Certification TOSA - Sujets de veilles

I. Monde de la cybersécurité

A. Acteurs - Identification des rôles

1. Attaquants - profils - champs d'actions[1]
2. Acteurs de la cybersécurité[2] - institutions publiques et personnel d'entreprise de référence

B. Cibles et impacts d'une attaque - Identification

1. Zones de risques ciblées, catégorisation faille, indices d'une attaque (côté client, côté serveur, faille logicielle, faille matérielle[3], exposition de données, injection de scripts…)
2. En fonction du but recherché (récupération, divulgation de données, usurpation d'identité, extorsion de fonds,...)
3. Impacts d'une attaque sur les activités d'une entreprise (impacts financiers, paralysie de l'activité, préjudice commercial, atteinte à la réputation…)

C. Réaction suite à une attaque - Procédures

1. Soupçonnée: Collecte d'indices rapport et transmission à qui de droit et procédure de signalement, mesures de protection
2. Avérée: Collecte d'informations, rapport et transmission à qui de droit et procédure de signalement, mesures en vue de contenir l'attaque

D. Identité et authentification numériques - Mesures préventives

1. Caractères d'un mot de passe fort: Ce qu'il faut exclure par rapport à ce qu'il faut privilégier
2. Outils et modes d'identification sécurisés

---

[1] Veilles de François, Matthias, Gauthier, Guy
[2] Veille de Benjamin
[3] Veille de Guillaume

II. Sécurité au bureau

A. Sécurisation du poste de travail - Accès restreint

1. Sûreté et restriction d'accès à tout dispositif véhiculant des données en fonction du secteur d'activité (bancaire, public…)

B. OSINT

1. Facteurs humains constituant des postes (vecteurs) d'attaques (publicité des données personnelles sur les réseaux sociaux et leviers de manipulation…)
2. Modes de réaction et d'alarme à toute alerte

C. Périphériques amovibles - Transport de données

1. Sécurisation des données qui transitent entre différents postes distants (clefs USB, dispositifs de stockage externes, téléphone portable, tablette…)

D. Versions de logiciel et mises à jour

1. Sources de confiance (éditeur de programme, dépôt officiel, sécurité des sites web[4]…)
2. Mise à jour des logiciels et systèmes d'exploitation (intérêt, régularité, mise en place…)

[4] Veille de AnthonyS

III. Sécurité en déplacement

A. Sécurité physique des terminaux - Dispositifs exposés

1. Terminaux susceptibles d'être exposés en déplacement, risques physiques ou non (PC professionnel dans un environnement non professionnel, accès au réseau mobile dans les transports, vol…)

B. Smartphones et sécurité - Bonnes pratiques[5]

1. Sécurisation des données et services - Master Data Management (MDM)

C. Réseaux sans fils - Identification des risques liés

1. Identifier les risques et mesures de sécurisation des connexion non filaire à des réseaux externes (wifi, bluetooth, vpn[6]…)

D. Surexposition des données

1. Sources potentielles de fuite de données (limiter la diffusion et partage de données sensibles ou non sous toutes ses formes…)

[5] Veille de Corinne
[6] Veille de Jason

IV. Sécurité à la maison

A. Hameçonnage - Identification et procédure de traitement

1. Éléments de vérification à l'ouverture d'un mail
2. Détection d'une tentative d'hameçonnage
3. Réaction à une tentative d'hameçonnage

B. Cloud et sauvegarde de fichiers - Fonctionnement

1. Outils de gestion électronique de documents (GED) (sauvegarde de données et continuité de l'activité grâce à elle…)
2. Services Cloud (sécurité des infrastructures, attaque interne, externe, sabotage…)

C. Fichiers externes - Risques liés à leur manipulation

1. Énumération des risques liés au téléchargement et à l'utilisation de fichiers externes (extension de fichier, validation MIME…)
2. Degré et risque potentiel d'un fichier dangereux (réseaux de partage, fichier joint à un mail…)

D. Vie privée et protection personnelle - Scission entre vie privée et vie professionnelle

1. Séparer les usages numériques personnels des usages numériques professionnels (ne pas utiliser les mêmes mots de passe, messagerie pro et perso différente…)
2. Protéger ses informations personnelles et sa vie privée dans le cadre de son travail