bonnes pratiques présentées dans les fiches qu'elles a préparées à cet effet disponibles ci-dessous : une fiche destinée à tout internaute et une fiche destinée aux administrateurs de site Internet.
Enfin, l'application des recommandations du *Guide d'hygiène informatique* et de la *Note sur la sécurisation des sites Web* est fortement recommandée.

*Défiguration (defacement) : Résultat d'une activité malveillante visant à modifier l'apparence ou le contenu d'un serveur Internet. Cette action malveillante est souvent porteuse d'un message politique et d'une revendication.
**Déni de service (Denial of Service, DDoS) : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. Dans le cas d'un site Internet, celui-ci devient inaccessible à la consultation.

RESTER VIGILANT

Parmi les mesures techniques que les entreprises doivent prendre pour garantir la sécurité de leurs systèmes d'information, il en existe des simples, qualifiées d'hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.



Vous êtes responsable de la sécurité des systèmes d'information de votre organisation ou, plus simplement, c'est à vous que revient la responsabilité du bon fonctionnement de son informatique. Ce guide s'adresse à vous. Il vous présente les 40 règles d'hygiène informatique essentielles pour assurer la sécurité de votre système d'information et le moyen de les mettre en œuvre.

Non exhaustives, ces règles représentent cependant le socle minimum à respecter pour protéger les informations de votre organisation. Une fois ces règles partagées et appliquées, vous aurez accompli une part importante de votre mission : permettre à votre organisation d'interagir avec ses fournisseurs et ses partenaires, de servir ses clients, en respectant l'intégrité et la confidentialité des informations qui les concernent.

signal spam

SIGNALER, C'EST AGIR - WWW.SIGNAL-SPAM.FR

SIGNALER, C'EST AGIR !

Signaler **un Spam**

Tous les modules Se connecter

SIGNALEZ LE SPAM EN UN CLIC, UN GESTE CITOYEN POUR :

- ✓ Renforcer la sécurité sur Internet
- ✓ Participer à l'identification des spammeurs
- ✓ Permettre le suivi et l'intervention des acteurs Internet

Vite, découvrez les bénéfices d'agir avec nous...

Devenir partenaire Espace presse