BREVET DE TECHNICIEN SUPÉRIEUR

SERVICES INFORMATIQUES AUX ORGANISATIONS

BLOC DE COMPÉTENCES N°3

–

Cybersécurité des services informatiques

Évaluation semestre 1

Décembre 2024

———

P. GAHIDE

DOSSIER A	Participation à l'atelier d'analyse des risques sur l'application Web	35 points
DOSSIER B	Analyse d'une attaque et audit	20 points
	TOTAL	55 points

Matériel autorisé : aucun matériel ni document n'est autorisé.

Le sujet est constitué de deux parties qui peuvent être traitées de façon indépendante. Les documents sont fournis en fin de sujet. Toutes les réponses sont à donner **sur votre copie**, dont vous **numéroterez** les pages comme sur ce document.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Présentation du contexte

La grotte de Lascaux, située à Montignac en Dordogne, est une grotte ornée du paléolithique, découverte en 1940. Elle fait partie du patrimoine mondial de l'Unesco depuis 1979.

Le Ciap, appelé également Lascaux IV, offre au public une réplique de la grotte de Lascaux en permettant aux visiteurs d'utiliser les technologies d'aujourd'hui pour personnaliser leur visite avant, pendant et après.

Le conseil départemental de la Dordogne a été nommé maître d'ouvrage de Lascaux IV.

Cette réplique de la grotte comporte une partie musée où le visiteur est en interaction permanente avec ce qu'il côtoie, grâce à l'utilisation d'une tablette appelée compagnon de visite (CDV). Mille six cents CDV en dix langues sont mis à la disposition des visiteurs.

Le CDV est connecté à un maillage de dispositifs Wi-Fi et *Bluetooth* du bâtiment composé de cinquante bornes Wi-Fi et de deux cents balises *Bluetooth* qui permettent au CDV de se localiser, de communiquer et aussi de se synchroniser avec les serveurs multimédias du Ciap. Des centaines de tablettes sont prêtées chaque jour pour permettre à chaque visiteur d'avoir une expérience numérique unique et personnalisée.

L'organisation cliente

Le Ciap dispose de plusieurs systèmes d'information (SI) internes. Il peut y avoir cinq mille visiteurs par jour. Grâce à l'application tablette pour les CDV, le site internet, la plateforme d'échanges (MyLascaux), la solution mégadonnées (*big data*), il s'agit d'assurer un service très complet de gestion de la relation client avant, pendant et après la visite. Sur la partie après visite, plus d'un million de visiteurs peuvent se connecter.

L'entreprise prestataire de services

L'ESN Aquilasc, éditeur de logiciels de gestion sur mesure de type client lourd, *Web* ou mobile et spécialisée dans le secteur du tourisme, a été retenue pour la mise en place d'une partie du SI liée du Ciap.

Vous faites partie de l'équipe qui participe au développement et au déploiement des applications *Web* et mobile qui ont été définies par le cahier des charges. Vous participez notamment à l'atelier analyse de risques et à la sécurisation des données.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

Dossier A – Participation à l'atelier d'analyse des risques sur l'application Web

Mission A1 – Évaluation des risques à partir des récits utilisateurs

Dans un premier temps, vous participez à un atelier d'analyse de risque au sein de l'équipe de développement afin d'évaluer les risques sur les récits utilisateurs (scénarios d'utilisation) qui ont été recensés lors d'une première phase d'analyse.

Question A1.1 (2 pts)
Indiquez si le tableau contenant les acteurs à l'origine de malveillance est complet. **Justifiez votre réponse**.

Le tableau « Besoins de sécurité pour les récits utilisateurs » propose pour chaque récit une évaluation des besoins de disponibilité, d'intégrité et de confidentialité des données manipulées et la nécessité d'éléments de traçabilité faisant office de preuve. L'évaluation des récits utilisateurs n'a pas été finalisée.

Question A1.2 (4 pts)
Proposez une évaluation des récits utilisateurs 1 et 25 pour **chacun** des 4 critères DICP. **Aucune justification n'est demandée**.

Mission A2 – Gestion des événements redoutés

Le tableau « Impacts des événements redoutés » permet de définir l'impact et la gravité en terme de sécurité des événements liés à des actes de malveillance pour l'entreprise.

Question A2.1 (4 pts)
Proposez, pour les événements 1 et 3 fournis dans ce tableau, **les impacts** pour l'entreprise ainsi qu'une **estimation de leur gravité** respective (vous **justifierez** des estimations).

À l'aide des deux tableaux, l'équipe met en évidence un premier risque intitulé **R1** en associant l'exploitation **P3** à l'événement **E4** : ***R1 = P3 x E4 = 2 x 1***.

Question A2.2 (4 pts)
Recensez, selon le même modèle, les **cinq autres risques** intitulés R2 à R6 que l'on peut dégager de l'association de ces deux tableaux.

Question A2.3 (4 pts)
Sur la base des documents présentés, proposez une représentation graphique de **cartographie des risques**. **Placez** sur cette cartographie les risques référencés **R1 à R6**, en vous basant sur vos réponses précédentes, sans justifiez davantage.

Question A2.4 (4 pts)
En vous appuyant sur cette cartographie, expliquez la notion de **priorisation** dans la gestion des risques. **Expliquez** également en quoi la gestion de risques est un **processus itératif**.

Il a été décidé par la SSI de s'attaquer aux problèmes posés par l'événement 3 pour la prochaine itération de gestion de risques.

Question A2.5 (3 pts)
Proposez au moins trois contre-mesures pour minimiser **la probabilité** de l'événement 3.

Question A2.6 (2 pts)
Proposez au moins une contre-mesure pour minimiser **l'impact** de l'événement 3.

À la fin de l'itération, toutes ces contre-mesures ont été mises en place.

Question A2.7 (2 pts)
Expliquez comment la cartographie des risques est affectée.

On s'intéresse maintenant au récit utilisateur numéro 15.

Question A2.8 (4 pts)
Proposez un nouvel événement redouté (le numéro 5), depuis une attaque extérieure, en lien avec les besoins de sécurité du récit utilisateur numéro 15. Vous indiquerez le ou les **impact(s)** associé(s) et estimerez sa **gravité** (en **justifiant** de la gravité).

Christine Berton, la responsable de produit, vous demande d'ajouter un nouveau récit utilisateur : « En tant que visiteur, je veux être déconnecté du site lorsque je ferme mon navigateur ou à l'issue d'une période d'inactivité fixée ».

Question A2.9 (2 pts)
Expliquez à quel risque de cybersécurité (non en lien avec les précédents) vient répondre ce nouveau récit utilisateur.

Dossier B – Analyse d'une attaque et audit

Dans le cadre de votre stage, vous avez l'honneur d'intervenir dans le service informatique du *Palace-Hôtel Le Vallon*, un hôtel de luxe qui emploie environ 200 personnes. La DSI de l'hôtel est composée d'un petit groupe de techniciens logiciels et réseaux, placés sous la direction de M. Jean-Pierre Estampe. Aucun de ces techniciens n'a de réelles compétences en cybersécurité, et aucune réelle politique de sécurité n'est encore implémentée dans l'organisation, même si certaines mesures sont en place.

En mai 2025, l'hôtel est victime d'une cyberattaque, décrite dans le document 3.

Question B.1 (1 pt)
Donnez les noms anglophone et francisé de ce type d'attaque.

Question B.2 (1 pt)
Comment s'appelle la technique visant à cibler par email *personnalisé* un petit groupe de personnes comme les employés du service d'accueil et de réservation ?

Question B.3 (2 pts)
Pourquoi cette technique avait-elle ici raisonnablement plus de chances de réussite qu'un envoi massif à tous les salariés identifiés dans l'entreprise, qui aurait augmenté la « probabilité de clic » ?

Question B.3 (7 pts)
En vous basant sur vos connaissances et les documents 3 et 4, expliquez précisément les éléments d'ingénierie sociale utilisés par les attaquants, et donnez la chronologie de tout le processus d'attaque. Expliquez également comment celle-ci se déroule techniquement, une fois le malware activé.

Suite à cette attaque, il a été décidé d'auditer et de redéfinir la politique de sécurité de l'entreprise. Vous suivez l'équipe en charge de cette tâche. Après un audit préliminaire, un document listant sommairement les mesures existantes en matière de cybersécurité est rapidement rédigé (document 5).

Question B.4 (9 pts)
Sans attendre les résultats complets de l'audit, le DSI vous demande de lui rédiger au plus vite une note exprimant brièvement votre point de vue sur chaque problème et / ou amélioration potentielle que vous avez identifiés à partir de ce premier document.

Document 1 - Besoins de sécurité pour les récits utilisateurs de l'application gestion des billets et des visites sur le site Web (extraits)

	Intitulé du récit utilisateur	Disponibilité	Intégrité	Confidentialité	Preuve
1	En tant qu'acheteur, je veux acheter en ligne les billets pour plusieurs personnes afin de pouvoir participer à une visite.				
2	En tant qu'acheteur, je veux télécharger les billets d'une de mes réservations au format *PDF* afin de les transmettre aux personnes pour lesquelles j'ai réalisé la réservation.	**	**	*	-
5	En tant qu'acheteur, je veux consulter les caractéristiques des seniors pour lesquels j'ai acheté un billet sur un mois donné afin de réaliser une campagne publicitaire.	-	*	**	-
15	En tant que visiteur, je veux poster un commentaire afin de donner mon avis sur la qualité de la visite organisée.	*	**	-	*
22	En tant que visiteur, je peux créer, à l'issue de ma visite, un compte afin de retrouver sur le site *Web* les photos, vidéos et expériences effectuées sur le CDV.	*	**	**	*
25	En tant que responsable commercial, je veux consulter les statistiques de temps passé par zone de visite et les activités réalisées par les visiteurs afin de proposer un meilleur service aux visiteurs.				
27	En tant que visiteur, je veux être déconnecté du site lorsque je clique sur le bouton déconnexion afin de ne plus être identifié.	**	*	-	-
30	En tant que guide, je veux modifier mon mot de passe sur l'application mobile en toute sécurité afin de sécuriser mon compte.	*	**	**	*

- : pas de besoin ** : besoin important* *** : besoin très important*

Preuve : les traces de l'activité du système sont opposables en cas de contestation.

Les espaces grisés seront à compléter sur votre copie au niveau de la question correspondante.

Document 2 : Extrait de l'analyse des risques et menaces de l'environnement

Acteurs à l'origine de la malveillance

Acteurs malveillants (menace)	**Modes opératoires (par exploitation d'une vulnérabilité)**	**Intitulé de l'exploitation**	**Probabilité**
Attaquant externe (*hacker*)	L'attaquant externe accède à la base de données	P1	**
	L'attaquant externe surcharge le système	P2	***
Acheteur	L'acheteur envoie de fausses informations	P3	**
	L'acheteur surcharge le système	P4	*
Visiteur	Le visiteur envoie de fausses informations	P5	*
	Le visiteur surcharge le système	P6	*

** : faible probabilité* *** : forte probabilité* **** : très forte probabilité*

Impacts des événements redoutés

Numéro de l'événement	Événement	Impact pour l'entreprise	Gravité
E1	Le système ne répond pas		
E2	Un attaquant accède à la base de données et ajoute des enregistrements dans la table billet	Perte financière pour l'entreprise	**
E3	Un attaquant accède à la base de données et efface la totalité des données		
E4	Un acheteur accède aux billets au format *PDF* d'un autre acheteur en modifiant le numéro de réservation dans la barre d'adresse	Problème de confiance. Désorganisation des visites	*
E5			

** : gravité modérée* *** : gravité très élevée*

Les espaces grisés seront à compléter et à justifier sur votre copie au niveau des questions correspondantes.

Document 3 : Description de l'attaque sur l'hôtel *Le Vallon*

Le 2 juin 2025, à 7 h 30 du matin, trois employés du service d'accueil et de réservation reçoivent un email provenant de `jpestampe@hotel_le_vallon.com`, expliquant que l'application de réservation doit être mise à jour immédiatement. Cyril Venart, qui prend son poste à l'accueil de l'hôtel à cette même heure, se connecte au système et vérifie sa messagerie. Il télécharge et installe immédiatement le fichier joint.

À 7 h 50, le poste de travail de Cyril ainsi que d'autres postes connectés au réseau commencent à ouvrir des fenêtres *popup* avertissant les utilisateurs que les fichiers de l'appareil ont été chiffrés, et que le seul moyen de les récupérer est d'acheter une clé de déchiffrement en suivant la procédure indiquée. Immédiatement prévenue, la DSI coupe tous les accès réseau, puis toutes les machines du SI. L'examen ultérieur des dégâts permettra de constater que tout l'intranet avait en fait déjà été touché : les bases de données contenant les données personnelles des clients et des employés étaient compromises, ainsi que certaines données légales et professionnelles annexes relatives au fonctionnement de l'organisation et de ses applications. Les sauvegardes sont également devenues inutilisables. Sans accès au réseau, des processus et des fonctions importantes (facturation, accès aux copieurs, prise de réservation, autres services...) sont devenus impossibles.

L'employé fautif justifiera son action malheureuse en indiquant qu'il avait reçu, quelques jours plus tôt, un email provenant déjà de M. Estampe expliquant qu'une mise à jour du logiciel était effectivement prévue ce lundi 2 juin.

Durant la semaine qui suit l'incident, la DSI tente de récupérer les données et le contrôle du système d'informations, en contractant par ailleurs les services d'une société spécialisée dans la cybersécurité. Toutes ces tentatives se révèlent infructueuses. Ayant déjà perdu plusieurs dizaines de milliers d'euros en pertes sèches, compensation et prestations externes, sans compter l'impact sur l'image de l'hôtel, la direction se résout finalement à payer la somme demandée par les pirates. Trois autres journées passent avant la réception de la clé de déchiffrement. Cependant, même avec celle-ci, la récupération des données sera longue et seulement partielle.

Document 4 : mail reçu par l'employé du service de réservation

De: "Jean-Pierre Estampe" <jpestampe@hotel_le_vallon.com>
Objet: URGENT: Mise à jour du logiciel de réservation
Date: Lun 2 Juin 2025 07:29:22 +0100
To: cvenard@hotel-le-vallon.com

Bonjour M. Venard,

Comme annoncé jeudi dernier, nous procédons aujourd'hui au déploiement de la mise à jour des applications clientes de réservation. La nouvelle procédure est automatisée, rapide et, si tout se passe bien, ne nécessite l'intervention sur place d'aucun technicien.

Nous souhaiterions tester au plus vite le bon fonctionnement des applications clientes mises à jour dès notre arrivée vers 8 h 00, à partir du serveur d'applications. Merci de bien vouloir procéder à la mise à jour d'ici là. Si le processus rencontre un problème, nous interviendrons alors très rapidement.

Veuillez suivre la procédure suivante :

- Vérifiez que tous les postes du service sont préalablement connectés (la mise à jour se fera automatiquement sur chacun d'entre eux) ;
- Initiez la mise à jour à partir de votre poste (fichier en pièce jointe) ;
- Patientez jusqu'à la fin du processus de mise à jour, qui ne devrait prendre que quelques minutes ; n'utilisez pas le système pendant ce temps ;
- Une fois la mise à jour terminée sur tous les postes, un message vous préviendra de la fin de la procédure ; le logiciel est alors de nouveau immédiatement opérationnel : vous n'avez pas à redémarrer le système.

Je vous remercie par avance pour votre implication dans cette nouvelle procédure de déploiement et vous souhaite une bonne journée.

Bien cordialement,

Jean-Pierre Estampe
Directeur des Systèmes d'Information
Hôtel Le Vallon

AVAST - L'absence de virus dans ce courrier électronique a été vérifiée par le logiciel antivirus Avast.
www.avast.com

PJ : Déploiement_MAJ_20250602.exe

Document 5 : Recensement des mesures de sécurité existantes identifiées

- Le système d'exploitation installé sur les postes clients est Windows 10 Professionnel.
- Dans le service restauration, un poste cependant tourne sous Windows XP SP2 (version la plus à jour) ; la mise à jour vers un OS plus récent n'est pas possible actuellement : ce PC est dédié exclusivement au pilotage d'un four-automate dont le logiciel ne fonctionne que sous Windows XP.
- Tous ces postes clients sont reliés au même réseau physique.
- Un logiciel antivirus est installé sur chaque poste client.
- Les logiciels, systèmes d'exploitation et antivirus sont mis à jour à chaque intervention des techniciens de la DSI sur un poste donné.
- L'accès physique à tous les postes est contrôlé par l'intermédiaire du système de caméras de surveillance de l'hôtel.
- L'accès à un poste de travail est contrôlé à l'aide d'un identifiant et d'un mot de passe ; l'utilisateur choisit librement son mot de passe lors de la création du compte utilisateur.
- Les mots de passe sont hachés en base de données (MD5)
- Les droits associés à chaque compte utilisateur sont ceux donnés par défaut par une installation standard (administrateur Windows).
- Les données utilisées par le logiciel de réservation, notamment, sont stockées dans une base de données sur le disque dur du serveur d'applications.
- À chaque accès en écriture à la base de données, le serveur enregistre, en local, dans un batch de fichiers de logs, une entrée sous cette forme (aucune autre journalisation n'a été recensée sur le SI) :
  - `2024-12-18T13:01:56 192.168.1.24`
- Sur ce serveur est installé un logiciel de sauvegarde qui fait une copie quotidienne automatique de la base de données sur deux disques durs externes connectés en permanence en USB à la machine.
- Une politique de sauvegarde sensiblement identique est utilisée sur les autres serveurs de l'intranet, la dureté de la redondance étant appliquée en fonction de l'importance des données stockées. Ces serveurs disposent notamment de plusieurs répertoires partagés sur le réseau pour les besoins des différents services. Le groupe Windows « Tout le monde » a les accés en lecture et en écriture sur chacun d'entre eux.
- Les employés de chaque département ont été efficacement formés à l'utilisation des logiciels qu'ils utilisent quotidiennement. Ils ont également été sensibilisés à la protection des données à caractère personnel des clients et des employés.