La sécurité en déplacement

Groupe 5 TOSA

1

3.1 La sécurité physique des terminaux 2

En règle général 2

Dans les transports ou en voyage : 5

Prendre des mesures de sécurisation physique des terminaux nomades 5

Avant le voyage 5

Pendant le voyage 6

Avant votre retour de voyage 7

Après le voyage 7

Établir une politique d'utilisation mobile claire 9

Segmenter les données et les applications sur les appareils de l'entreprise 9

Chiffrer les données 9

Surveiller le comportement des utilisateurs 9

Sensibiliser à la sécurité mobile 9

Comment rendre le smartphone plus sécurisé ? 10

Installer un antivirus 10

Utiliser un VPN 10

Activer le chiffrement des données 10

Configurer l'effacement à distance 10

Protéger les mobiles Android : informations supplémentaires 10

Autres bons à savoir pour les utilisateurs d'iPhone 10

Conclusion 11

Ressource 11

https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf?v=1647428178 11

https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/ 11

https://www.lebigdata.fr/cybersecurite-mobile-dossier 11

La multiplication des ordinateurs portables, des clés USB et des *smartphones* rend indispensable d'anticiper les atteintes à la sécurité des données consécutives au vol ou à la perte de tels équipements.

3.1 La sécurité physique des terminaux

Les smartphones/tablettes et ordinateurs sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires.

En règle général

1. La première option est de verrouiller les terminaux avec un code pin + un code d'accès

le code d'accès ou verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas

2. Installer des applications que depuis les sites ou magasins officiels

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées.

Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications ou qui les offrent gratuitement alors qu'elles sont normalement payantes: elles sont généralement piégées.

Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application.

Au moindre doute, n'installez pas l'application et choisissez-en une autre.

3. Appliquer les mises à jours de sécurité

Qu'il s'agisse du système d'exploitation ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4. Faites des sauvegardes

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5. Utilisez une solution de sécurité contre les virus et autres attaques

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (ransomware), l'hameçonnage (phishing)…

Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

6. Chiffrez les données de l'appareil

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations.

7. Contrôler les droits d'utilisation de vos applications

Vérifiez également les autorisations que vous donnez à vos applications. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez en une autre.

8. Ne laissez pas votre appareil sans surveillance

Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

Conservez le code IMEI de votre appareil mobile

Composé de 15 à 17 chiffres, le code IMEI est **le numéro de série de votre appareil mobile**. Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.

Notez le soigneusement et, si vous l'avez égaré, **vous pouvez le récupérer en tapant *#06# sur votre clavier.**

9. Ne stockez pas d’informations confidentielles sans protection

Ne notez jamais d’informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile.

Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

Dans les transports ou en voyage :

Prendre des mesures de sécurisation physique des terminaux nomades

Avant le voyage

1. Relisez attentivement et respectez les règles de sécurité édictées par votre organisme.
2. Renseignez-vous sur les lois régissant la propriété intellectuelle, les données numériques et les données cryptées dans les pays que vous visitez

Se familiariser avec la législation locale, ainsi qu'avec la réglementation pour l'entrée sur le territoire et la sortie.

La loi peut viser non seulement les données, mais aussi les logiciels, les applications et le matériel informatique et le support de stockage.

3. Utilisez de préférence du matériel dédié aux missions (ordinateurs, ordiphones, supports amovibles tels que les disques durs et clés USB)

Certaines unités mettent à la disposition de leurs employés des équipements réservés exclusivement au voyage. Il faut que vous vérifiiez auprès de l'assistance technique de votre unité si vous pouvez vous procurer ce matériel pour votre voyage;

Ces appareils (ordinateurs, téléphones intelligents, tablettes, supports amovibles, etc.) ne doivent pas contenir d'autres informations que celles dont vous avez besoin durant votre voyage;

Il est recommandé que le matériel dédié dispose d'une configuration minimale et qu'il ne contienne que les données et les logiciels requis pour le voyage.

4. Sauvegardez les données que vous emportez et laissez la sauvegarde en lieu sûr.

En sauvegardant ces données dans un lieu sûr, il vous sera ainsi possible de récupérer vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements.

5. Évitez de partir avec des données sensibles.

Privilégiez, si possible, la récupération de fichiers chiffrés sur votre lieu de mission en accédant au réseau de votre organisme avec une liaison sécurisée, sinon à une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées. Il faut supprimer les informations de cette boîte après lecture.

6. Utilisez un filtre de protection écran pour votre ordinateur.

Cela vous permettra de travailler sur votre ordinateur, durant vos trajets, en toute discrétion.

Le filtre de confidentialité

Le filtre de confidentialité s'utilise pour protéger son écran des regards indiscrets et lutter contre la tentation naturelle de regarder un écran allumé. Il permet à l'utilisateur nomade de pouvoir utiliser son équipement dans des lieux publics tels que le train, l'avion, les lieux de passage sans qu'un voisin ne puisse voir ce qui apparaît sur l'écran. Il s'utilise en open space quand l'employé travaille à la vue de tous sur des données confidentielles.

Le filtre est maintenu sur l'écran par des glissières adhésives placées sur les bords ou directement appliqué sur l'écran à l'aide d'un adhésif repositionnable. Il est conçu pour être placé et enlevé à volonté afin de partager son écran.

Ces filtres sont aussi disponibles pour les nouveaux outils nomades tels que les smartphones ou les tablettes.

7. Marquez vos appareils d'un signe distinctif (comme une pastille de couleur).

Cela vous permet de surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment pendant le transport. Pensez à mettre un signe également sur la housse.

8. Activez la fonctionnalité de géolocalisation et installez un logiciel antivol si c'est possible

Certains équipements disposent d'options de localisation automatique et de logiciels antivol. Il est fortement recommandé de se familiariser avec ces options et d'envisager la possibilité de les activer

Pendant le voyage

1. Gardez vos appareils, supports et fichiers avec vous.

Prenez-les en cabine lors de votre voyage. Ne les laissez jamais dans un bureau ou dans la chambre d'hôtel (même dans un coffre).

2. Protégez l'accès de vos appareils par des mots de passe forts.

Configurer un mot de passe pour pouvoir accéder au contenu de vos appareils. Ce mot de passe doit être constitué d'au moins huit (8) caractères et 2 caractères spéciaux

3. Ne vous séparez pas de vos équipements.

Si vous devez vous séparer de votre smartphone ou de votre tablette, conservez avec vous la carte SIM. et pour les ordinateurs, mettre un cadena (câble antivol)

4. Utilisez un logiciel de chiffrement pendant le voyage

Ne communiquez pas d'information confidentielle en clair par téléphone ou tout autre moyen de transmission de la voix (services de VoIP comme Skype).

5. Pensez à effacer l'historique de vos appels et de vos navigations

Outre l'historique, il faut effacer les données laissées en mémoire cache, cookies, mot de passe d'accès aux sites web et fichiers temporaires.

6. En cas d'inspection ou de saisie par les autorités, informez immédiatement votre organisme.

Fournissez les mots de passe et clés de chiffrement si vous y êtes contraint par les autorités locales puis alertez votre SI.

7. En cas de perte ou de vol d'un équipement ou d'informations, informez immédiatement votre organisme.

Demandez conseil au consulat avant toute démarche auprès des autorités locales.

8. N'utilisez pas les équipements qui vous sont offerts (clés USB). Ils peuvent contenir des logiciels malveillants.

Les clés USB, de par leurs multiples vulnérabilités, sont un vecteur d'infection privilégié par des attaquants.

Verrouillage des ports USB

Les ports USB sont des stations de travail non surveillées, et même des appareils comme les imprimantes, les caméras et les lecteurs externes pourraient être exploités pour dérober des données d'entreprise ou introduire un malware dans le réseau via des ports USB. Pour stopper les malwares, éviter le vol de données et maintenir vos pratiques de sécurité Zero Trust, les administrateurs doivent utiliser une approche de moindres privilèges pour régir de façon granulaire qui a accès à quels ports USB et où.

9. Ne connectez pas vos équipements à des postes ou des périphériques informatiques qui ne sont pas sûrs.

Attention aux échanges de documents (par exemple : par clé USB lors de présentations commerciales ou lors de colloques). Emportez une clé destinée à ces échanges et jetez la après usage

10. Ne rechargez pas vos équipements sur les bornes électriques libre-service.

Certaines de ces bornes peuvent avoir été conçues pour copier les documents à votre insu.

11. Évitez les réseaux publics Wifi publics ou inconnus

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

Avant votre retour de voyage

1. Transférez vos données

Sur le réseau de votre organisme à l'aide de votre connexion sécurisée sinon sur une boîte de messagerie en ligne dédiée à recevoir vos fichiers chiffrés (qui seront supprimés dès votre retour).

Puis effacez-les ensuite de votre machine, si possible de façon sécurisée, avec un logiciel prévu à cet effet.

2. Effacez l'historique de vos appels et de vos navigations

Cela concerne aussi bien vos appareils nomades (tablette, téléphone) que votre ordinateur.

Après le voyage

1. Changez tous les mots de passe que vous avez utilisés pendant votre voyage.

Ils peuvent avoir été interceptés à votre insu.

2. Analysez ou faites analyser vos équipements.

Ne connectez pas les appareils à votre réseau avant d'avoir fait ou fait faire au minimum un test antivirus.

3. Effectuez un inventaire de vos données et équipements

Vérifiez la présence de tous les équipements et les données que vous avez apportés avec vous pendant votre voyage.

4. Signalez tout élément SDI notable

Rapportez à votre gestionnaire responsable de la sécurité de l'information (GRS) tout élément notable, concernant la sécurité de l'information qui s'est déroulé pendant le voyage.

5. Effacez complètement votre équipement de déplacement

procédez à l'effacement sécuritaire de tout équipement qui vous a été prêté pour votre usage durant le déplacement.

3.2 Smartphones et sécurité

(de connaître les principes et l'utilité d'une gestion de flotte de mobiles professionnels (MDM).)

Il n'est plus nécessaire de présenter l'utilité de disposer d'une flotte mobile et ce depuis plusieurs années. Les terminaux se sont de plus en plus diversifiés avec de plus en plus d'applications (que ces dernières soient métiers ou non). Cette multiplicité de fonctions peut rendre la tâche du personnel en charge de la maintenance très compliquée.

Notre gamme AviTice School Integral dispose, dans sa version Advanced, d'un module AviTice Clyd qui propose une interface simple et ergonomique pour prendre en main les terminaux Android. De nombreuses fonctions permettent de gérer les tablettes ou smartphones :

- Inventaire matériel et logiciel
- Création d'un catalogue d'application
- Déploiement d'applications
- Personnalisation des interfaces des terminaux (kiosque)
- Blocage des fonctionnalités
- Lancement de processus personnels
- Géolocalisation

En 2021, le monde comptait 3,8 milliards d'utilisateurs de smartphones contre 2,5 milliards en 2016. Le nombre de mobinautes augmente chaque année et le taux de risque d'attaque suit le mouvement.

En 2019 par exemple, le nombre de cyberattaques a augmenté de 50 % d'une année à l'autre. Et avec le **boom du travail à distance dans un contexte pandémique**, le bilan en 2020 est encore plus lourd. En France, les cyberattaques ont été multipliées par quatre durant cette année.

L'utilisation massive des réseaux sociaux constitue une autre source de préoccupation majeure. Les hackers peuvent toucher un plus grand nombre de mobinautes grâce à ces plateformes en plus de pouvoir les manipuler plus facilement. Les réseaux sociaux sont devenus un terrain de jeu parfait pour les pirates informatiques.

Les recherches évoquent également les campagnes de piratage soutenues par l'État, qui utilisent de plus en plus les appareils mobiles pour recueillir des renseignements. Malgré l'explosion des menaces, **la plupart des PME mettent du temps à réagir et à mettre en œuvre une stratégie de sécurité mobile.**

Cette dépendance aux gadgets connectés signifie pourtant qu'il est urgent pour les petites et moyennes entreprises d'adopter une approche proactive face à la menace externe qui pèse sur leurs processus commerciaux internes.

La cybersécurité des mobiles est devenue vitale pour les entreprises. Les organisations qui fournissent des appareils mobiles à leurs employés doivent **établir des mesures de sécurité strictes**. Il en est de même pour celles qui intègrent l'usage des appareils personnels dans le cadre du travail. Les entreprises peuvent suivre les étapes suivantes pour mettre en œuvre la sécurité mobile.

Établir une politique d'utilisation mobile claire

Les entreprises doivent **inclure les appareils mobiles dans les politiques de sécurité à l'échelle de l'organisation**. Ces politiques incluront entre autres les limites et les cadres d'utilisation, les mesures antivol, les paramètres de sécurité obligatoires à configurer. Le plan stratégique suppose aussi la **surveillance de la conformité et la correction des lacunes**.

Segmenter les données et les applications sur les appareils de l'entreprise

Les experts en cybersécurité recommandent de segmenter les utilisateurs mobiles au sein de l'entreprise en groupes avec **différents niveaux de privilèges d'accès selon leur fonction**. Cela réduit la surface d'attaque exposée si un appareil est compromis.

La segmentation des applications est tout aussi nécessaire. Cela empêchera les utilisateurs d'installer des logiciels indésirables qui pourraient compromettre le réseau. **Les programmes BYOD ou Bring Your Own Device (apportez votre propre appareil) ont fait leurs preuves dans la sécurisation du système de l'entreprise. Une piste à explorer.**

Chiffrer les données

Les **données chiffrées** ne sont pas accessibles à l'utilisateur malveillant en cas de vol ou de perte de l'appareil mobile. **Minimiser la visibilité sur les appareils qui ont accès au réseau de l'entreprise permet aussi de renforcer la cybersécurité mobile. Cela implique l'utilisation d'un système de gestion des identités et des accès (IAM) ainsi que des solutions de protection des données.**

Surveiller le comportement des utilisateurs

Surveiller le comportement des utilisateurs peut **révéler des anomalies pouvant indiquer une attaque en cours**. Une surveillance automatisée peut aussi s'avérer crucial pour s'assurer que les politiques de sécurité mobile de l'organisation sont bien respectées.

Sensibiliser à la sécurité mobile

Les entreprises doivent **mettre en place des programmes de formation pour sensibiliser aux risques de sécurité inhérents à la technologie mobile**. Les enjeux de la sécurité des appareils mobiles ou les pratiques courantes à mettre en œuvre pour éviter les menaces par exemple sont des thèmes pertinents à aborder durant ces formations.

Comment rendre le smartphone plus sécurisé ?

Chaque utilisateur peut aussi prendre les mesures nécessaires pour assurer la cybersécurité de l'appareil. Quel que soit le système d'exploitation utilisé, **configurer l'authentification biométrique permet de sécuriser l'accès au smartphone et autre support mobile.**

La reconnaissance d'empreinte digitale ou faciale peut être combinée avec un mot de passe fort. En cas de perte ou de vol, l'appareil restera verrouillé. Il existe d'autres techniques pour upgrader le niveau de sécurité mobile.

Installer un antivirus

Les antivirus protègent les smartphones et les tablettes des menaces **en scannant les éléments entrants. Il peut s'agir des applications, des pièces jointes ou encore des messages. Ces outils alertent aussi les utilisateurs en cas de site frauduleux ou usurpés. Les meilleurs antivirus proposent une large gamme de fonctionnalités supplémentaires comme l'antivol ou encore la localisation de l'appareil en cas de vol ou de perte.**

Utiliser un VPN

Les VPN vous fournissent essentiellement une connexion téléphonique sécurisée. **Les données sont cryptées et sécurisées en passant d'un serveur à un autre.**

Activer le chiffrement des données

La plupart des smartphones offrent aux utilisateurs la possibilité de **chiffrer les données**. Le cryptage des données protège les informations contre le piratage grâce à l'encodage. Les données ne sont donc pas lisibles en passant d'un serveur à un autre.

Configurer l'effacement à distance

En activant cette fonctionnalité, l'utilisateur peut **supprimer les données à distance**. Cette fonction de sécurité se révèle particulièrement nécessaire en cas de perte ou de vol du mobile.

Protéger les mobiles Android : informations supplémentaires

Les experts en cybersécurité mobile recommandent d'**acheter les appareils Android uniquement auprès des fournisseurs qui publient des correctifs**. Et l'achat des applications se fera seulement sur Google Play. Il faut aussi éviter d'enregistrer les mots de passe et d'activer l'authentification à deux facteurs.

Activer l'ensemble des dispositifs de sécurité intégrés ne peut qu'améliorer le niveau de protection de l'appareil. L'utilisateur doit par ailleurs s'assurer que le réseau Wi Fi utilisé soit sécurisé. Dans le même temps, il faut être particulièrement vigilant par rapport au Wi-Fi public.

N'hésitez pas à explorer notre **top des antivirus pour Android.**

Autres bons à savoir pour les utilisateurs d'iPhone

En plus de l'utilisation de VPN et du chiffrement des données, voici comment sécuriser davantage un appareil iPhone :

- mettre régulièrement à jour leur système d'exploitation
- changer le mot de passe de préréglage de 4 choisir et en choisir un plus fort
- activer la fonction autodestruction qui protège automatiquement l'appareil après 10 tentatives de mot de passe infructueuses
- changer régulièrement les mots de passe iCloud et iTunes
- utiliser uniquement les bornes de recharge pour iPhone de confiance
- révoquer les autorisations d'application pour utiliser la caméra et le microphone.

Mobile Device Management (MDM)

Le MDM est une application permettant la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones, ou d'ordinateurs portables. Cette gestion est effectuée au niveau du service informatique de l'organisation.

L'objectif du MDM est d'harmoniser et de sécuriser la flotte d'appareil de la société en s'assurant que tous les collaborateurs aient des programmes à jour et que leurs appareils soient correctement configurer et sécurisés. Le programme facilite également la propagation de patchs de sécurités ou de nouveaux logiciels pour l'ensemble des collaborateurs.

La MDM gère des tailles et des types de flottes variées allant d'une dizaine de terminaux identiques, jusqu'à des milliers de terminaux tous différents et utilisant différents systèmes d'exploitation.

C'est au début des années 2000 que l'on a vu les solutions de MDM apparaître dans un premier temps pour les PDA, les assistants personnels numériques précurseurs des tablettes numériques.

Principe

- FOTA – Firmware over the air : permet de mettre à jour le système d'exploitation des téléphones et tablettes à distance.
- Monitoring : contrôle les erreurs d'un parc entier de terminaux.
- Prise de contrôle à distance : le plus souvent utilisée pour dépanner les utilisateurs.
- Gestion d'inventaire : inventaire des terminaux actifs, consultation des communications en temps réel…

Securité

- Sauvegarde et restauration : les comptes utilisateurs et les données associées sont enregistrés sur le serveur de l'entreprise, ce qui permet de les restaurer en cas de changement de mobile.
- Blocage et effacement à distance, dans le cas de la perte ou du vol de téléphone.
- Installation de logiciels à travers le réseau cellulaire (over the air : OTA)
- Performance et diagnostics : information sur l'état du terminal, à l'aide de différents indicateurs tels que l'état de la batterie, les informations réseaux, la localisation, le nombre d'heures d'utilisation.
- Gestion du roaming : permet d'interdire ou de limiter l'installation d'applications sur des terminaux se trouvant hors d'un territoire géographique donné.

Différent type de mdm

- MDM monoplateforme : ceux qui n'acceptent qu'un seul système d'exploitation (Microsoft avec son System Center MDM 2008)
- MDM multiplateforme : une approche dite agnostique puisqu'elle ne se limite pas à un système d'exploitation mais permet de gérer des mobiles fonctionnant avec les

principaux OS mobiles, parmi lesquels iOS d'Apple, Android, BlackBerry, Windows phone, voire des systèmes plus anciens tels que Windows Mobile, PalmOS ou Symbian.

Conclusion

Les avancées technologiques dont bénéficient les mobiles révolutionnent la civilisation de l'homme et améliorent son quotidien. Mais il y a un revers à cette médaille. Les gadgets mobiles et connectés peuvent également être dévastateurs s'ils tombent sous les mains des pirates.

Les menaces sont partout, mais il est tout à fait possible de s'en protéger efficacement. La cybersécurité mobile est simple. Il suffit d'**appliquer les règles de sécurité de base** susmentionnées. Une **utilisation responsable de l'appareil** permet aussi de protéger particuliers et entreprises.

Ressource

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/appareils-mobiles

https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf?v=1647428178

https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

https://www.lebigdata.fr/cybersecurite-mobile-dossier

https://bbernede.fr/cours/sio1-bloc3/pdf/Fiche%20techno%204%20-%20La%20s%C3%A9curit%C3%A9%20des%20terminaux%20utilisateurs%20et%20de%20leurs%20donn%C3%A9es.pdf

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf (page 42)

https://www.pgsoftware.fr/blog/solutions-manageengine/securite-des-terminaux-la-cle-de-la-protection-de-votre-entreprise