Points particuliers à l'ESE qui doivent être améliorés après la lecture de la PSSI UPS.

Premiers écarts à la PSSI

1/ *Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local d'une entité. Pour les équipements non-maîtrisés (postes prévus par les invités, visiteurs, etc.), un réseau spécifique (invité ou collaborateurs) sera prévu.*
Dans le cas de l'ESE, ce réseau est 172.23.32.0
De plus, dans ce sous-réseau, l'utilisateur, pour aller sur Internet, doit passer par un proxy : cache.universite-paris-saclay.fr avec le port 8080
Par contre, les visiteurs ne pouvaient pas imprimer parce qu'il n'y a pas d'imprimantes sur ce réseau. J'ai demandé un pont d'impression entre le réseau 172.23.32.0 et 172.24.28.0 qui est opérationnel et doit être testé. Ce pont ne paraît pas encore opérationnel. Test en cours.

2/ *D'une manière générale le déploiement de réseau sans fil, par un ou des usagers, à l'intérieur de l'unité est interdit.*
Il me semble qu'il y a quelques Wifi autres que eduroam et eduspot, notamment chez Marc Girondot et Yvan Zivanovic.

3/ *Il faut tenir un tableau de bord SSI. Seules les interventions majeures (ex : le changement d'un système d'exploitation (OS), d'une version majeure à une autre, le rajout d'OS en boot multiple ou en émulation avec une autre adresse IP) sur les systèmes sont consignées dans un tableau de bord SSI. Sur les serveurs, en plus, le changement de versions majeures des composants essentiels en fonctions des services fournis (ex : version majeure de Samba sur serveur de fichiers, version 2.2 à 2.4 d'Apache sur serveur web majeur, etc.) seront indiquées dans le tableau de bord SSI.*
Pas de tableau de bord SSI actuellement.

4/ *La période de validité des accès et leur étendue (email, wifi, site intranet labo) en fonction du type de poste (membre permanent du laboratoire, stagiaire, visiteur, …) est établie selon des règles de base par défaut et les particularités aménagées selon les indications des responsables d'équipe et de la direction (modification durée, accès à des services spécifiques selon besoin, par exemple machines calcul, accès réseau par VPN, etc.).*
Dans le cas de l'ESE, le compte sous Adonis donne accès au SI. Il est donc important de bien maîtriser la durée du compte de messagerie.
Pour l'instant un tableau Excel tenu par Nicolas Moulonguet essaie de répertorier les durées des comptes Adonis.
De plus un autre tableau Excel est tenu par Nicolas Moulonguet pour lister les utilisateurs de VPN. Si un utilisateur de VPN quitte l'ESE en gardant sont e-mail sur l'Université, les accès VPN lui sont enlevés.

5/ *Pour les identifiants d'administration des serveurs ou postes critiques, des identifiants d'administration et les clés de chiffrage des disques/dossiers seront déposés sous séquestre en enveloppe scellée dans le coffre-fort ou armoire blindée de la direction.*
Un coffre-fort existe. Le mot de passe de la session *moulonguetn* a été donné au DU Nathalie Frascaria et aux deux directeurs adjoints Bruno Colas et Stéphane Bazot.

6/ *Pour les outils d'administration (interfaces), les noms des administrateurs et des interfaces auxquelles ils ont accès sont spécifiés dans un tableau de bord SSI. Ils sont validés par la direction. L'administration se fait par protocole sécurisé (à défaut d'un réseau spécifique pour les salles machines).*
L'outil IPM est utilisé par Nicolas Moulonguet pour gérer le réseau filaire de l'ESE (réseaux, adresses IP, adresses MAC, …). Il a accès aux réseaux de EGCE et GQE, de même que les utilisateurs d'IPM des

ces deux laboratoires ont accès aux réseaux de l'ESE. Les deux intervenants au 11/04/24 sont Jean-Bernard Emond et Olivier Langella.

7/ *Lorsqu'une ressource informatique est amenée à quitter définitivement l'entité, les données (chiffrées ou non) présentes sur les disques durs ou la mémoire intégrée doivent être effacées de manière sécurisée. L'effacement des données et la sécurisation de l'espace libre doit s'appuyer sur des produits qualifiés (recommandés par les tutelles et approuvées par l'unité).*
Les disques durs obsolètes sont actuellement gardés dans le bureau de Nicolas Moulonguet. Ils doivent être effacés avant d'être sortis du laboratoire. Ils sont actuellement tous formatés en NTFS, mais sont conservés en cas de réutilisation.

8/ *Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif mis en œuvre par le service informatique de l'unité (commun ou autonome selon les cas).*
A l'ESE, cela n'est pas le cas actuellement. Les mises à jour des systèmes ne sont pas gérées de manière centralisée, mais poste par poste. Les mises à jour de l'Antivirus Windows Defender, un Antivirus généralisé à l'ESE, dépendent des mises à jour des systèmes Windows.
Trend Micro est proposé par l'Université Paris Saclay et Nicolas Moulonguet est en contact avec Daniel Morbin.

9/ *Pour les cas des postes avec un OS obsolète (plus de mises à jour existantes), mais pour lesquelles il n'est pas possible de les migrer car ils gèrent un équipement matériel spécifique ou des programmes de commande bien particuliers, une isolation réseau (filtrage strict) doit être envisagée (à définir en collaboration avec la DSI), de même lorsqu'un antivirus actuel ne peut plus opérer sur un tel poste. La limitation d'une possible contamination par échanges par clé USB doit être prévue.*
Après vérification pour Gwendal Latouche et Peter Streb, il faut envoyer un message aux chefs d'équipe pour s'assurer que les systèmes avec d'anciens systèmes d'exploitation ne sont pas connectés au réseau.

10/ *Pour accéder au réseau de l'unité, les utilisateurs extérieurs doivent obligatoirement utiliser les portails et méthodes mises en place en accord avec la DSI (les accès VPN gérés par la DSI).*
Le VPN GlobalProtect est utilisé.

Sécurité du poste de travail

11/ *Les boîtiers d'unités centrales sont de préférence verrouillés par cadenas. Les plus petites doivent être attachées par câble antivol. Les postes portables sont munis systématiquement d'un câble antivol et les utilisateurs sensibilisés à l'utiliser.*
Beaucoup de postes à l'ESE ne sont pas cadenassés.

12/ *Les utilisateurs ne doivent pas travailler avec des comptes « administrateur » et le principe du « moindre privilège » s'appliquera. L'accès au compte « administrateur local » se limite aux personnes du service informatique en charge et en cas de besoin pour les postes utilisées à la recherche aux personnes désignées dans les équipes et notées dans un tableau SSI et tenu à jour.*
Attention ! Gros changement en vue. Je mets actuellement tous les postes Windows en Administrateur. Question subsidiaire : Qu'en est-il avec Mac et Linux ?
Le passage en compte Utilisateur a été commencé pour : Telesto, Cap Vert, Luxembourg, Réunion, Andorre, Bucarest, Beyrouth, encelade, soleil, corse.

13/ *Une solution de sauvegarde chiffrée des données de travail sera proposée aux utilisateurs.*
Cirrus est-il chiffré ?

14/ *La mise en place de services serveur est interdite (sauf accord exceptionnel des équipes informatique et de la direction) ex : (s)ftp, web, services DHCP, DNS, etc.*
Les machines max6 et max7 de la salle serveurs ont été arrêtées et déconnectées du réseau.

15/ *Les appareils réseaux comme copieurs multifonction, imprimantes, onduleurs, interfaces de gestion doivent avoir le mot de passe usine changé dès leur mise en place.*
Le changement est fait pour HP M552 (admin), HP M553 (admin), Lexmark MX410de, Lexmark MX510dn, HP Laserjet 4200, Ricoh MPC2004ex, Ricoh MPC2004exse, Ricoh MPC3003 (admin ou moulonguetn pour les 3 Ricoh), Canon_C5760i (Administrator).
Le mot de passe est le mot de passe de la session moulonguetn qui a été donné aux directeurs.

16/ *Il est convenu que la prise à distance d'écran (active ou passive) des postes de travail (fixes ou mobiles) n'est pas autorisée dans l'unité.*
L'ordinateur de la serre est parfois utilisé à distance par le constructeur avec Teamviewer.
De plus cette phrase demande une explication. Avec VPN+Connexion Accès à distance, on peut très bien prendre le contrôle de son ordinateur de bureau allumé.