Université de Lille

Note de service
Sécurité des postes de travail

—
Direction générale déléguée
Numérique

—

Affaire suivie par :
Cédric Foll
Directeur général délégué au numérique
cedric.foll@univ-lille.fr
T. +33 (0)6 37 24 06 55

Le Directeur général délégué au numérique

à
Mesdames et Messieurs les Doyennes et Doyens

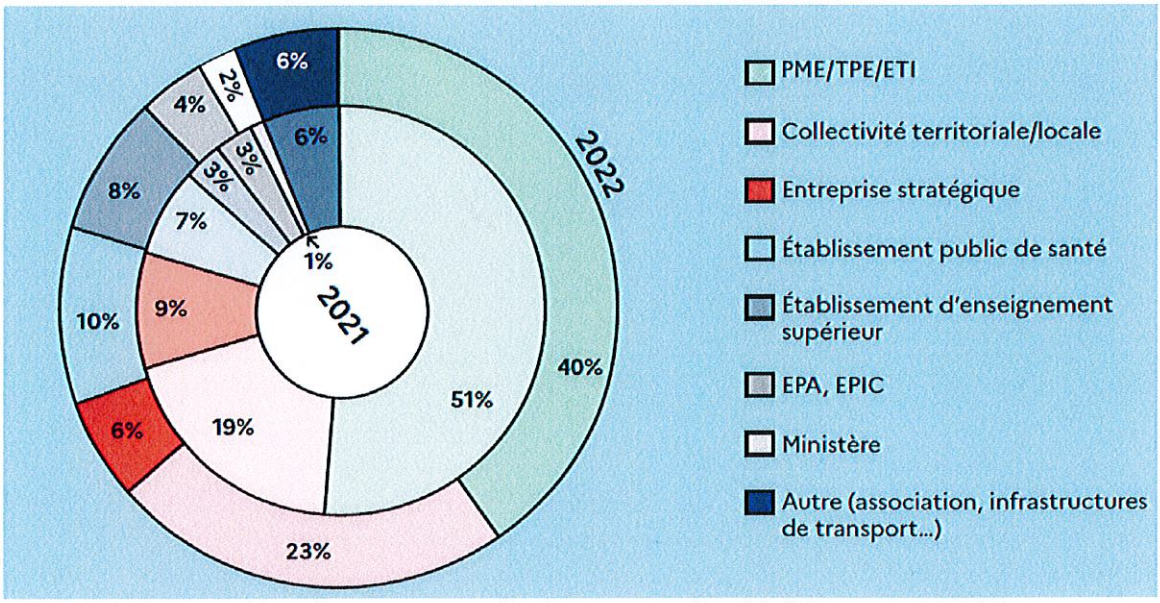
Mesdames et Messieurs les Directrices et Directeurs de composante

Mesdames et Messieurs les Directrices et Directeurs des services communs

Mesdames et Messieurs les Directrices et Directeurs des services d'appui

Lille, le 25 janvier 2024

La menace pesant sur les systèmes informatiques ne fait que croître, et plusieurs établissements ont subi de graves préjudices à la suite de compromissions ces dernières années et particulièrement depuis 2021.



Répartition des attaques selon le secteur d'activité (Source : ANSSI)

Les postes de travail représentent l'un des principaux points de vulnérabilité des systèmes d'information. Il est donc nécessaire d'apporter un soin tout particulier à leur connaissance, à leur configuration et à leur gestion.

Dans le but de limiter les risques, l'Université de Lille a choisi de mettre en place un ensemble de prérequis pour la connexion de terminaux à son réseau.

Les mesures figurant dans ce document s'appuient sur les recommandations de l'Agence Nationale de sécurité des systèmes d'information (ANSSI) et sur la politique de sécurité du système d'information de l'établissement (PSSI).

Il est important que ces préconisations soient appliquées à l'ensemble des ordinateurs en service au sein de l'établissement, quelle qu'en soit le service détenteur et la source de financement de l'équipement.

La configuration des postes doit respecter les consignes suivantes :

1. Inventaire
2. Chiffrement (postes fixes et nomades)
3. Antivirus à jour et pare-feu
4. Déclaration sur le réseau
5. Système d'exploitation (OS)
6. Logiciels
7. Intégration aux outils de gestion centralisés
8. Moindres privilèges
9. Sauvegarde des données
10. Utilisation du VPN

1. Inventaire

La sécurité d'un parc informatique passe par sa connaissance.
Les postes de travail doivent être dotés d'un outil de gestion d'inventaire, permettant d'en recueillir :

- Les caractéristiques matérielles,
- L'utilisateur qui en a la jouissance,
- La présence de certains logiciels installés, ceci à des fins de gestion des licences,
- certains paramètres de sécurité (si le poste est chiffré, par exemple),
- La version du système d'exploitation et le niveau de correctif,
- La présence ou non d'une solution d'antivirus.

L'Université utilise un logiciel d'inventaire et d'assistance utilisateur nommé GLPI. Un agent d'inventaire doit être installé sur chaque poste de l'Université de Lille. Les postes appartenant aux co-tutelles doivent exécuter au moins celui de la tutelle propriétaire. Si les postes sont gérés par les équipes de la DGDNum, ils exécuteront aussi celui de l'université.
Dans tous les cas, dès lors que le poste bénéficie d'un service de l'Université de Lille (utilisation de logiciel mutualisé par exemple), il est nécessaire qu'il soit inventorié dans le GLPI de l'établissement.

2. Chiffrement (postes fixes et nomades)

Quel que soit le système d'exploitation, afin d'éviter toute fuite d'information en cas de vol ou de perte de la machine, l'ensemble des disques durs (internes et externes) d'un ordinateur doit être chiffré. Cela vaut particulièrement pour les postes nomades (ordinateurs portables) mais également pour les postes fixes (tous usages : administratif, enseignement, recherche et process). Ces postes fixes devront être eux aussi chiffrés dans un délai de 2 ans à compter de la date d'application de cette note.

Les clés permettant le déchiffrement doivent être collectées et stockées dans un système sécurisé et centralisé.

3. Antivirus à jour et pare-feu

La recrudescence des infections virales sur les postes de travail menace non seulement les données qui y sont stockées (destruction, demandes de rançon, divulgation) mais aussi celles qui sont hébergées sur les espaces partagés.
La présence d'un logiciel de protection à jour sur chaque poste de travail est indispensable, *quel que soit son système d'exploitation*. En effet, un poste peut transmettre un logiciel malveillant (sous forme de message électronique par exemple) même s'il n'est pas lui-même infecté. L'Université de Lille a choisi d'utiliser une solution professionnelle multi-plateforme centralisée et performante parmi les solutions sélectionnées dans le marché national.
La fonction de pare-feu qui permet de se prémunir contre les intrusions en provenance des réseaux non fiables doit être activée.

4. Déclaration sur le réseau

Les équipements personnels (ordinateurs portables, tablettes, téléphones mobiles) ne sont pas maîtrisés par les équipes informatiques de l'Université. Leur contrôle est techniquement impossible et leur niveau de sécurité est donc tributaire des choix de leur utilisateur. Seule la connexion de terminaux maîtrisés par l'Université doit donc être autorisée sur ses réseaux filaires.
Cet accès est donc soumis à une déclaration des terminaux qui doit être effectuée par les gestionnaires de parc dans le référentiel technique. Une machine non présente dans ce référentiel verra son accès limité au seul réseau sans fil (WIFI).

5. Système d'exploitation (OS)

Quel que soit le système d'exploitation choisi, toutes les machines doivent remplir les obligations suivantes :

- Le paramétrage matériel de la machine (BIOS ou équivalent) doit être protégé par mot de passe.
- La version du système d'exploitation doit être maintenue à jour par son éditeur tout au long de son utilisation.
- Les mises à jour de sécurité doivent être systématiquement installées sur les postes.
- Si un système d'exploitation n'est plus maintenu par son éditeur, il est alors nécessaire de migrer la machine vers une version plus récente ou de la déconnecter du réseau.
- Les machines ne pouvant pas être mises à jour parce qu'elles contrôlent un équipement scientifique devront être déconnectées du réseau ou placées dans un VLAN à part.

6. Logiciels

Au même titre que les systèmes d'exploitation, les logiciels utilisés sur les postes de travail nécessitent d'être mis à jour régulièrement. Les versions de logiciels qui ne sont plus maintenues par l'éditeur doivent être remplacées par des versions plus récentes ou supprimées des postes de travail concernés.

7. Intégration aux outils de gestion centralisés

Les outils de gestion centralisée permettent une homogénéisation des politiques de sécurité des établissements. Les postes des composantes de l'Université de Lille doivent être rattachés au système de gestion centralisé en place :

- Ceux exécutant le système d'exploitation Windows : Active Directory
- Ceux exécutant le système d'exploitation macOS : JAMF Pro

Le rattachement à un système de gestion centralisé permet notamment la diffusion au poste de travail des mises à jour de sécurité logicielles.
Les postes des laboratoires propriétés d'autres tutelles (CNRS, INRIA, INSERM, Institut Pasteur de Lille, etc.) doivent être rattachés aux outils de gestion centralisée de ces structures ou à minima à un système de gestion assurant leurs mises à jour.

8. Moindres privilèges

Aucun utilisateur du SI, quelles que soient sa position hiérarchique et ses attributions, ne doit disposer de privilèges d'administration sur son poste de travail. Cette mesure, apparemment contraignante, vise à limiter les conséquences de l'exécution malencontreuse d'un code malveillant (virus) et convient parfaitement pour la plupart des usages courants.

Les comptes d'administration sont réservés aux techniciens qui assurent la maintenance de la machine.

Si une délégation de privilèges sur un poste de travail est réellement nécessaire pour répondre à un besoin ponctuel de l'utilisateur, celle-ci doit être tracée, limitée dans le temps et retirée à échéance.

Pour des besoins exceptionnels, un utilisateur peut faire une demande dérogatoire de co-administration de sa machine de travail. La charte établie qui sera consignée engagera l'utilisateur au respect de règles qui sont rappelées dans cette même charte.

9. Sauvegarde des données

Tout usager de l'Université de Lille bénéficie :
- D'un dossier personnel.
- D'espaces de travail de groupes (création à la demande).
- D'un espace de stockage en mode cloud (NextCloud).

Ces espaces de stockage mutualisés sont sauvegardés automatiquement, leur usage est indispensable pour pallier la perte de données sur les postes utilisateur. Ils affranchissent donc les utilisateurs de la gestion de leurs sauvegardes.
D'autres espaces de stockage plus importants peuvent être mis en place avec les usagers après étude.

10. Utilisation du VPN :

L'accès au VPN de l'Université est réservé aux machines gérées par l'établissement. Son utilisation sur une machine personnelle n'est pas autorisée.

Outre ces points, il est souhaitable :

- De limiter les possibilités de connexion de périphériques externes USB sur les postes de travail et désactiver l'exécution automatique en cas d'insertion d'un périphérique de ce type.
- D'activer le verrouillage automatique de la session utilisateur après 10 minutes d'absence, indépendamment de cela, le verrouillage manuel de chaque poste de travail est souhaitable en cas d'inutilisation s'il est laissé sans surveillance.
- En cas de déplacement à l'étranger, chacun est invité à prendre en compte les suggestions qui se trouvent dans le guide *Bonnes pratiques à l'usage des professionnels en déplacement* publié par l'ANSSI (https://cyber.gouv.fr/publications/bonnes-pratiques-lusage-des-professionnels-en-deplacement).

Vos correspondants informatiques de proximité sont à votre disposition pour vous accompagner dans la mise en œuvre de ces mesures.

La DGDNum est responsable de la sécurité du système d'information de l'établissement. À ce titre, la DGDNum, en coordination avec le Fonctionnaire de Sécurité de Défense (FSD), pourra déconnecter des machines ne respectant pas les mesures techniques citées dans ce document si elle estime qu'elles font peser un risque sur le patrimoine informationnel de l'établissement.

La Directrice Générale des Services

Anne-Valérie CHIRIS FABRE

Le Président

Régis BORDET