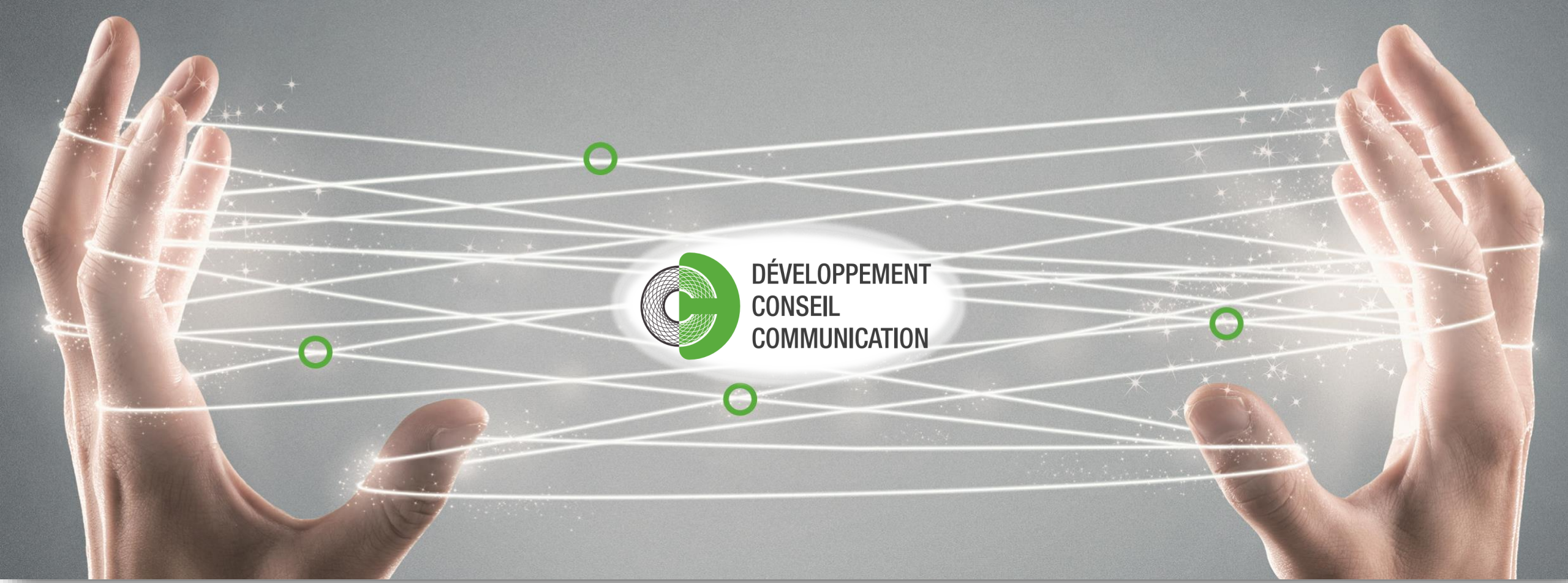


Sensibilisation **Sécurité**, **risques** et **exfiltration de données**

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Thématiques

- Les obligations juridiques et les risques qui en découlent
- Les pirates et leurs motivations
- L'exfiltration de données
- L'obsolescence logicielle et matérielle
- Les smartphones sont vulnérables
- Les attaques les plus communes en entreprise
- Les bonnes pratiques à adopter
- Les tests et analyses de sécurité
- Questions / réponses

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

SOMMAIRE

Sommaire Enjeux juridiques

1ère partie Les responsabilités des DSI

2ème partie Risques financiers administratifs

3ème partie Risques financiers liés au piratage

4ème partie Les acteurs juridiques et leur actualité

Présentateur

François DUQUENOY
Ingénieur Analyste Data & Consultant RGPD

LES RESPONSABILITÉS DES DSI

Dans quels cas suis-je responsable ?

Deux cas de figure :

- **Délégation de pouvoir par le directeur :**
  - **Non ambiguë**
  - **Précise**
  - **Limitée à un périmètre défini**
  - **Limitée dans le temps**

- **Faute personnelle :**
  - **Créant directement un sinistre**
  - **En cas de défaut de sécurité du SI**

DÉVELOPPEMENT CONSEIL COMMUNICATION

LES RESPONSABILITÉS DES DSI

Les étendues de ma responsabilité

- **En cas d'intrusion non autorisée dans un autre SI à partir de celui de son organisme**

- **En cas de consultation, téléchargement ou publication de contenus illicites :**
  - **Propos diffamatoires, injurieux, tout type de discrimination**
  - **Escroquerie**
  - **Contenu protégé par droit d'auteur**
  - **Contenu web illégal**

- **En cas d'utilisation de logiciels en dehors des termes de leur licence, acte de contrefaçon**

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

LES RESPONSABILITÉS DES DSI

Comment m'en prémunir et protéger ma responsabilité personnelle ?

- **Rédiger et transmettre aux employés une Politique de Sécurité des Systèmes d'Information (PSSI) :**
  - **Encadre l'ensemble des règles d'utilisation du SI**
  - **L'employé signataire devient en partie responsable de ses utilisations interdites par la PSSI**
- **Sensibiliser les personnels en plus de la signature de la PSSI**
- **Contractualiser attentivement la délégation de pouvoirs et les relations avec les sous-traitants**
- **Avoir un plan d'action de sécurisation avec budget associé**

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs : sanction administrative, RGPD – Art. 83

- Avertissement ou mise en demeure, qui peut être **rendu public**

- Injonction : **100 000 €** maximum par jour de retard

- Une injonction de cesser le traitement, la suspension des flux de données

- Sanction pécuniaire : **20 000 000 €** ou **4% du chiffre d'affaires annuel mondial**

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs : exemples de sanctions administratives

- **CNIL** – 21 janvier 2019, **Google**

Sanction de **50 000 000 €**

Manque de transparence, information insatisfaisante, absence de consentement valable.

- **CNIL** – 7 décembre 2020, **Amazon**

Sanction de **35 000 000 €**

Manquements relatifs aux cookies et à l'information des personnes.

- **CNIL** – 7 décembre 2020, **Google**

Sanction de **100 000 000 €**

Dépôt de cookies publicitaires sans consentement préalable des utilisateurs sur le site « *www.google.fr* ».

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs : chez les entreprises françaises...

- **CNIL** – 6 juin 2019, **Sergic**

Sanction de **400 000 €**

Atteinte à la sécurité des données et non-respect des durées de conservation.

- **CNIL** – 26 novembre 2020, **Carrefour France et Carrefour Banque**

Sanction de **2 225 000 €** et **800 000 €**

Manquement à l'obligation d'informer les personnes, manquements relatifs aux cookies, manquement au respect des droits.

- **CNIL** – 7 juin 2018, **Optical Center**

Sanction de **250 000 €**

Atteinte à la sécurité des données des clients du site internet « *www.optical-center.fr* ».

Amende descendue à **200 000 €** le 17 avril 2019, considérant la célérité avec laquelle la société avait remédié au défaut de sécurisation de son site internet.

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs : et même chez les organismes publics !

- **CNIL** – 31 juillet 2018, **Office Public pour l'Habitat de Rennes : Archipel Habitat**

Sanction de **30 000 €**

Utilisation du fichier de ses locataires à d'autres fins que celle de gestion de l'habitat social.

- **Comissão Nacional de Proteção de Dados** (CNIL portugaise) – Juin 2018, **Hôpital de Barreiro**

Sanction de **150 000 €**

Violation des principes d'intégrité et de confidentialité des données.

+ sanction de **150 000 €**

Violation du principe de limitation d'accès aux données.

+ sanction de **100 000 €**

Incapacité du responsable de traitement à garantir l'intégrité des données.

Sanction totale de **400 000 €**

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers administratifs : Cas du Ministère de l'Intérieur

- **CNIL** – 14 janvier 2021, **Ministère de l'Intérieur**

Sanction de **0 €**

Utilisation de drones équipés de caméras pour surveiller le respect des mesures de confinement.

La CNIL ne peut pas prononcer d'amende à l'encontre de l'État.

Injonction à cesser tout vol de drones équipés de caméras sans finalité explicite validée au préalable par la CNIL.

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers liés au piratage

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers liés au piratage : le cas British Airways

Vol des coordonnées bancaires de plus de **430 000 clients**.

Amende record :

200 000 000 €

Amende finale :

20 000 000 £

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Risques financiers liés au piratage : autres types de sanctions financières

- **Baisse de la réputation**

- **Incessibilité**

  Cass. 25 juin 2013 : Un fichier incluant des données à caractère personnel non déclaré à la commission nationale informatique et libertés (CNIL) est une chose hors du commerce, du fait de son objet illicite.

- **Irrecevabilité de la preuve**

  Cass. Soc. 8 octobre 2014 : Les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la CNIL constituent un moyen de preuve illicite et irrecevable.

Les acteurs juridiques et leur actualité

- **La CNIL**

Publication du référentiel sur l'accompagnement social et médico-social.

Mise en application des règles sur les cookies web.

- **L'ANSSI**

Orientation dédiée à la cyber défense, accompagnement de professionnels cyber.

- **CERT-FR**

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.

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

- **Le Forum International de la Cybersécurité (FIC)**

Événement de référence en Europe en matière de sécurité, cyber sécurité, digitalisation et confiance numérique

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

- **Qui sont les pirates et quelles sont leurs motivations ?**
- **Qu'est-ce que l'exfiltration de données ?**
- **Hacking lab**
- **L'obsolescence logicielle et matérielle**
- **Les smartphones sont vulnérables**
- **Les attaques les plus connues en entreprise**
- **Les bonnes pratiques à adopter en entreprise**

Présentateur

Sébastien Pyl
Responsable de la Sécurité des Systèmes d'Information

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Qui sont les pirates et quelles sont leurs motivations ?

4 grandes familles :

- Hacktiviste
- Cyberterroriste
- Cyber-criminel
- Script-kiddie

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Qu'est-ce que l'exfiltration de données ?

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Qu'est-ce que l'exfiltration de données ?

Etape 1

Compromission du système

Etape 2

Recherche de données / automatisation

Etape 3

Exfiltration des données vers une source externe

Etape 4

Dissimulation et/ou suppression des traces

Etape 5

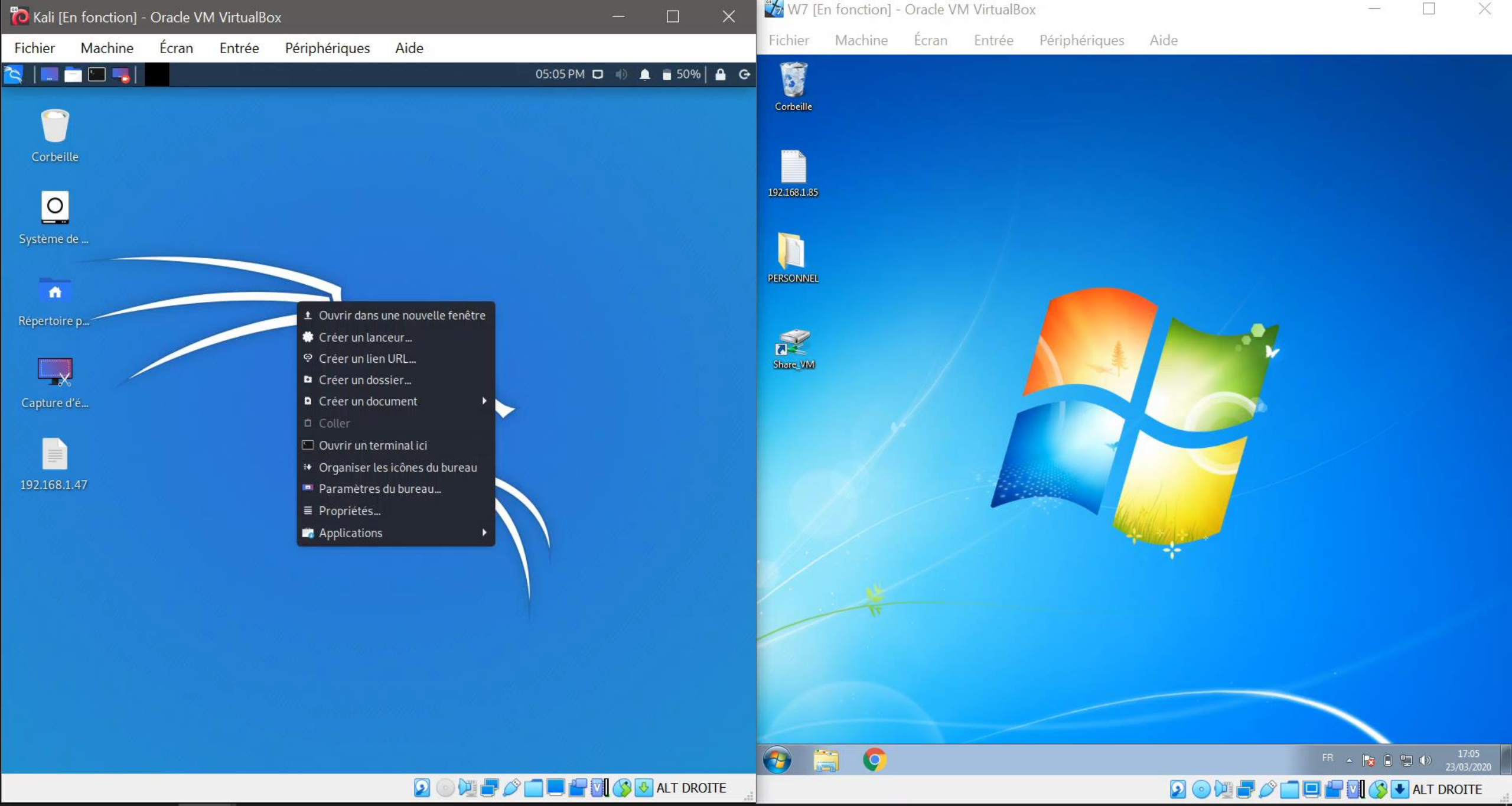
Partage des données volées à des tiers (revente, réutilisation, etc.)

Etape 6

Réutilisation frauduleuse ou médiatisation du vol pour décrédibiliser l'entreprise

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Hacking lab : exfiltration de données


Kali [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
05:05 PM 50%
Corbeille
Système de ...
Répertoire p...
Capture d'é...
192.168.1.47
Ouvrir dans une nouvelle fenêtre
Créer un lanceur...
Créer un lien URL...
Créer un dossier...
Créer un document
Coller
Ouvrir un terminal ici
Organiser les icônes du bureau
Paramètres du bureau...
Propriétés...
Applications
ALT DROITE
W7 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Corbeille
192.168.1.85
PERSONNEL
Share_VM
FR
17:05
23/03/2020
ALT DROITE
17:05
23/03/2020

Hacking lab : conclusion

Les pirates utilisent le facteur humain :

- Inattentions
- Manque de connaissances
- Manque de sensibilisation

Extensions dangereuses :

- Fichier texte **.pdf** / **.docx**
- Tableur macros **.xlsm** (la charge peut être une macro VBS du document, **très courant** et **dangereux**)
- Audio et vidéo **.mp3** / **.wav** / **.mp4** / **.mkv** / **.avi**
- Fichier exécutable **.exe** / **.msi** / **.dll** / **.sys** (normalement impossible sur un logiciel de mailing récent)

Hacking lab : conclusion

Ne pas avoir pleinement confiance dans les partenaires, collaborateurs et collègues.

- Victimes
- Transferts de mails
- Pièces jointes vérolées

Propagation des malwares :

- Carnet d'adresses mail
- Listes de distribution
- Réseau
- Automatisation

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Obsolescence logicielle et matérielle

Obsolescence logicielle

- Mise à jour des composants matériels
- Mise à jour des logiciels métier et programmes tiers
- Licences

- Mise à jour du système d'exploitation
  - **Plus de support !**
  - **Plus de patchs de sécurité !**
  - **Incompatibilités logicielles !**

Obsolescence matérielle

- Composants récents
- Respect des normes

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les smartphones sont vulnérables

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les smartphones sont vulnérables : que contient un smartphone ?

Un smartphone est un mini-ordinateur.

Il contient comme son grand frère l'ordinateur :

- Un processeur 

- De la mémoire vive (RAM) 
- De l'espace de stockage (interne et carte SD) 

- Un système d'exploitation (Android ou iOS pour les smartphones, Windows pour les ordinateurs)

PC = vulnérable —ainsi→ **Smartphone = vulnérable**

Les smartphones sont vulnérables : comment les malwares pénètrent-ils dans un smartphone ?

- **Pièces jointes de mails vérolés** (via applications ou versions web)
- Installation d'**applications tierces non-officielles**
- Installation d'applications depuis les stores officiels (et oui...)

Le Play Store Android a beau être sécurisé, il arrive que des applications malveillantes extrêmement bien conçues passent au travers des mailles du filet.

Un procédé connu par les hackers pour bypass le système de sécurité est d'utiliser un dropper.

C'est-à-dire que l'application sera « légitime » mais possèdera un petit bout de code discret sous forme de « **bombe logique** » qui importera depuis une source externe (internet) le réel programme malveillant.

Les smartphones sont vulnérables : les malwares récents sous Android

StrandHogg

WhatsApp

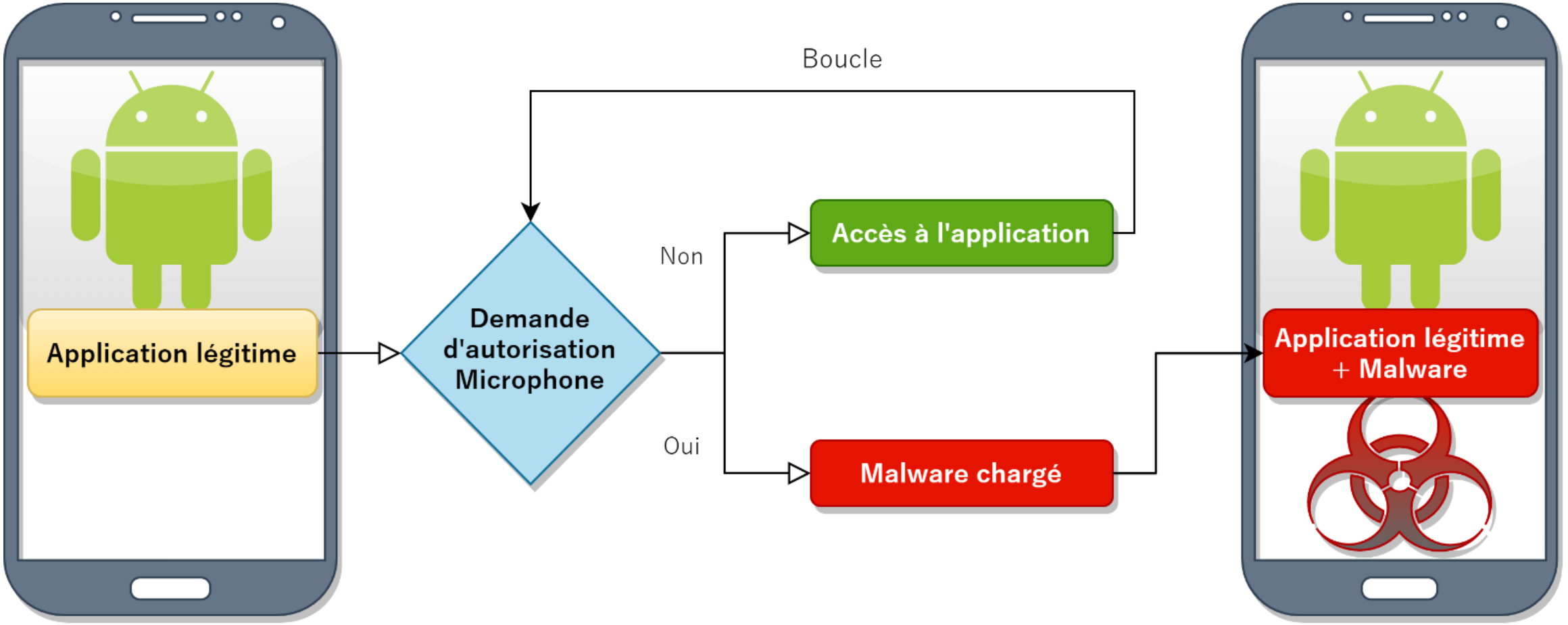
CVE-2019-11931

Les smartphones sont vulnérables : StrandHogg

- Découverte par des chercheurs début décembre 2019
- **Se camoufle dans les applications légitimes du Play Store**
- **36 applications corrompues** retirées du Play Store
- Utilise un « dropper » (code qui va télécharger un autre programme)
- **Se greffe aux applications du smartphone**

- Lors de la consultation d'une application, demande d'autorisation de privilèges système
  - Accès au microphone
  - Accès au stockage, photos, vidéos
  - Écrire et lire des SMS/MMS
  - Accès aux coordonnées bancaires
  - Accès aux identifiants et mots de passe

Les smartphones sont vulnérables : StrandHogg → fonctionnement



Les smartphones sont vulnérables : StrandHogg → état actuel de la vulnérabilité

A l'heure actuelle, aucun patch n'a été trouvé afin d'empêcher le malware de se propager sur d'autres applications du Play Store, de l'identifier avec précision et de l'éradiquer des systèmes déjà infectés.

Les smartphones concernés par cette vulnérabilité sont la totalité des appareils sous Android !

Les smartphones sont vulnérables : WhatsApp (CVE-2019-11931)

- **Application du Play Store**
- Vulnérabilité découverte le 13 avril 2019
- Référence : CVE-2019-11931
- **N'utilise pas de malware !**
- Technique très avancée de piratage : **Buffer Overflow** (débordement de mémoire tampon)

- Versions d'OS impactées :
  - **Android** < 2.19.274
  - **iOS** < 2.19.100
  - **Enterprise Client** < 2.25.3
  - **Windows Phone** <= 2.18.368

Les smartphones sont vulnérables : comment les victimes se font-elles infecter ?

- Le pirate envoie un fichier **.mp4**
  - Malware dissimulé en arrière-plan
  - S'exécute à l'ouverture du fichier

Ce malware est appelé Spyware (logiciel espion) et comme nom l'indique, il permet d'espionner le téléphone de la victime.

Le malware de la CVE-2019-11931 a quant à lui été programmé pour ne cibler que les conversations WhatsApp.

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les smartphones sont vulnérables : comment éviter l'infection et comment s'en débarrasser ?

- Mettre à jour l'application depuis son interface ou depuis le store officiel
- Mettre à jour l'application depuis le site internet du développeur (attention aux faux sites)
- Mettre à jour son système d'exploitation, même si cela modifie le design !

La sécurité prime sur le design !

Si l'application possède déjà la dernière version stable et identifié comme infectée, il faut attendre que les développeurs fournissent aux utilisateurs un patch (mise à jour corrective de sécurité).

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les smartphones sont vulnérables : les informations stockées sur nos smartphones

- Coordonnées bancaires
- Coordonnées Paypal si pas de données bancaires enregistrées
- Identifiants et mots de passe de boîte mail
- SMS, MMS, photos, vidéos, documents
- ID de connexion aux sites web et réseaux sociaux (applications et sites web) sous forme de cookies
- Liste de contacts téléphoniques et mail
- Applications de double-authentification (bypass avec accès aux ID de boîte mail)
- Informations de géolocalisation (passées et temps réel)
- Etc.

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les smartphones sont vulnérables : les bonnes pratiques à adopter

- Ne télécharger des applications que depuis les stores officiels

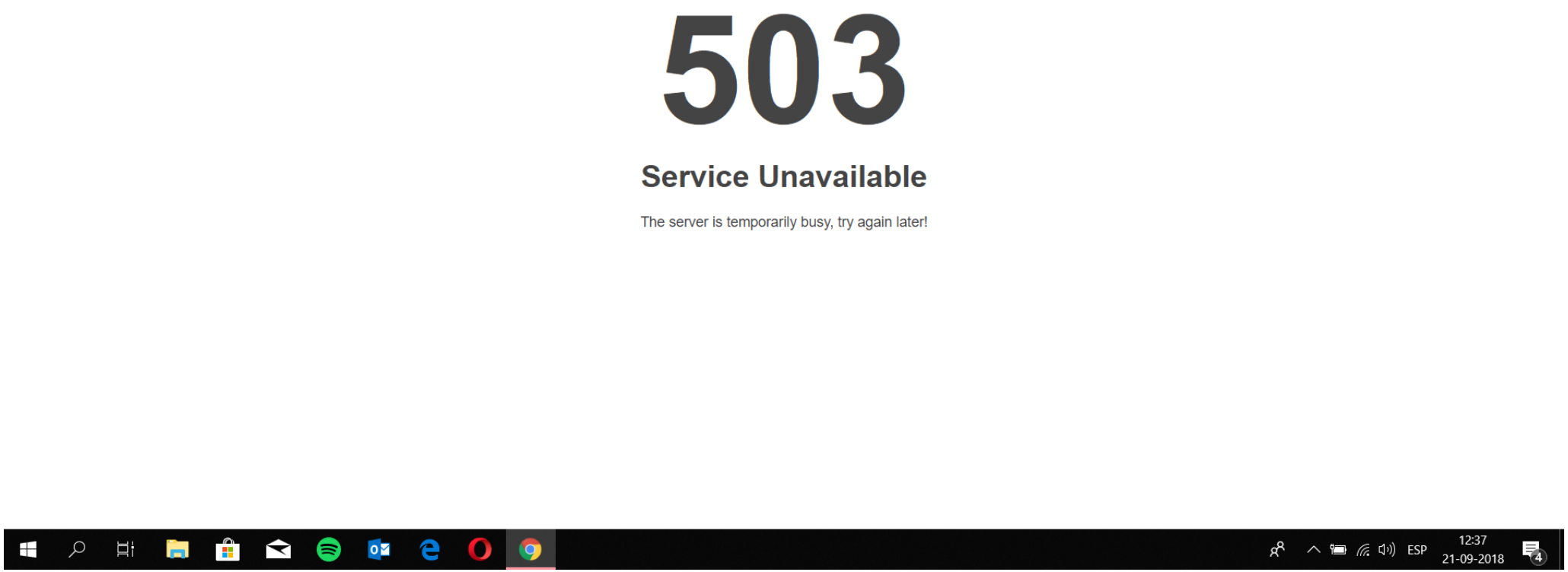
- Ne pas stocker d'informations professionnelles si son smartphone n'est pas en accord total avec les mesures de sécurité imposées par l'entreprise

- Se déconnecter des sites et applications avant leur fermeture (valable aussi sur ordinateur)

- Utiliser des mots de passe complexes et différents pour chaque utilisation

- Ne pas stocker d'informations confidentielles sur son smartphone (vol, piratage, faille humaine)

Les attaques les plus communes en entreprise



DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les attaques les plus communes en entreprise : vecteurs et attaques

La plupart des attaques en entreprise repose sur le **vecteur humain**, mais d'autres plus poussées se focalisent sur l'**exploitation de vulnérabilités** dans les équipements (ex. processeur) et sur les logiciels métiers et grand public.

- WIFI (Guest)
- Phishing
- Ransomware
- Interruption de service
- Faiblesses de configuration

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Bonnes pratiques

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Bonnes pratiques : autant en entreprise que chez soi

Les bonnes pratiques sont à mettre œuvre autant dans un cadre professionnel que domestique !

- Ne pas mélanger sur un même dispositif les données professionnelles et personnelles
- Appliquer une sécurité physique aux dispositifs (cadenas, mots de passe, empreinte digitale, etc.)
- Etablir et faire respecter la charte informatique de l'entreprise
- Campagnes de sensibilisation
- N'utiliser que des applications métiers approuvées par le RSSI

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Bonnes pratiques : autant en entreprise que chez soi

- En cas de suspicion d'infection sur le réseau interne, **déconnecter** immédiatement son ordinateur **du réseau** (câble réseau, WIFI et puce 4G) et **avertir le personnel compétent**

- Prendre garde aux **pièces jointes** de mails, aux **URL inexactes** (ex. twiitter.com), aux **offres alléchantes** et aux **adresses mails d'expéditeurs** (pas seulement le nom affiché dans l'application mail)

- Utiliser le **VPN** de l'entreprise en cas de déplacement ou aucune connexion internet si cela n'est pas strictement nécessaire (consultation PDF, rédaction Word, Excel, etc.)

- Utiliser des mots de passes sécurisés (ex. **J5sd#p_2qs**), ne pas les stocker sur un document texte, un post'it, un espace commun, etc.

Les tests et analyses de sécurité

- **Scans de vulnérabilités**

  Détecte l'ensemble des vulnérabilités machines présentes sur le réseau

  Joue des charges à blanc et relève les succès et échecs

  Liste complète des failles et leur niveau de criticité

- **Web Application Scans (WAS)**

  Détecte l'ensemble des vulnérabilités des applications exposées sur le web

  Liste complète des failles applicatives et leur niveau de criticité

- **Scans de trafic réseau**

  Détecte les applications utilisées sur le réseau, les performances du réseau, les flux de données en entrée / sortie

  Évite les failles humaines de consultation ou utilisation d'applicatifs douteux

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les tests et analyses de sécurité

- **Test d'intrusion**

  Mise en situation avec un hacker cherchant à s'infiltrer dans le réseau

  Recherche d'une ou plusieurs failles exploitables

  Rapport d'utilisation des failles et périmètre compromis

- **Analyse de risques**

  Identification de l'ensemble des risques organisationnels, physiques et d'utilisation du SI

  Classification par gravité et vraisemblance et plan d'action associé

- **Contrôle de conformité - RGPD**

  Entretiens oraux et documentaires des pratiques de sécurité et déclarations juridiques (RGPD) d'un périmètre défini

  Liste complète des points de non-conformité et des améliorations à apporter dans un plan d'action

DÉVELOPPEMENT
CONSEIL
COMMUNICATION

Les tests et analyses de sécurité

- **Campagnes de faux phishing**

  Sensibilisation par la pratique

  Mesure le niveau de sensibilisation des personnels

  Prévient les mails pouvant causer des dégâts

- **Sensibilisation des personnels**

  Tables rondes, scénettes ludiques ou mise en situation dans un Escape Game

  Apprentissage et sensibilisation sur tous les sujets clés pour éviter les failles humaines

- **Externalisation du Système d'Information**

  Permet de maîtriser les coûts, bénéficier de compétences d'experts et disposer de ressources adaptées au besoin

  Accompagne le développement de l'organisme

Toute l'équipe de DC Communication vous remercie pour votre participation.