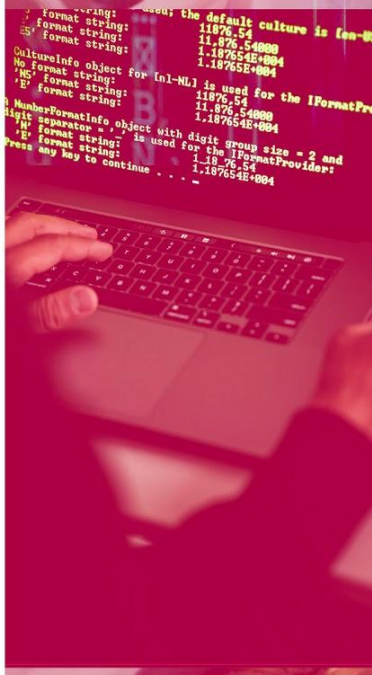
Service de santé des armées

LA LETTRE TRIMESTRIELLE DU SSA SUR LA CYBERSÉCURITÉ ET LES CYBERMENACES

SENSIBILISATION
S'authentifier pour se protéger

ACTUALITÉ DE LA CYBERSÉCURITÉ ET DE LA MENACE

FOCUS DU MOIS
Télétravail : évitez les mauvaises surprises



PREMIER TRIMESTRE 2021

SOMMAIRE

SENSIBILISATION

S'authentifier pour se protéger

L'authentification en ligne pour protéger ses comptes et ses données

L'authentification peut être définie comme une procédure permettant à un système informatique d'obtenir la garantie de l'identité d'une personne ou d'une machine, afin de l'autoriser à accéder à un lieu, un système, un réseau, une application ou des données. **Il s'agit de répondre à la question: qui suis-je et comment puis-je le prouver?**

L'identité numérique est un pilier de la **confiance numérique.**

- La généralisation et la multiplication des applications numériques et des processus et données dématérialisées, ainsi que la multiplication des cyberattaques, rendent indispensable la **protection de l'accès à ses ressources et équipements numériques** grâce à un **processus d'authentification.**
- L'enjeu est de concevoir et de mettre en œuvre des processus d'authentification **sécurisés, simples et respectueux du droit fondamental à la protection des données à caractère personnel**.
- Le niveau d'authentification exigé doit reposer sur une démarche de **gestion des risque.** Il doit être plus ou moins élevé selon les ressources auxquelles il faut autoriser l'accès : comptes bancaires, acte notarié, abonnement à un média en ligne... De même l'authentification d'un administrateur doit être plus forte que celle d'un utilisateur.

Les 3 types de facteurs d'identification

Ce que je sais

Mot de passe, question de sécurité, code PIN, etc. Niveau de sécurité limité, même avec un mot de passe robuste, s'il est utilisé comme facteur unique pour s'authentifier.

Ce que je possède

Dispositif (smartphone, générateur de mot de passe, etc.) permettant de recevoir ou générer un mot de passe unique et à validité limitée (OTP, One-Time Pasword)

Ce que je suis

Analyse biologique (sang, salive, ADN...), analyse morphologique (empreinte digital, reconnaissance faciale, vocale, de l'iris...) et analyse comportementale (signature, façon de marcher, de bouger...),

L'ambition numérique du ministère des Armées prévoit que le ministère se dote de services et de composants techniques novateurs afin de créer un socle technique dont l'une des lignes de force est « **l'identification et l'authentification des différents utilisateurs permettant une gestion optimale des autorisations** ».

Authentification en ligne: à chaque risque sa solution !

⚠️ L'authentification par mot de passe est considérée "faible" s'il est trop simple, car il est alors plus facile à pirater.

✅ Des mots de passe d'au moins 8 caractères comprenant majuscules, minuscules, chiffres et caractères spéciaux.

⚠️ L'utilisation d'un même mot de passe, même complexe, sur plusieurs comptes, permet aux pirates d'accéder à tous vos comptes s'il est compromis ou volé.

✅ Un mot de passe différent pour chaque compte, à changer régulièrement. On peut les sauvegarder dans un gestionnaire de mots de passe, sorte de coffre-fort numérique, comme LockPass et KeePass certifiées par l'ANSSI.

⚠️ L'authentification biométrique n'est pas infaillible ! Utilisée seule, elle est elle aussi réutilisable par l'attaquant qui l'a interceptée (et contrairement à un mot de passe, ne peut pas être renouvelée!).

✅ Associer l'utilisation d'un facteur d'authentification biométrique à un second facteur.

⚠️ La "fédération d'identités" (qui permet de ne s'authentifier qu'une fois pour accéder à plusieurs comptes ou applications) doit être utilisée avec précaution car l'accès à un compte donne accès à tous les autres.

✅ Utiliser un gestionnaire de mots de passe ou des systèmes sécurisés de fédération d'identités (FranceConnect.)

⚠️ La sécurité d'une authentification simple (1 seul facteur), reste limitée, même en respectant les principes ci-dessus.

✅ Pour les comptes les plus sensibles, la solution la plus sécurisée est la combinaison de plusieurs facteurs d'authentification. On parle alors d'**authentification forte**.

On parle d'**authentification forte** lorsque la procédure de vérification de l'identité est composée **d'au moins 2 facteurs d'authentification**. Elle permet de renforcer la sécurité du processus sans affecter l'expérience utilisateur. **Plus le nombre de facteurs est important, plus l'authentification est sécurisée**. Complexifier le processus d'authentification permet de réduire le risque d'usurpation d'identité et de vol de données. La multiplication des facteurs est souvent proposée par les concepteurs d'équipements informatiques (sur les smartphones par exemple, il est souvent possible de choisir d'utiliser 1 ou 2 facteurs d'authentification) ou de solutions (boîtes emails, applications bancaires, etc.).

L'authentification à 2 facteurs (2FA) est de plus en plus généralisée dans de nombreux domaines : accès aux comptes bancaires, aux boîtes email, à des données sensibles, paiements en ligne, etc.. Cette procédure d'authentification engage 2 facteurs, par exemple mot de passe + biométrie ou OTP. Des mesures additionnelles de sécurité peuvent parfois s'ajouter aux facteurs d'authentification utilisés :

- Blocage du processus au bout d'un nombre défini de tentatives d'accès (souvent entre 3 et 5) ;
- Blocage de la carte bancaire dans certains pays, pour éviter les tentatives d'usurpation d'identité.

En France, la carte de professionnel de santé (CPS) est une carte à puce qui permet d'accéder aux systèmes d'information des secteurs de la santé et du médico-social et de sécuriser les échanges, après une authentification d'un niveau de sécurité équivalent à celui des cartes bancaires.

La CPS peut maintenant être remplacée par une application pour smartphone, la e-CPS, qui permet au professionnel de santé de se connecter aux systèmes d'information santé et médico-social sans avoir besoin d'un ordinateur configuré et équipé d'un lecteur de carte.

ACTUALITÉ DE LA CYBERSÉCURITÉ ET DE LA MENACE

Cyberattaques, l'autre crise de la Covid-19

Une augmentation spectaculaire des cyberattaques

La société Imperva Research Lab a observé une augmentation de 51% des cyberattaques contre le secteur de la santé en décembre 2020, suite à l'arrivée des premiers vaccins contre la Covid-19. Cette augmentation spectaculaire marque la fin d'une année particulièrement lourde puisqu'en 2020, le secteur de la santé a subi en moyenne 187 millions de cyberattaques par mois au niveau mondial, soit environ 500 attaques par organisme de santé. Cela représente une augmentation de 10% par rapport à 2019, et souligne la vulnérabilité croissante des organisations du secteur de la santé, pour la plupart débordées par les conséquences de la crise sanitaire.

Parmi les principaux pays visés : les États-Unis, le Brésil, le Royaume-Uni et le Canada, qui a connu l'augmentation la plus spectaculaire, avec une augmentation du nombre d'attaques de plus de 250%, suivi de près par l'Allemagne (+220%). En France, l'augmentation des cyberattaques, contre des organisations du secteur de la santé, plus faible mais non négligeable, s'élève à 26%.

Le gain financier reste la motivation première des attaquants, juste avant la déstabilisation

La majeure partie des attaques actuelles visent à voler des données personnelles de santé ou des secrets pharmaceutiques pour les revendre, ou à bloquer les systèmes numériques des établissements de santé jusqu'au paiement d'une rançon (*ransomware*, ou rançongiciel). D'autres n'ont pour but que de déstabiliser les États et les organisations de santé, déjà sous forte pression en raison de la crise sanitaire.

Les attaques par rançongiciel, en très forte augmentation, créent des situations dramatiques dans les organismes de santé visés, surtout en cette période d'extrême tension médicale, car le blocage de leurs activités font peser un risque très élevé sur la vie de nombreux patients. Ce constat a conduit les cybercriminels à cibler plus encore les établissements de soin, espérant que les risques encourus les inciteront à payer rapidement les rançons demandées.

Exemple parlant, en septembre 2020, une cyberattaque apparemment dirigée contre la mauvaise cible a bloqué les systèmes informatiques d'un hôpital de Düsseldorf : conséquence dramatique de cette attaque, une patiente devant être opérée d'urgence a dû être transférée dans une autre ville et est décédée lors du trajet. En France, les campagnes de ransomware visant des hôpitaux ont marqué l'actualité récente, comme à Dax ou à Villefranche-sur-Saône où les activités des deux établissements ont été sérieusement affectées.

Des pirates vendent des données volées sur le vaccin Pfizer-BioNTech

Des documents confidentiels sur le vaccin Pfizer-BioNTech ont été dérobés à l'Agence européenne des médicaments en décembre 2020 puis mis en vente sur dark web. Des informations relatives à des "médicaments contre la Covid-19", également dérobées à cette Agence, ont aussi été divulguées par les cybercriminels.

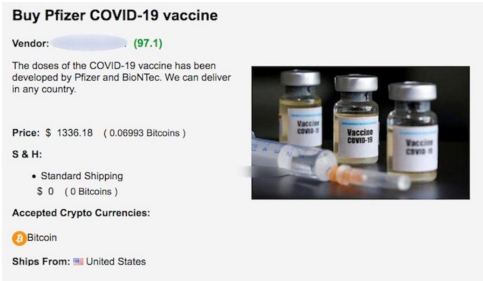
Le laboratoire AstraZeneca, à l'origine d'un autre vaccin contre la Covid-19, a lui aussi fait l'objet d'attaques.

Les vaccins anti-Covid dans le viseur des cybercriminels

De faux vaccins vendus à prix d'or sur le dark web

Des doses de vaccins anti-Covid contrefaits sont en vente sur le dark web depuis novembre 2020. Les transactions sont réalisées en Bitcoin. Les prix équivalents en euros oscillent généralement entre 250 et 800€ pour une dose, mais pourraient aller jusqu'à 20 000€.

L'émergence d'un marché noir de vaccins anti-covid sur le dark web s'explique notamment par la crainte d'une troisième vague de la pandémie et l'apparition des variants.



Exemple d'interface de vente de faux vaccins anti-Covid-19 sur le dark web

La vente de sang de patients atteints de la Covid-19 aurait également été repérée sur le dark web, avec la garantie d'une "immunité à vie" contre le virus s'il était injecté à une personne saine.

Les données personnelles de santé, le casse-tête cyber

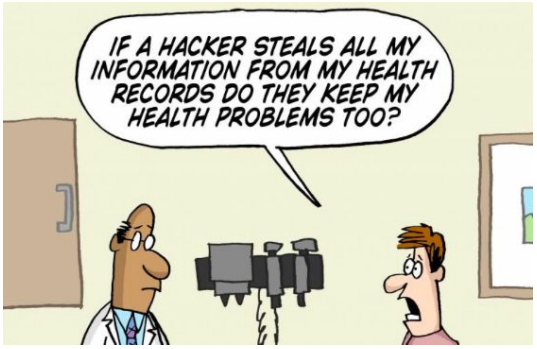
La protection des données personnelles est aujourd'hui un véritable enjeu. De plus en plus de patients exigent que la confidentialité de leurs données de santé soit assurée sans faille par les établissements de santé. Au sein de ceux-ci, le délégué à la protection des données et le responsable de la sécurité des systèmes d'information ont pour mission d'informer, de sensibiliser et de conseiller le personnel aux enjeux de la protection des données et aux bonnes pratiques de cybersécurité.

La médecine libérale ne fait pas exception. En décembre 2020, la CNIL a sanctionné deux médecins libéraux pour n'avoir pas suffisamment protégé les données personnelles de leurs patients et laisser fuiter des images médicales sur Internet. Les serveurs informatiques hébergeant ces images étaient insuffisamment protégés. La CNIL rappelle qu'elle préconise l'usage de solutions présentant "*le maximum de garanties en termes de sécurité informatique et de protection des données personnelles*" et alerte sur "*la prudence au moment de l'élaboration et du paramétrage de leur système informatique interne, en s'entourant si nécessaire de prestataires compétents en la matière*".

Une problématique au coeur de la crise de la Covid-19

La problématique de la protection des données de santé s'est renforcée depuis le début de la crise sanitaire de la Covid-19. Les établissements de santé, débordés, n'ont pas forcément le temps de gérer les dossiers de manière optimale et omettent parfois involontairement d'appliquer les précautions d'usages relatives à la confidentialité des données personnelles des patients.

Or, les données de santé volées sont faciles à revendre sur le dark web, où se tient depuis plusieurs années un véritable marché noir des dossiers médicaux.



"Si un pirate vole toutes les données de mes dossiers médicaux, est-ce qu'il récupère aussi mes problèmes de santé ?"

Pour un patient maître de ses données de santé

En janvier 2021, le Cercle Prévention & Santé et le Club Numérique & Territoires ont publié un livre blanc intitulé "Pour un patient maître de ses données de santé", qui appelle, entre autres, à :

- Intensifier la formation et la sensibilisation des professionnels de santé aux nouvelles technologies et en particulier à la collecte et à l'utilisation des données ;
- Créer des mécanismes d'information automatique des patients sur l'usage de leurs données et leur donner la possibilité de faire jouer leur droit d'opposition ;
- Renforcer les standards de cybersécurité qui doivent être respectés par les acteurs traitant des données de santé.

7 raisons qui font du secteur de la santé une cible privilégiée

1. **Les données personnelles de santé s'échangent à prix d'or sur le dark web**. Les données de santé volées, particulièrement sensibles, représentent également un moyen de pression en cas d'attaque par rançongiciel (ransomware) : les établissements de santé sont incités à payer la rançon demandée pour retrouver l'accès aux systèmes paralysés et éviter la publication des données personnelles volées.

2. **Les dispositifs médicaux connectés constituent autant de points d'entrée faciles d'accès pour les cyber-attaquants** : plus un établissement ou un praticien utilise de dispositifs connectés, plus la surface d'attaque est étendue et les points d'entrée nombreux vers le système d'information de l'établissement ou du praticien.

3. **Le nombre important de dispositifs connectés utilisés dans les établissements de santé rend leur sécurisation difficile** : les établissements de santé disposent d'un vaste réseau de dispositifs médicaux connectés, allant jusqu'à plusieurs milliers pour les établissements les plus gros, tous connectés au même réseau. Chaque dispositif représente un point d'entrée potentiel (cf. point 2).

4. **Les données de santé doivent être facilement et rapidement échangeables** : les données des santé doivent être accessibles au personnel, tant sur place qu'à distance, et sur plusieurs appareils simultanément. Le personnel doit pouvoir partager les informations immédiatement, souvent dans l'urgence, et parfois au détriment de certaines considérations de sécurité.

5. **Le personnel médical accède aux données de santé des patients depuis des dispositifs différents, ce qui multiplie les points d'entrée sur le SI de l'organisme concerné.** Certains pratiquent à l'hôpital, d'autres en libéral, d'autres encore au sein du même établissement mais dans des services différents...

6. **Le personnel médical n'est pas forcément formé aux risques cyber** : ils n'ont souvent tout simplement ni le temps, ni les ressources nécessaires pour se former ou être formés aux nouveaux usages et aux risques associés.

7. **Certains équipements sont vieillissants** : par manque de budget, certains établissements restent équipés de technologies vieillissantes et donc potentiellement vulnérables.

L'ENISA veut aider le secteur de la santé à adopter le *cloud* en toute sécurité

Depuis décembre 2020, la Commission européenne met en oeuvre l'initiative de l'Espace européen des données sur la santé afin de promouvoir l'échange sécurisé des données des patients et l'accès aux données de santé.

Dans ce cadre, l'Agence européenne de cybersécurité (ENISA) a publié en janvier 2021 un rapport intitulé *Cloud Security for Healthcare Services*. Le rapport évalue les risques de cybersécurité des services *cloud* et propose des bonnes pratiques pour leur intégration sécurisée dans le secteur de la santé. Il fournit notamment des lignes directrices en matière de cybersécurité pour trois domaines dans lesquels les services *cloud* sont utilisés :

- Les dossiers médicaux électroniques (collecte, stockage, gestion et transmission de données de santé, telles que les résultats d'examens médicaux) ;
- La télémédecine, qui permet la consultation à distance entre le patient et le médecin ;
- Les dispositifs médicaux connectés dont les données collectées sont stockées dans le cloud.

Actualité des vulnérabilités : la cyberveille de l'ANS

L'ANS (Agence du Numérique de Santé) a lancé en 2019 le Portail d'Accompagnement Cybersécurité des Structures de Santé, sur lequel elle publie des instructions ministérielles et des guides de bonnes pratiques en matière de cybersécurité. Elle y diffuse aussi une veille quotidienne sur les actualités et sur les menaces propres au secteur de la santé. Des bulletins et alertes de sécurité relatives aux équipements biomédicaux sont ainsi fournis en temps réel dans l'onglet Cyberveille Santé du portail.

Digitalisation des soins : télémédecine et hôpital de demain

L'essor de la télémédecine

Fin 2019, l'Agence du Numérique en Santé (ANS) a lancé un baromètre sur la Télémédecine afin de mesurer l'adhésion des Français à ce nouveau service. Sans surprise, le recours à la télémédecine explose depuis le début de la crise sanitaire de la Covid-19. Les professionnels de santé soulignent cependant que les outils logiciels disponibles sont trop nombreux et manquent d'interopérabilité.

L'explosion du recours à la télémédecine doit s'accompagner d'une sécurité renforcée des solutions utilisées afin de garantir la confidentialité des données de santé des patients.

Hôpital du futur : 5 tendances à suivre

1. **L'utilisation de la réalité virtuelle pour les soins** : traitement des douleurs chroniques, traitement du stress post-traumatique, accompagnement d'enfants autistes pour les aider à interagir avec le monde extérieur, etc.
2. **La généralisation de l'usage de wearables pour le suivi de santé** : capteurs de rythme cardiaque, dispositifs de mesure de la glycémie en continu, oxymètres connectés pour mesurer le taux d'oxygénation du sang, etc.
3. **La médecine prédictive** : utilisation du big data (volume massif de données) et de l'intelligence artificielle pour prédire l'évolution de la santé d'un individu, la propagation d'un virus, etc.
4. **La généralisation de l'intelligence artificielle** : pour l'aide à la décision médicale, l'assistance à la chirurgie assistée par ordinateur, la médecine prédictive, la recherche de nouveaux médicaments ou encore la médecine sur-mesure grâce au développement de molécules spécifiquement adaptées à chaque patient.
5. **La blockchain pour protéger les données de santé** : la blockchain est une technologie de stockage et de partage d'informations de manière immuable et horodatée. Il s'agit d'un registre sécurisé qui pourrait permettre de stocker les données de santé et de les protéger de toute tentative de modification et d'effacement.

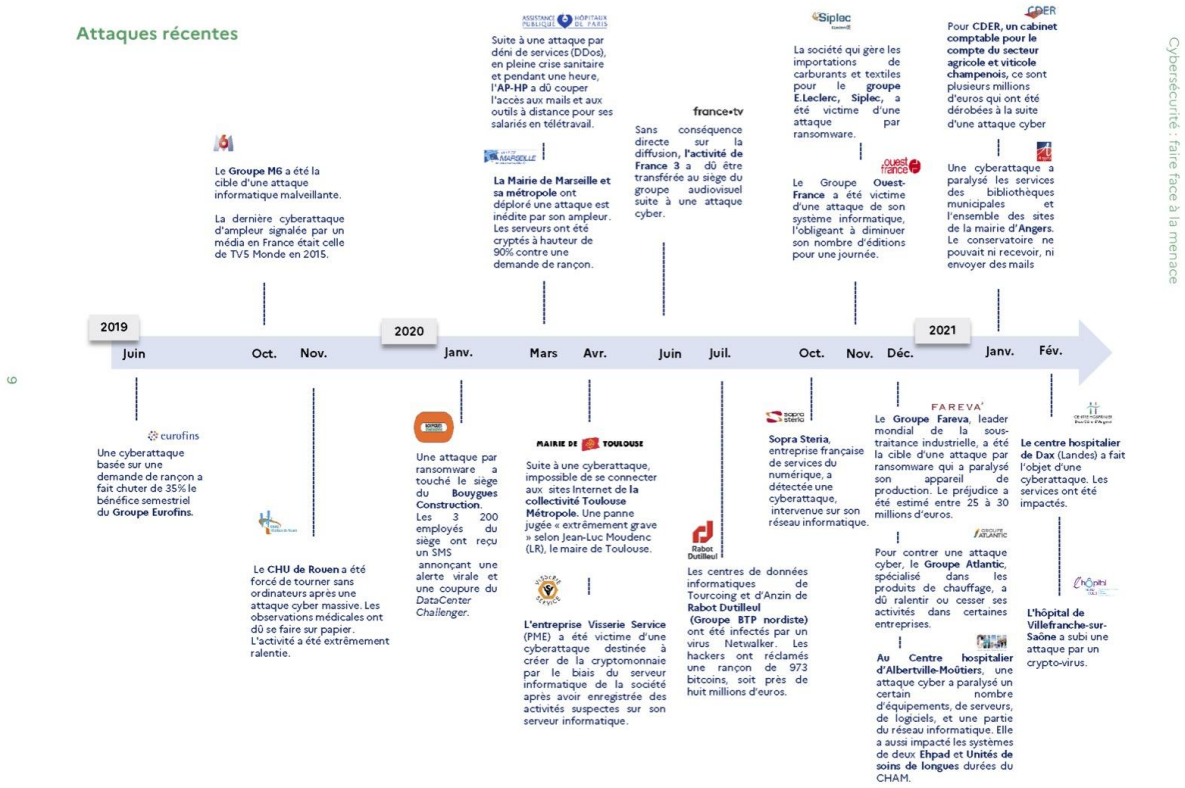
Le gouvernement français lance une stratégie nationale pour la cybersécurité

Afin de faire face à l'augmentation des cyberattaques, le Gouvernement a lancé en février 2021 une **stratégie nationale pour la cybersécurité**, dont les principaux objectifs à l'horizon 2035 sont :

- la multiplication par trois du chiffre d'affaires de la filière française de la cybersécurité (passant de 7,3 milliards à 25 milliards d'euros) ;
- positionner la France par rapport à la concurrence internationale, notamment en doublant les emplois de la filière (passant de 37 000 à 75 000) ;
- structurer la filière et repositionner la France par rapport à la concurrence internationale en nombre d'entreprises ;
- faire émerger trois champions français de la cybersécurité en s'appuyant sur les grandes start-ups du secteur, notamment celles membres de la French Tech 120 ;
- diffuser une véritable culture de la cybersécurité dans les entreprises ;
- stimuler la recherche française en matière de cybersécurité et d'innovation industrielle (en visant une hausse de 20% des brevets).

Pour la mise en oeuvre de cette stratégie, le Gouvernement a mobilisé 1 milliard d'euros, dont 720 millions de financements publics issus du plan France Relance et du Programme d'investissement d'avenir.

L'infographie ci-dessous, issue de la présentation de la stratégie nationale pour la cybersécurité, présente les plus grosses cyberattaques ayant eu lieu en France depuis juin 2019. Celles-ci ont essentiellement touché des grands groupes (M6, Eurofins, Bouygues Construction, France TV, Rabot Dutilleul, Sopra Steria, etc.), des administrations publiques (Mairies de Marseille, Toulouse, d'Angers, etc.), ainsi que des établissements de santé (CHU de Rouen, AP-HP, centre hospitalier de Dax, hôpital de Villefranche-sur-Saône, etc.).



FOCUS

Télétravail : évitez les mauvaises surprises

Comment télétravailler en toute (cyber)sécurité

La crise sanitaire de la Covid-19 a porté le télétravail sur le devant de scène et par là même mis en lumière les risques qu'il comporte. Le télétravail n'est pas une pratique nouvelle, de nombreuses entreprises et organisations le proposaient déjà de manière systématique ou ponctuelle à leurs salariés. Le travail en mobilité (déplacement, opération, mission) est également assimilé à du télétravail, puisque le travail est réalisé à distance et nécessite une connexion et un partage d'information avec le siège de l'organisation.

La pandémie de la Covid-19 a poussé les entreprises à basculer brutalement vers le télétravail afin de préserver leur activité, y compris lorsque cette modalité n'était pas encore déployée en leur sein. La transition a parfois été très (voire trop) rapide, et les risques en matière de sécurité peu ou mal appréhendés. Selon l' étude When the World Stayed Home de la société Tanium, menée en juin 2020 auprès de 1004 dirigeants américains, britanniques, français et allemands, 85% d'entre eux s'estimaient prêts à adopter le télétravail comme pratique exclusive alors même que 98% d'entre eux ont dû faire face à des problématiques de sécurité au cours de cette transition.

Télétravail : les principales menaces

Le télétravail accroît des menaces et des risques déjà existants sur les entreprises et organisations publiques :

Perte ou vol des outils informatiques : en télétravail, les employés utilisent leurs appareils dans des lieux divers (domicile, cafés, hôtels, restaurants, lieux de conférence, gares, aéroports...). Un appareil peut être perdu ou volé et utilisé par des individus mal intentionnés pour accéder au réseau de l'entreprise et/ou récupérer des informations.

Réseaux de communication faiblement sécurisés : les télétravailleurs utilisent des réseaux non maîtrisés par l'entreprise (wifi du domicile, wifi public, 4G, etc.), souvent peu sécurisés, ce qui peut favoriser l'interception d'informations ou l'accès aux appareils utilisés.

Vulnérabilité des appareils personnels : utilisés à des fins professionnelles, les appareils personnels présentent un risque. Souvent connectés sur des réseaux externes à l'entreprise ou l'organisation publique, ils sont susceptibles d'être infectés par des virus informatiques ou atteints par des pirates. Un fois connectés au réseau interne de l'entreprise, ils deviennent un vecteur potentiel d'infection. De plus, en cas de travail dans un lieu public il est également pertinent d'utiliser un filtre de confidentialité afin de protéger l'écran de tout regard curieux.

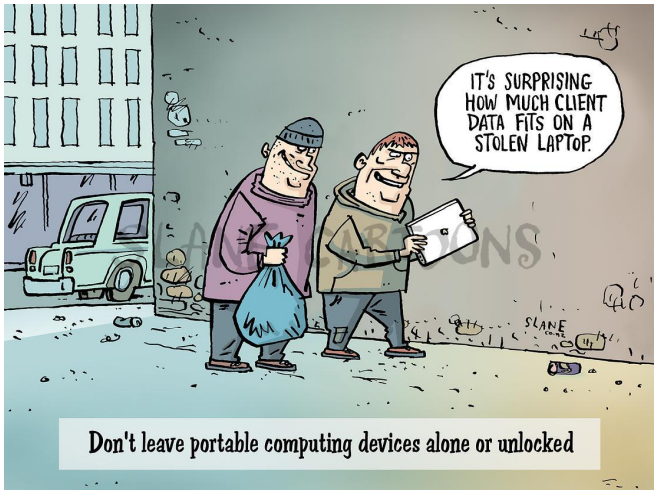
Le télétravail en 3 questions

Avec quoi les télétravailleurs travaillent-ils? Ordinateurs, smartphones, tablettes... Ils peuvent être fournis par l'entreprise ou il peut s'agir d'appareils personnels utilisés à des fins professionnelles. En télétravail depuis chez eux, les employés utilisent principalement leur box Internet personnelle. S'ils travaillent depuis un hôtel, un aéroport, un café, ou tout autre espace public, ils utilisent parfois le wifi gratuit du lieu en question.

Quelles activités les télétravailleurs réalisent-ils? Les activités sont variées : échange d'emails, utilisation de bases de données et dossiers partagés, utilisation d'applications de messagerie instantanée et d'applications professionnelles, recherches sur Internet, etc.

Quels sont les principaux objectifs de sécurité en télétravail? La disponibilité des ressources à distance, la confidentialité des communications et des données, l'intégrité des informations échangées et la garantie de l'authentification du salarié.

"Tu devrais vraiment t'équiper d'un filtre de confidentialité"
"Ne faites pas l'autruche en matière de protection des données"



"C'est surprenant le volume de données clients qu'on peut trouver sur un ordinateur volé"
"Ne laissez pas un appareil mobile seul ou déverrouillé"

Quelques principes de base pour télétravailler en tout sécurité

En réponse aux menaces précédemment décrites, quelques principes de base sont nécessaires pour télétravailler de manière sécurisée :

- **Mettre en place le travail à domicile ne consiste pas simplement à dire aux employés de travailler chez eux.** Il est fondamental de mettre en place un certain nombre de mesures et de bonnes pratiques pour assurer la sécurité des équipements informatiques utilisés pour télétravailler, ainsi que de la connexion et des informations échangées. En effet, peu ou pas sensibilisés, nombreux sont ceux qui ne procéderont pas à la mise à jour de leurs appareils et antivirus, qui mélangeront parfois les messageries personnelles et professionnelles, qui se connecteront sur des réseaux wifi peu sécurisés...
- **Les données de l'organisation doivent être catégorisées**. Les données les plus sensibles doivent ainsi être particulièrement protégées : leur accès à distance peut être plus sécurisé que pour les données moins stratégiques, voire interdit. De même, il convient de limiter le stockage de données sensibles sur les appareils mobiles des employés, et de mettre en place des systèmes d'authentification forte pour accéder aux ressources informatiques de l'entreprise.
- **Les flux d'échanges de données entre les terminaux qui servent au télétravail et le système d'information de l'entreprise, doivent être sécurisés** grâce à la mise en place d'un réseau privé virtuel (VPN - cf. encart ci-dessous).
- **Une solution sécurisée de visioconférence doit être mise en place** afin d'assurer la confidentialité des échanges.

Au sein des entreprises et organisations publiques, les directeurs des systèmes d'information (DSI) sont en charge d'assurer le bon fonctionnement de l'environnement informatique. C'est également à lui que revient de s'assurer que les employés sont équipés et suffisamment sensibilisés pour télétravailler de manière sécurisée.

Un réseau privé virtuel (VPN, Virtual Private Network) est une sorte de tunnel sécurisé et chiffré qui permet d'échanger des données entre des systèmes informatiques distants de manière totalement séparée des autres flux présents sur le réseaux utilisé.

Dans le cadre du télétravail, un VPN permet ainsi d'utiliser son réseau personnel ou un réseau public pour connecter le poste du télétravailleur au système d'information de son entreprise et échanger des données en toute sécurité.

Cybersécurité et télétravail : le risque zéro n'existe pas

Comme les entreprises et administrations, les pirates et individus malveillants se sont adaptés à la crise et en profitent pour exploiter les vulnérabilités des entreprises et des employés. Beaucoup ciblent les équipements personnels pour accéder aux systèmes professionnels. Ce mode d'action est particulièrement efficace si le propriétaire de l'équipement personnel visé l'utilise pour travailler à distance. D'autres attaquants utilisent le phishing, ou hameçonnage, une méthode classique qui consiste à envoyer un email d'apparence légitime afin obtenir du destinataire ses identifiants de connexion ou des données confidentielles comme les coordonnées bancaires. Ces emails frauduleux sont aujourd'hui de plus en plus sophistiqués et donc de plus en plus crédibles, et les pirates réussissent parfois à accéder aux réseaux professionnels après avoir obtenu des identifiants d'accès de la part d'employés. Les applications les moins utilisées par les usagers, et donc rarement mises à jour, sont également des cibles faciles car elles peuvent constituer une brèche de sécurité dont ils peuvent profiter.

Les pirates ciblent autant les grosses structures que les plus petites, entreprises privées comme organismes publics. De plus, le risque ne s'arrête pas à la fin de la journée de travail, la sécurité des équipements doit être assurée 24/24.

Pour aller plus loin

Le site cybermalveillance.gouv.fr a publié un ensemble de recommandations de cybersécurité pour le télétravail. Si cet article s'ancre dans le contexte de la crise sanitaire de la Covid-19, l'ensemble des recommandations s'appliquent au télétravail et au travail en mobilité en dehors de toute situation de crise.

EN BREF

Optimiser la sécurité des vos appareils connectés en télétravail

Mettre à jour le système d'exploitation de ses objets connectés

Vérifier les applications installées : sont-elles nécessaires? Quelles applications fonctionnent sans être ouvertes?

Désinstaller ou déconnecter les applications non utilisées : attention, effacer une icône du bureau ne désinstalle pas une application)

Vérifier les autorisations que vous donnez aux applications : les accès que vous approuvez permettent à l'application de mettre en place des actions potentiellement dangereuses

Utiliser, si possible, un appareil (ordinateur, téléphone) professionnel : si vous utilisez un appareil personnel, assurez-vous de connaître les bons usages de cybersécurité

Vérifier vos comptes bancaires régulièrement pour repérer d'éventuelles opérations inhabituelles

Sensibiliser les enfants aux règles élémentaires de cybersécurité : utiliser le contrôle parental lorsqu'ils utilisent vos objets connectés et lorsqu'ils sont en ligne

Installer un anti-virus ou mettre à jour l'anti-virus en place ainsi que tous les logiciels de sécurité

S'assurer que la connexion wifi est sécurisée et changer le mot de passe par défaut de la box

Mettre en place un VPN avec le DSI ou son partenaire informatique

Vérifier la source avant de cliquer sur un lien ou d'ouvrir une pièce jointe : une demande inhabituelle de la part d'une connaissance doit alerter, appeler la personne avant de cliquer

S'assurer que l'accès aux documents internes est bien encadré afin d'éviter les fuites de données vers l'extérieur et éviter, autant que possible, de partager des documents en pièce jointe avec l'externe.

Créer des mots de passe renforcés, éviter d'utiliser le même sur différents comptes et se méfier des emails demandant de vérifier ou renouveler un identifiant de connexion ou un mot de passe si vous n'avez pas initié la démarche

Eviter de supprimer les paramètres de sécurité du système de votre opérateur

Permettre les synchronisations et les sauvegardes automatiques : cela sera utile en cas de vol de votre appareil

Sauvegarder les fichiers importants (sur des disques durs externes ou un cloud fiable) et utiliser un outil de chiffrement des fichiers et du disque dur

SSA et télétravail : les bonnes pratiques

Les différentes mesures de sécurité mises en oeuvre dans le civil sont déclinées via les **solutions de mobilité de l'Intradef (SMOBI)** :

- le **Token USB** crée un **VPN** entre vos smartphone, tablette ou ordinateur portable et le réseau Intradef pour éviter l'interception des données ;
- le **chiffrement du disque dur** au démarrage évite l'accès aux données stockées en local en cas de perte ou de vol, et sert d'ultime rempart ;
- l'association d'une **identification en cascade pour le déchiffrement**, puis l'**accès Windows** et le **pont VPN** vers l'intradef (Token) donnent une **authentification forte**, qui permet à chacun de travailler en sécurité en protégeant les Armées.

Evitez d'écrire vos mots de passe sur des post-its!
Source : CNIL

Afin que cela fonctionne, chacun doit rester vigilant et mettre en œuvre les bonnes pratiques.

Rapprochez-vous de votre officier ou correspondant de sécurité des systèmes d'information (OSSI ou CSSI) pour toute question.

Les solutions proposées

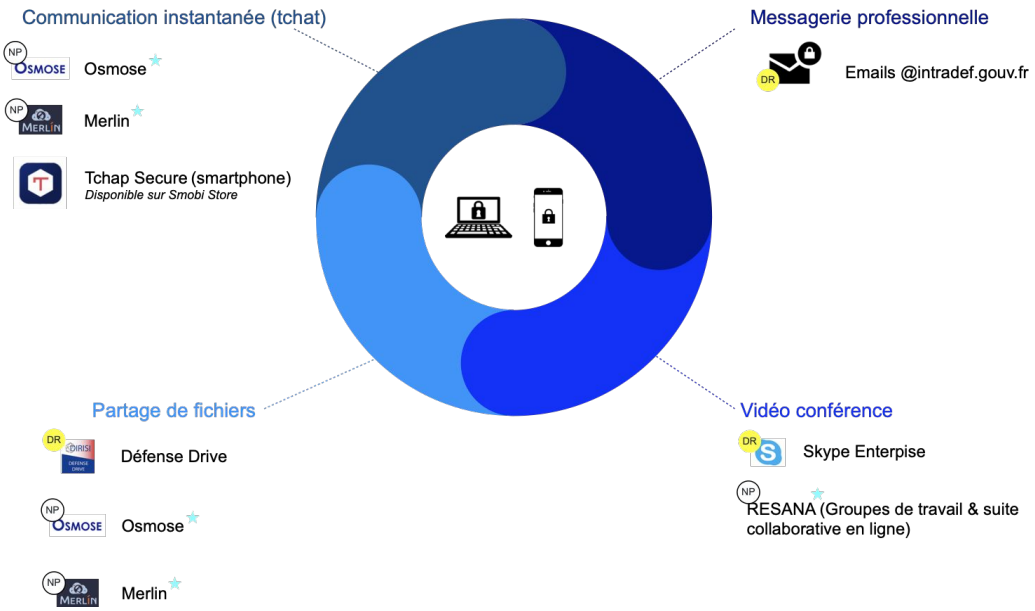
Le ministères des Armées a mis en place plusieurs outils afin de permettre à son personnel de travailler en mobilité de manière sécurisée, notamment :

- Défense Drive → guide d'utilisation disponible ici
- Merlin → contexte d'utilisation expliqué ici & tutoriels disponibles ici et ici
- Tchap → Guide d'utilisation disponible ici & plus d'informations ici
- Osmose
- RESANA

Certains outils externes sont également utilisés, tels que Skype Enterprise et Tixeo.

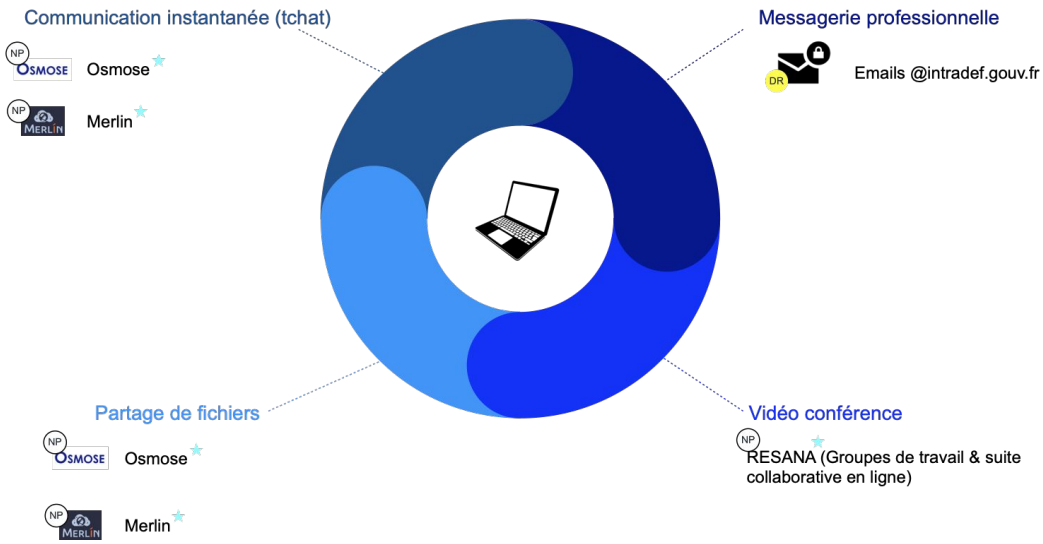
Leur utilisation est résumée dans les infographies ci-après:

Scénario 1: PC et smartphone SMOBI

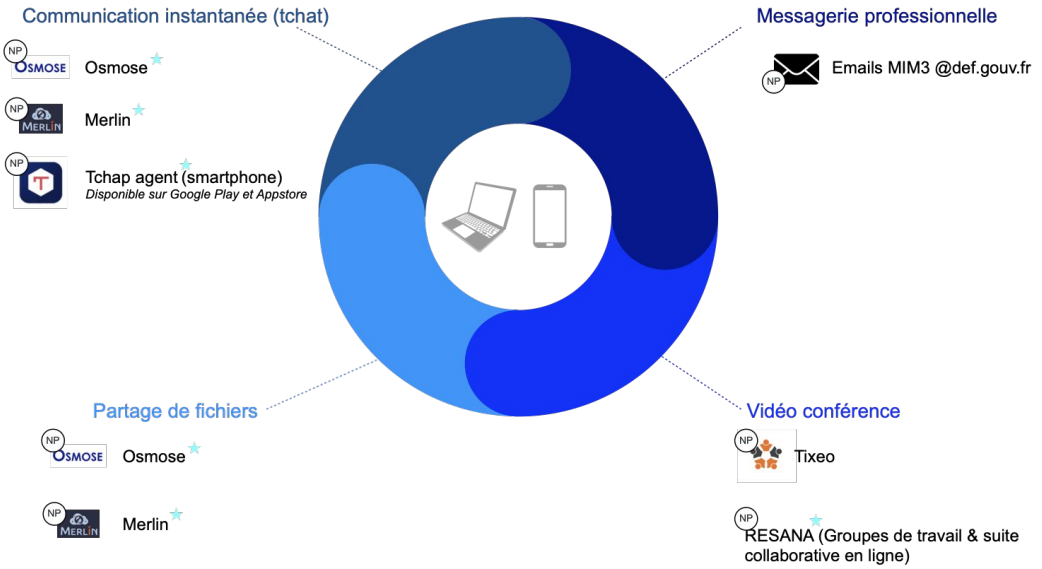


DR Diffusion Restreinte NP Non Protégé ★ Ouvert aux externes

Scénario 2: Poste IntraDef non SMOBI



Scénario 3: Poste personnel



DR Diffusion Restreinte NP Non Protégé ★ Ouvert aux externes

BIBLIOGRAPHIE

Sensibilisation

https://www.ssi.gouv.fr/entreprise/glossaire/

https://www.ssi.gouv.fr/uploads/2020/12/guide_protection_des_systemes_essentiels.pdf

https://www.youtube.com/watch?v=XCr7Mi8D7-c&feature=youtu.be

https://www.kaspersky.fr/blog/stealing-digital-identity/4997/

https://esante.gouv.fr/securite/cartes-et-certificats/CPS

https://esante.gouv.fr/securite/e-cps

Actualité

https://www.imperva.com/blog/web-application-attacks-on-healthcare-spike-51-as-covid-19-vaccines-are-introduced/

https://www.globalsecuritymag.fr/Les-attaques-contre-les-organismes,20210106,106892.html

https://infodsi.com/articles/188140/pourquoi-les-cyber-attaques-contre-les-organismes-de-sante-explosent.html

https://www.bbc.com/news/technology-55411830

https://www.enisa.europa.eu/news/enisa-news/securing-cloud-services-for-health

https://www.digitalauthority.me/resources/state-of-digital-transformation-healthcare/

https://www.comarch.fr/livres-blancs/lb-la-telesurveillance-des-patients/lb-la-telesurveillance-des-patients/?utm_campaign=remote%20patient%20monitoring&utm_medium=pop-up&utm_source=pop-up%20page%20Healthcare

https://esante.gouv.fr/actualites/lans-publie-un-nouveau-barometre-sur-la-telemedecine

https://www.usine-digitale.fr/editorial/quelles-pistes-pour-ameliorer-le-soin-digital-10-ans-apres-le-lancement-de-la-telemedecine.N1045619

https://www.rts.ch/info/sciences-tech/11898342-la-sante-numerique-star-du-salon-de-linnovation-virtuel-de-las-vegas.html

https://www.dsih.fr/article/4069/pour-un-patient-maitre-de-ses-donnees-de-sante.html

https://www.usine-digitale.fr/article/la-cnil-sanctionne-deux-medecins-pour-violation-de-donnees-de-sante.N1042589

https://www.clubic.com/pro/actualite-349429-donnees-de-sante-le-dpo-du-chu-de-bordeaux-partage-son-retour-d-experience.html

https://www.lci.fr/sante/donnees-personnelles-la-cnil-valide-le-fichier-si-vaccin-covid-et-promet-des-controles-2174229.html

https://www.usine-digitale.fr/article/les-donnees-volees-du-vaccin-pfizer-biontech-ont-ete-publiees-sur-internet.N1048714

https://www.estrepublicain.fr/sante/2021/01/06/vaccins-contre-le-covid-19-des-faux-produits-sur-le-dark-web-mis-en-vente-jusqu-a-1-000-dollars

https://www.leparisien.fr/high-tech/des-fioles-a-1000-dollars-sur-le-dark-web-l-autre-campagne-de-vaccination-contre-le-covid-05-01-2021-8417365.php

https://www.cnbc.com/2021/01/13/covid-19-vaccines-scammers-claim-to-sell-doses-on-dark-web-for-bitcoin.html

https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

http://www.compublics.com/sites/default/files/u3/livre_blanc_sante_2.pdf

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-A-European-Health-Data-Space-

https://www.cyberveille-sante.gouv.fr

https://www.lesechos.fr/industrie-services/pharmacie-sante/la-blockchain-un-remede-aux-donnees-de-sante-1221651

https://www.futura-sciences.com/sante/questions-reponses/corps-humain-sante-intelligence-artificielle-revolution-nous-attend-14432/

Focus

https://www.cadre-dirigeant-magazine.com/manager/le-salarie-en-teletravail-est-il-un-danger-pour-la-cybersecurite-de-lentreprise/

https://www.gatewatcher.com/fr/nos-actualites/blog/cybersecurite-et-teletravail-lequation-impossible

https://www.matthieu-tranvan.fr/management/double-authentification.html

https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/

https://effectiveyellow.com/le-dossier-teletravail-conseils-pour-securiser-cette-pratique-devenue-courante/

https://effectiveyellow.com/le-dossier-le-teletravail-remet-la-cybersecurite-sur-le-devant-de-la-scene/

https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

https://www.tchap.gouv.fr

https://www.numerique.gouv.fr/uploads/tchap-prise-en-main.pdf

https://www.numerique.gouv.fr/outils-agents/tchap-messagerie-instantanee-etat/

https://merlin.defense.gouv.fr

http://portail-armees.intradef.gouv.fr/transformation/index.php/2-non-categorise/980-merlin-une-offre-de-la-dirisi-pour-le-travail-collaboratif-en-toute-securite-de-l-intradef-vers-l-internet

https://portail-smobi.intradef.gouv.fr/images/video/Merlin-Fonctionnalites.mp4

https://portail-smobi.intradef.gouv.fr/images/video/Merlin-tutoriel.mp4

https://osmose.numerique.gouv.fr

https://resana.numerique.gouv.fr

https://defense-drive.intradef.gouv.fr

https://defense-drive.intradef.gouv.fr/pfv2-sharing/sharings/tl6ilcOK.AqqOqmqH#/files

Cette Lettre trimestrielle est réalisée par ceis avisa partners