***TIL support et maintenance & le BTS SIO***

*GLPI*

***Objectif****: Gérer les évènements, les problèmes, les incidents, les demandes, l’entretient, les accès*

***Les demandes****: installation, mise à jour, modification*

***Les incidents****: Résolution rapide, occasionnel*

***Les problèmes****: complication, récurrence*

***Les incidents****: importance, urgence, impact, localisation*

***Les tickets****: Numéro ticket, Date/délais, Urgence & importance, classifications / Type, identités, commentaires*

***Les processus****:*

*Réception d’appel (ouverture du ticket)*

*Classement (changement, incident)*

*Routage (demande, support NiveauX)*

GTI

GTR²

*Analyse => diagnostique + KB*

*Résolution Nx Escalade Nx+1*

*Résolution => Clôture => KB*

***Diagnostique****: Identifier, délimiter le périmètre, identifier la cause, lister les solutions possibles, corriger, tester, laisser des traces (KB)*

***Des méthodes*** *: TOP DOWN, BOTTOM UP, DIVIDE & CONQUER, COMPARE-CONFIGURATION, SWAP COMPONENTS*

***La qualité de service*** *: SLA Service Level Agreement :*

*Disponibilité et les temps de réponses, Résolution des problèmes/incidents, Mise à jour, Amélioration (Mineur), rapports (Knowledge base + Key performance.*

***RGPD règlement général sur la protection des données***

*Nouveau contexte => Internet cloud Big data IA,*

*Nouveau besoin => Donnée personnelle,*

*Cadre juridique => Droit à l’oubli Droit au contrôle,*

*Définir les rôles => CNIL sous-traitant DPO (délégué de protection)*

*Harmoniser & simplifier => Norme Européenne.*

***Une donnée personnelle*** *est toute information se rapportant à une personne physique identifiée ou identifiable*

*Nom prénom Adresse Téléphone*

*RIB, Ameli, N°Sécu*

*Email, contacts, Agenda*

*Règlement*

*Vidéo*

*Droit au contrôle, à l’information, à l’oubli, de rectification, à la portabilité, réparation.*

*Consentement explicite sur l’utilisation des données / Traitement des données conformes aux normes / Sécurisation des traitements / Outils et techniques adaptés au risque / Traçabilité et preuves*

*Les 6 bons réflexes de la CNIL*

*Ne collectez que les données vraiment nécessaires / Soyez transparent / Pensez aux droits des personnes / Gardez la maitrise de vos données / Identifiez les risques / Sécurisez vos données.*

***Traitant et sous-traitant***

*Article 32 – sécurité du traitement*

*Article 38 – sous-traitant*

*Devoir de conseil signaler*

*Règlement sanctions*

*EIVP Etude d’impact sur la vie privée*

*Authentifier et contrôler / Sécuriser les postes / Sécuriser les réseau / Sécuriser l’administration / Maintenir et superviser / lien avec le DPO*

***La sécurisation des données & respect des normes***

*Authentification nominative / réseau dédié / Matériels adapté / outils adapté / traçabilité*

*Analyser l’existant / Authentifier et contrôler / Sécuriser les postes / Sécuriser le réseau / Sécuriser l’administration / maintenir et superviser / Chiffrement symétrique / hachage/ Chiffrement asymétrique / autorité de certification / sécuriser le réseau / Sécuriser l’administration / Maintenir et superviser.*

***Résumé :*** *Comprendre le risque numérique / se protéger / sensibiliser les collaborateurs / choisir des solutions et des experts de confiance / Que faire en cas d’incident.*

***DICP***

*Pour évaluer si un bien est correctement sécurisé, il faut auditer de Disponibilité, Intégrité, Confidentialité et Preuve ou traçabilité. L’évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.*

***Disponibilité****: propriété d’accessibilité au moment voulu des biens par des personnes autorisées*

***Intégrité****: propriété d’exactitude et de complétude des biens et informations*

***Confidentialité****: Propriété des biens de n’être accessibles qu’aux personnes autorisées*

*Exemple d’évaluation Serveur Web*

*Disponibilité Très fort le site web doit être disponible sans quoi il ne ferait pas connaitre ses services au public*

*Intégrité l’entreprise ne souhaite pas qu’un concurrent modifie frauduleusement le contenu pour y insérer des informations erronées.*

*Confidentialité contenue dans le site web sont publiques par nature.*

*Preuve aucune interaction avec l’utilisateur, il fournit uniquement des informations fixes.*

*Antivirus DIC*

*Cryptographie ICP*

*Pare Feu DC*

*Contrôle d’accès logique ICP*

*Sécurité Physique des équipements et locaux DIC*

*Capacité d’audit, clauses contractuelles avec les partenaires, formation et sensibilisation DICP*

***Sureté***

*Protection contre des dysfonctionnements et incidents involontaires ex : saturation d’un point d’accès, panne d’un disque, erreur d’exécution, etc…*

*Quantifiable statistiquement ex : durée de vie moyenne d’un disque est de X milliers d’heures*

***Parade****: sauvegarde, dimensionnement, redondance des équipements…*

***Sécurité***

*Protection contre des actions malveillantes volontaires.*

*Ex : blocage d’un service, modification d’informations, vol d’information*

*Non qualifiable statistiquement, mais il est possible d’évaluer en amont le niveau du risque et les impacts*

***Parades****: contrôle d’accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

***Différences entre sureté et sécurité :*** *Ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises*

*Ensemble de mécanismes destinés à protéger l’information des utilisateurs ou processus n’ayant pas l’autorisation de la manipuler et d’assurer les accès autorises.*

***Vulnérabilité*** *faiblesse au niveau d’un bien (conception, de la réalisation, de l’installation, de la configuration, ou de l’utilisation du bien.*

***Diffèrent type de menace***

*Cause potentielle d’un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.*

*Stagiaire malintentionné, Perte de service, code malveillant et personnes malveillantes*

***SI Système*** *d’information doit faciliter la mission d’organisation*

*Actifs primordiaux et actifs supports un ensemble de bien la sécurité SI consiste donc à assurer la sécurité de l’ensemble des biens*

***La sécurité a pour mission*** *de réduire les risques pesant sur SI pour limiter leurs impacts.*

***Sécurité SI****: impacts financiers, impacts sur l’image et la réputation, impacts juridiques et réglementaires, impacts organisationnels.*

***Impacts sur la vie privée :***

*Sur l’image, le caractère, vie privée*

*Sur usurpation d’identité*

*Sur la perte définitive de donnés*

*Sur impact financier*

***Impacts sur la cybercriminalité sur les infra critiques :***

*Ensemble d’organisations critique pour la nation que des mesures de sécurité particulières doivent s’appliquer.*

*OVL liste inconnue du public*

***Cyber délinquance :*** *attiré par l’appât du gain, hacktiviste, motivation politique, religion, les concurrents, les fonctionnaires de l’état, mercenaires agissent pour le compte de commanditaires.*

*Gains financiers, utilisation de ressources, chantage, espionnage*

*Quelques menaces :*

***Hameçonnage et***

*Réception de mail utilisant le logo et les couleurs de l’entreprise / Demande pour effectuer une opération comme la mise à jour des données perso et confirmation de mot de passe/Connexion à un faux site identique contrôlé par l’attaquant / récupération par l’attaquant des identifiants et mdp saisie par le client sur le faux site.*

***Ingénierie sociale*** *constitue une attaque ciblée qui vise à abuser la naïveté des employés de l’entreprise.*

*Pour dérober directement des informations confidentielles ou introduire des logiciels malveillants.*

*Par téléphone, par réseaux sociaux, par e-mail.*

*Exemple : phishing un lien pointe en fait vers un site frauduleux, et non pas un serveur légitime de l’entreprise.*

*Attaque avancée 1. Envoi de courriel contenant une PJ (Attaquant vers la cible) 2. Annonce de la compromission (victime vers attaquant) 3. Prise de contrôle de l’attaquant.*

*4. connexion a la tête de pont(victime) 5. Attaque et prise de contrôle du serveur de l’entreprise 6. Exfiltration de mots de passe 7. Prise de contrôle et transformation en ordinateur de rebonds. 8.Prise de contrôle Machines rebonds 9. Demande de contenu des répertoires cibles du serveur de fichiers 10. Renvoi du contenu des répertoires cibles 11. Exfiltration du contenu 12. Effacement des traces de l’exfiltration.*

***Fraude interne***

*Sujet tabou pour les entreprises*

*Fraudeur occasionnel, récurrent, personne ne se fait embaucher pour effectuer une fraude, fraude en groupe*

* *Faiblesse des procédures de contrôle interne et de surveillance des opérations, gestion permissive des habilitations informatiques, absence de séparation des taches et de rotation*
* *Typologie des fraudes : Le détournement des avoirs de la clientèle et de l’entreprise, la création de fausses opérations, la personne qui fausse ses objectifs pour augmenter sa rémunération.*

***Violation d’accès non autorisé***

*Des mots de passe simples ou faibles sans caractères spéciaux ou sans les chiffres permettent à des attaquants de mener des actions utiliser des scripts qui permettent de tester les logins avec tous les mdp couramment utilisés (issue d’un dictionnaire) ou utiliser des outils pour tenter de casser les mdps.*

*Les intrusions informatiques constituent des attaques cibles qui exploitent 1 ou 2 vulnérabilités techniques pour dérober des informations confidentielles (md, carte bleu…) ou prendre contrôle des serveurs ou poste de travail depuis le réseau internet sur les ressources exposées : serveur de messagerie, services d’accès à distance, etc…*

*Depuis le réseau interne sur active directory ou applications sensibles.*

***Virus informatique***

*Constituent des attaques massives ciblés sur un secteur d’activité (télécom, banque, Energie…) de plus en plus sophistiqués et furtifs.*

*Vecteurs d’infections : Message avec PJ, support amovible, site Web malveillant ou piraté, partages réseaux ouverts systèmes vulnérables systèmes*

*Avec comme conséquences : installation de cheval de Troie, récupération de données, surveillance à distance, destruction des données, chiffrement des données.*

***Déni de service distribué***

*Constituent une attaque ciblée qui consiste à saturer un site web de requetés pour le mettre hors service à l’aide de botnets réseaux d’ordinateurs infectés et contrôlés par les attaquants.*

*Milliers ou millions d’ordinateurs infectés, prêts à attaquer la cible sur ordre de l’attaquant. Les propriétaires ne savent pas que leur pc participe à un botnet.*