Points clefs de la sécurité informatique.

Point 1

La perte de données et la sauvegarde.

Pourquoi sauvegarder.

Documents perdu (par exemple erreur de manipulation), documents inexactes ou infectés par un virus, programmes défectueux, panne matériel etc..

La sauvegarde est le point clef de la garantie de fonctionnement d'un système d'information.

Elle sert aussi souvent d'archivage informatique mais ce n'est pas son but premier.

Les sauvegardes sont en général automatisées et des messages d'alertes sont envoyés aux responsables en cas de disfonctionnement.

Mais si vous laissez une alerte (même bégnine) non traitées vous risquez de ne pas vous rendre compte le jour ou la sauvegarde n'aura pas fonctionnée. Par exemple un message vous alerte tous les jours car un ou plusieurs fichiers étaient ouverts donc n'ont pas pu être sauvegardés. Après analyse vous avez vu que ces fichiers n'étaient pas importants et vous les laissez en l'état. Mais si un jour un fichier fondamental à l'entreprise n'est pas sauvegardé vous ne le verrez pas.
Souvent c'est un utilisateur qui laisse régulièrement sur un serveur de fichier un fichier Word ou Excel ouvert ou laisse son ordinateur allumé en partant le soir.

Voir aussi le cas des bases de données.
Maintenant parlons des photos de votre téléphone portable.

Point 2

Le piratage informatique et les idées fausses.

Si vous regardez la série télé NCIS, Timothy McGee vous donne une impression très fausse de ce qui peut être fait par l'extérieur, que ce soit pour remonter au propriétaire d'un site qui veut se cacher via un VPN, ou simplement le piratage d'information d'une entreprise par l'extérieure.
A la télé, en quelques instants, un prétendu spécialiste informatique (un greec) rentre dans les bases de données des grandes agences de sécurité internationales, puis récupère les comptes bancaires du suspect et même récupère les positionnement téléphonique etc..

Mais ce n'est que du cinéma. Ce n'est pas impossible à faire en théorie mais cela demande un travail énorme, beaucoup, beaucoup de temps et d'efforts et en plus il faut trouver ou créer des complicités internes dans les centres informatiques cibles que ces complicités soient volontaires ou involontaires.

Pirater de l'extérieure un site informatique demande une complicité interne. Cette complicité est parfois voulue mais le plus souvent elle a été installée au part-avant via un virus ou par quelqu'un de malveillant qui a installé d'avance un logiciel adéquat.

Depuis plus de 10 ans il est quasiment impossible de pirater de l'extérieur, sans installer une complicité interne dans l'entreprise cible.

Point 3

La sécurité des informations internes à l'entreprise.

Une entreprise doit protéger ses informations que ce soit par rapport à l'extérieur mais aussi et surtout à l'intérieur de l'entreprise.

Fichiers du personnel, des offres commerciales, etc. ... La plupart des documents d'une entreprise sont confidentiels et cela, service par service.

Quand les entreprises appartiennent à un groupe toute une hiérarchie de sécurité de l'information se met en place. Car souvent l'informatique est celle de la maison mère du groupe.

Voir le fonctionnement de : « Active Directory «. Une partie de la sécurité interne à l'entreprise est basée sur une bonne compréhension du fonctionnement de l'Active Directory.

Point 4

Sécurité de l'information de l'entreprise vis-à-vis de l'extérieur.

Elle est de plus en plus difficile à mettre en œuvre à cause du télé travail.

Pour pallier aux risques venant de l'extérieur (et aussi de l'interne) beaucoup d'entreprises utilisent des solutions de type « Citrix ».
Citrix est un logiciel qui replace le fonctionnement de votre ordinateur par un poste de travail virtuel qui tourne sur un serveur de l'entreprise.
De votre propre ordinateur seul, le clavier, la souris et l'écran est utilisé.
Une fois « loggé » sous Citrix vous retrouvez votre poste de travail habituel quel que soit l'ordinateur sur lequel vous démarrez.
Par exemple vous êtres comptables et vous vous déplacez sur un ordinateur du service de maintenance de l'usine, dès que vous êtes en Citrix, vous retrouvez vos programmes de comptabilité habituel.

Avec un bon VPN c'est l'outil parfait pour le télétravail.

Mais le risque n'est pas totalement supprimé il est seulement plus difficile de pirater.

Par exemple avec un logiciel de piratage de type « bureau à distance » ou via une attaque HID, il est possible d'enregistrer les touches claviers dans un fichier log. Et la lecture de ce keyboard log peut (ou pas) vous donner la possibilité de vous connecter en utilisant des identifiants volés.

Point 5

Démonstration : Comment pirater un réseau informatique de l'extérieur. Ou comment faire une attaque HID.

Demander l'accord du professeur avant de développer le sujet.

Point 6

Comment préserver un réseau informatique d'une attaque de l'extérieur.

Protections des Postes de travail dans une entreprise.

Point 6-1

Avoir sur tous les serveurs et tous les poste de travail les anti-virus à jour et opérationnel.

Point 6-2

Vérifier que sur tous les postes de travails de l'entreprise on demande bien un mot de passe à la mise sous tension.
C'est un point de détail mais qui a son importance car on se préserve d'une malveillance faite par un amateur par exemple un employé de ménage. (voir le type de mot de passe au point 6.3)

Point 6-3

Mettre en place l'écran de vielle sur votre ordinateur avec une durée d'environ de 10 minutes avec un mot de passe à la reprise. Utiliser un mot de passe simple car rapidement votre mot de passe sera connu de vos collègues de travail. Ne pas utiliser votre mot de passe (complexe) utilisé pour vous connecter aux serveurs de l'entreprise.

Point 6-4

Si utilisation d'Active Directory vérifier le respect des règles d'installations. Même chose pour le bureau Citrix.

Ces deux points protègent surtout les informations en interne dans l'entreprise.

Point 6-5

Pour tous les outils manageables tels les routeurs, les switches, les camera IP ou les imprimantes ne pas laisser le mot de passe d'installation du type : ----→ identifiant : Admin ; password : Admin. (ou 1234)

Point 6-6

Utiliser un logiciel de sécurité et d'inventaire du type Lansweeper ou équivalent pour les petites et moyennes installations et du type Solar Win pour les très grosses configurations. Ces logiciels sauvegardent les configurations matériels et logiciels ce qui permet de comparer par différence les logiciels nouvellement installés.

Car au-delà d'un petit réseau avec un seul serveur et quelques postes de travail il est presque impossible de savoir ce qui est installé sur les postes de travail.

Point 6-7

Être à l'écoute des utilisateurs surtout s'ils vous informent d'un ralentissement ou que le fonctionnement de leur PC a changé.
Dans ce cas aller sur le poste de travail, vérifier l'antivirus puis vérifier ce qui a été installé récemment sur le poste.

Faire une démo avec les dates d'installation dans : user/Appdata/Local/ etc..

Point 7 et denier point.

Souvent il vaut mieux se taire.

Exception faite pour des problèmes de sauvegarde qui ne fonctionne pas ou d'anti-virus désactivé accidentellement il ne faut pas faire de remarque sur la sécurité ou la faire avec beaucoup, vraiment beaucoup, de précautions.

Si vous découvrez une faille de sécurité dans l'entreprise ou vous travaillez, et si vous n'êtes pas en charge de la sécurité, il vaut mieux ne rien dire ou le signaler avec beaucoup de précautions car la personne en charge de la sécurité va sans doute très mal le prendre et c'est encore plus vrai du responsable informatique.

Et si vous êtes un prestataire extérieur vos remarques risquent de vous faire perdre votre client car un client n'accepte pas qu'un prestataire

porte un jugement de sécurité sur son informatique, sauf, si spécifiquement, il lui demande un audit de sécurité.

Faire un commentaire sur la sécurité informatique dans un centre informatique c’est comme faire un commentaire sur la propreté dans un restaurant.