Notion de risques : Chap.9.b : Part 2 : Rapport et Matrice des risques

mardi 13 février 2024 10:01

Chapitre 9.b : Rapport et Matrice des risques

Objectifs

- Avoir des notions sur la gestion des risques
- Rédiger un rapport qui permettra aux directions de définir une stratégie globale de sécurité
- Savoir orienté les rapports en fonction du public

A. Introduction

Quel que soit la forme de l'audit interne/externe, qu'il s'appuie sur une approche top/down ou bottom/up, il convient de rédiger un rapport qui permettra de conduire une stratégie de sécurité globale. Celui-ci, s'il était complet devrait aborder :

- Identification des Vulnérabilités : Détecter les faiblesses dans les systèmes, applications, et configurations réseau qui pourraient être exploitées par des attaquants.
- Évaluation de l'Impact des Vulnérabilités : Comprendre l'impact potentiel d'une exploitation réussie sur les ressources et les opérations de l'organisation.
- Validation des Contrôles de Sécurité : Tester l'efficacité des mécanismes de défense en place, y compris les dispositifs de prévention d'intrusion, les firewalls, et les politiques de sécurité.
- Conformité aux Normes et Réglementations : Aider les organisations à se conformer aux exigences de sécurité spécifiées par les réglementations et les normes de l'industrie, telles que le PCI DSS, le GDPR, et l'ISO 27001.
- Formation et Sensibilisation à la Sécurité : Fournir une expérience pratique aux équipes de sécurité et sensibiliser le personnel à l'importance de la cybersécurité et aux techniques d'attaque courantes.
- Planification des actions (PA), des corrections et des améliorations : Proposer un planning, un suivi (actions, recommandations, améliorations, corrections) pour inscrire la sécurité comme une problématique globale de l'entreprise.

B. Notion de gestion des risques

B.1 : Introduction

La gestion des risques, de façon générale) vise à identifier, évaluer et hiérarchiser les risques liés aux activités d'une organisation, puis à les traiter méthodiquement, de manière coordonnée et économique, afin de réduire et contrôler la probabilité des événements redoutés, et leur impact éventuel. Pour ce qui nous concerne, nous devons appliquer certains principes et outils d'analyses de risques :

- Les matrices de gestion des risques servent à formaliser les risques potentiels(sources), leur périodicité de survenance et leur conséquences.
- L'évaluation des risques permet de créer un plan d'actions.
- Actualiser selon les besoins et les contraintes (1 f/mois ; 1 f/trimestre; 1 f/semestre ; 1 f/an).
- Actualiser à chaque nouveau risque non prévu lors de l'évaluation des risques.

B.2 : Principes de gestion des risques

1. Evaluer les risques
2. Évaluer la Fréquence/Vraisemblance/Probabilité de survenance des risques.
3. Supprimer les risques à la source (PA) ou diminuer leur impact (éviter, contourner).
4. Prendre en compte les évolutions technologiques.
5. Préparer un plan d'actions (Planifier, Exécuter, Contrôler)
6. Donner les instructions appropriées aux utilisateurs

B.3 : Référentiels d'Analyse des risques

L'analyse des risques consiste à répertorier les différents risques encourus, à en estimer leur probabilité et à étudier leur impact. La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait. Sur cette base, il peut être intéressant de dresser un tableau des risques à partir de la gravite/impact et de la potentialité (probabilité de se produire), en leur affectant des niveaux selon une échelle appropriée (à définir). Pour cela, nous nous appuyons sur des référentiels : "Fréquence/Vraisemblance/Probabilité" et "Gravité/Impact" répertorier les différents risques encourus, à en estimer leur probabilité et à étudier leur impact. La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait. Sur cette base, il peut être intéressant de dresser un tableau des risques à partir de la gravite/impact et de la potentialité (probabilité de se produire), en leur affectant des niveaux selon une échelle appropriée (à définir). Pour cela, nous nous appuyons sur des référentiels : "Fréquence/Vraisemblance/Probabilité" et "Gravité/Impact".

- Fréquence/Vraisemblance/Probabilité :
  - Mesure de la "Fréquence/Vraisemblance/Probabilité" d'un événement exprimée sous forme d'un nombre d'événements ou d'effets par unité de temps donnée.
  - Exemple d'un référentiel de fréquence

Etat	Fréquence	Score
RARE	1 fois par an ou moins	1
OCCASIONNEL	1 fois par mois	2
FREQUENT	1 fois par semaine	4
PERMANENT	Tous les jours	8

  - Exemple d'un référentiel de probabilité

PROBABILITE	%	Score
TRES IMPROBABLE	0,01%	1
IMPROBABLE (RARE)	0,1%	2
PROBABLE (OCCASIONNEL)	1%	4
TRES PROBABLE (FREQUENT)	10%	8

- Gravité/Impact /Impact :
  - La gravité d'un risque représente l'intensité potentielle des dommages d'un risque représente l'intensité potentielle des dommages.
  - Exemple d'un référentiel de gravité en terme de conséquence en terme humain, technique ou business

Gravité/Impact		Score
MINIME	Peu de conséquence	1
SIGNIFICATIVE	Conséquence moyenne	2
ELEVEE	Conséquence élevée	4
GRAVE	Conséquence très élevée	8

- Matrice des Risques Brut (Criticité ou Sévérité)
  - Valeur évaluant le risque sans tenir compte des actions existantes.
  - Sévérité = Score F* Score G
  - Exemple de matrice des risques

Fréquence*Gravité =>	1	2	4	8
8	8	16	32	64
4	4	8	16	32
2	2	4	8	16
1	1	2	4	8

- Risque Net ou Risque Résiduel :
  - Valeur évaluant le risque à la date du jour en tenant compte des actions existantesà la date du jour en tenant compte des actions existantes.
  - Le risque résiduel est en effet plus précis si l'on tient compte des **mesures de prévention existantes**. En intégrant un **coefficient de mesure de prévention** (variant de 0,1 à 1), on peut ajuster l'évaluation du risque résiduel en fonction de l'efficacité des contrôles ou mesures de prévention déjà en place. Ce coefficient réduit l'impact du risque initial, car il prend en compte l'atténuation fournie par les mesures actuelles.
  - **Risque Résiduel = "Score Probabilité" × "Score Impact" × "Mesure de Prévention"**

C. Analyse des risques

C.1 Interprétation des résultats.

L'analyse des risques implique d'analyser les données recueillies pour classer et identifier les vulnérabilités, comprendre leur impact potentiel en terme de sécurité, et évaluer le risque global pour l'organisation.

- Analyse des Vulnérabilités : Examiner chaque vulnérabilité détectée pour comprendre sa nature, **sa probabilité**, et les conditions d'**exploitabilité**.
- Évaluation de l'Impact : Déterminer l'**impact potentiel/gravité potentielle** de chaque vulnérabilité sur les actifs de l'organisation, en tenant compte de la probabilité d'exploitation et des conséquences d'une attaque réussie.
- Priorisation des Risques : Classer les vulnérabilités identifiées en fonction de leur sévérité (Score du risque) et de leur impact potentiel pour aider l'organisation à allouer ses ressources de manière efficace.

Matrice d'Analyse des Risques (Vulnérabilités) :

- Une matrice des vulnérabilités synthétise les vulnérabilités découvertes après un audit/une étude.
- Informations à remplir : Identifiant, Description, Probabilité, Gravité/Impact, Exploitabilité, Recommandations, Statut

Matrice des Risques :

ID Vulnérabilité	Description	Score de Probabilité	Gravité	Score de Gravité	Score de Risque (Probabilité * Gravité)	Recommandations	Statut de Correction
VULN001	Exemple de vulnérabilité dans Apache	8	GRAVE (8)	8	64	Mettre à jour vers la dernière version	En cours
VULN002	Exemple de vulnérabilité dans MySQL	4	SIGNIFICATIVE (2)	2	8	Appliquer le patch XYZ	Planifié
VULN003	Injection SQL sur le formulaire de login en PHP	2	ELEVEE (4)	4	8	Consolider le développement : filtrage htmlentities, etc.	Corrigé
VULN004	XSS sur la table des articles en PHP	1	SIGNIFICATIVE (2)	2	2	Consolider le développement : filtrage htmlentities, etc.	En cours

Matrice des risques : Appliquer les priorités

La **priorisation des vulnérabilités** dans le cadre d'un audit/d'une étude peut-être dérivée d'une évaluation des risques, qui prend en compte à la fois la **probabilité** et **la gravité potentielle** sur l'organisation. Cette approche permet de s'assurer que les efforts seront concentrés là où ils sont le plus nécessaires, optimisant ainsi l'utilisation des ressources de sécurité.

- Une matrice des risques synthétise les **risques potentiels** d'une vulnérabilité en fonction de

"Fréquence/Vraisemblance/Probabilité" et de **"gravité/impact".**

- Elle facilite la prise de décision concernant les mesures correctives à appliquer en priorité.
- Comment la Priorité est-elle Obtenue ?
    - La priorité est généralement obtenue en fonction du score "risque potentiel"

C.2 Recommandations et mesures correctives

Les recommandations fournissent des orientations sur la manière de remédier aux vulnérabilités identifiées et de renforcer la posture de sécurité de l'organisation.

- Mesures Correctives Spécifiques : Pour chaque vulnérabilité, proposer des mesures correctives spécifiques, en indiquant des solutions possibles, des mises à jour de sécurité, des configurations à modifier, ou des pratiques à adopter.
- Plan d'Action : Élaborer un plan d'action priorisé pour les corrections, en tenant compte des ressources disponibles et de l'impact sur les opérations de l'organisation.
- Suivi et Réévaluation : Recommander un suivi et une réévaluation réguliers pour s'assurer que les mesures correctives sont mises en œuvre et pour détecter de nouvelles vulnérabilités potentielles.

Matrice d'un plan d'actions et des responsabilités

- Une matrice synthétise les actions à entreprendre suite aux vulnérabilités découvertes, elle définit les **priorités**, les équipes ou les personnes responsables de l'exécution de l'action, ainsi que son délai de correction attendu et son statut d'avancement.
- Informations à remplir : Identifiant, Recommandation, Priorité, Responsable, Délai, Statut

Matrice du plan d'action (Matrice RACI*Matrice des Risques) :

ID Vulnérabilité	Recommandation	Priorité	Responsable	Délai	Statut
VULN001	Mettre à jour Apache vers la dernière version	Très Élevé	Équipe web	30 jours	En cours
VULN002	Appliquer le patch de sécurité XYZ pour MySQL	Elevé	Administrateur DB	60 jours	Planifié
VULN003	Consolider les développement : filtrage htmlentities, etc… Requête préparée	Elevé	Équipe développement	15 jours	Corrigé
VULN004	Consolider les développement : filtrage htmlentities, etc…	Faible	Équipe développement	30 jours	En cours

Tableau Combiné : Matrice des Risques et Plan d'Actions :

ID Vulnérabilité	**Description**	**Score de Probabilité**	**Gravité**	**Score de Gravité**	**Score de Risque**	**Recommandation**	**Priorité**	**Responsable**	**Délai**	**Statut**
VULN001	Exemple de vulnérabilité dans Apache	8	GRAVE (8)	8	64	Mettre à jour Apache vers la dernière version	Très Élevé	Équipe web	30 jours	En cours
VULN002	Exemple de vulnérabilité dans MySQL	4	SIGNIFICATIVE (2)	2	8	Appliquer le patch de sécurité XYZ pour MySQL	Élevé	Administrateur DB	60 jours	Planifié
VULN003	Injection SQL sur le formulaire de login en PHP	2	ÉLEVEE (4)	4	8	Consolider le développement : filtrage htmlentities, etc. Requête préparée	Élevé	Équipe développement	15 jours	Corrigé
VULN004	XSS sur la	1	SIGNIFIC	2	2	Consolider le	Faible	Équipe	30 jours	En

	table des articles en PHP		ATIVE (2)			développement : filtrage htmlentities, etc.		développement		cours

D. Rédaction du Rapport (Méthode/Résultats)

D.1 Rédaction de rapports.

Le rapport documente les découvertes, l'analyse et les recommandations. Il doit être clair, précis, et compréhensible et adapter aux différents publics (Direction générale, DSI, équipes informatique.

- Structure du Rapport : Un rapport typique inclut un résumé exécutif, la portée du test, la méthodologie utilisée, les vulnérabilités découvertes avec des preuves, l'analyse de l'impact, et les recommandations.
- Clarté et Précision : Utiliser un langage adaptée aux interlocuteurs. Fournir des preuves concrètes, comme des captures d'écran ou des logs, pour étayer les découvertes.
- Confidentialité : Traiter le rapport comme un document sensible, car il contient des informations détaillées sur les vulnérabilités de l'organisation.

D.2 Structure du Rapport selon le public concerné :

1. Résumé Exécutif (pour la Direction Générale)
   - Objectif : Fournir une vue d'ensemble non technique des résultats, des risques principaux, et des recommandations.
   - Contenu: Un tableau récapitulatif des risques majeurs, avec une évaluation de l'impact sur l'entreprise.
     - Matrice des risques majeurs issue du plan d'action
   - Format: Langage clair, sans jargon technique, axé sur les implications commerciales et les mesures correctives stratégiques.

2. Portée du Test et Méthodologie (pour le DSI et les Équipes Techniques)
   - Objectif : Détail de la portée des tests, des objectifs, et de la méthodologie utilisée.
   - Contenu :
     - Matrice des Vulnérabilités
     - Matrice des risques
     - Matrice du plan d'action
     - Portée des tests : Liste des systèmes, applications, et réseaux testés.
   - Méthodologie : Description des étapes des tests(**reconnaissance, scanning, exploitation, post-exploitation**),des outils utilisés, et des approches (boîte noire, blanche, grise)
   - Format : Plus technique, incluant des détails spécifiques sur les tests réalisés.

3. Détails des Vulnérabilités et Analyse d'Impact (pour les Équipes Techniques)
   - Objectif : Présenter en détail chaque vulnérabilité, avec des preuves et une analyse d'impact.
   - Contenu :
     - Matrice des Vulnérabilités : Tableau listant les vulnérabilités, avec colonnes pour ID, description, sévérité, impact, et preuves (captures d'écran, logs).
   - Analyse d'Impact : Discussion sur les implications de chaque vulnérabilité sur la sécurité et les opérations.
   - Format : Technique, avec des preuves concrètes et une évaluation précise de l'impact.

4. Recommandations et Plan d'Action (pour le DSI et les Équipes Techniques)
   - Objectif : Fournir des recommandations spécifiques pour remédier aux vulnérabilités identifiées.
   - Contenu :
     - Matrice de Recommandations : Tableau avec des recommandations, priorités, responsables, et délais.
   - Plan d'Action : Étapes proposées pour les corrections, avec une timeline et des indicateurs de suivi.
   - Format : Pragmatique, avec des actions claires et des priorités basées sur l'impact et la sévérité.

   a. Annexes (pour les Équipes Techniques)
   - Objectif : Fournir des informations supplémentaires et des preuves techniques.
   - Contenu : Détails techniques supplémentaires, scripts utilisés, réponses complètes des systèmes, configurations

testées.
- Format : Très technique.

E. Référence de modèles de tableaux

Ces modèles simplifiés doivent accompagner le rapport d'étude ou d'audit. Ils peuvent être adaptés pour tout type de projet, ils présentent les informations minimales à fournir pour suivre une gestion de risques en sécurité informatique ou de cybersécurité. Il ne faut pas oublier de clarifier les rôles et responsabilités dans la gestion des risques ou de la sécurité de l'information par une matrice RACI.

Modèle de Matrice des Risques :

Risque	Probabilité	Impact	Risque	Classification
Attaque par Malware	4	5	20	Élevé
Perte de Données	3	4	12	Moyen

Modèle de Plan d'Action Corrective

Date	Description de l'Action	Responsable	Date de Début	Date d'Échéance	État
2023-01-01	Mise à jour des mots de passe	IT Security	2023-01-02	2023-01-15	Terminé
2023-02-15	Formation des utilisateurs	RH	2023-02-16	2023-03-01	En Cours

Modèle de Tableau de Bord de Sécurité

Date	Description de l'Incident	Gravité	Responsable	Statut
2023-01-01	Tentative de phishing	Élevé	IT Security	Résolu
2023-02-10	Fuite de données	Critique	Data Team	En cours

Modèle Combiné : Matrice des Risques et Plan d'Action

Identifiant	Risque	Probabilité	Impact	Risque	Classification	Description de l'Action Corrective	Responsable	Date de Début	Date d'Échéance	État
VUL-001	Attaque par Malware	4	5	20	Élevé	Mettre à jour les antivirus	IT Security	2023-01-05	2023-01-15	Terminé
VUL-002	Perte de Données	3	4	12	Moyen	Renforcer la sauvegarde des données	Data Team	2023-02-20	2023-03-01	En cours
VUL-003	Panne du Système	2	4	8	Moyen	Réviser les plans de reprise	Infra Team	2023-02-25	2023-03-05	En cours
VUL-004	Vol d'Identifiants	5	3	15	Moyen	Implémenter l'authentification 2FA	IT Security	2023-03-10	2023-03-20	En attente

Modèle de Tableau de Bord de Sécurité (Gestion des incidents)

Identifiant	Date de l'Incident	Type d'Incident	Gravité	Description de l'Incident	Responsable	État de l'Incident	Action Corrective	Date de Début	Date d'Échéance	État de l'Action
INC-001	2023-01-	Attaque	Élevé	Plusieurs	IT	Résolu	Sensibiliser	2023-01-	2023-01-	Terminé

	10	par Phishing		utilisateurs ciblés	Security		les utilisateurs	11	20	
INC-002	2023-02-05	Fuite de Données	Critique	Données clients exposées	Data Team	En cours	Mise en place de restrictions d'accès	2023-02-06	2023-02-15	En cours
INC-003	2023-03-12	Malware sur un Serveur	Élevé	Serveur compromis par malware	IT Security	Enquête	Mise à jour des antivirus	2023-03-13	2023-03-18	En attente
INC-004	2023-04-01	Tentative d'Intrusion	Moyen	IP suspecte détectée	Réseau	En cours	Renforcement du pare-feu	2023-04-02	2023-04-10	En cours

Modèle de Matrice de Responsabilités RACI

La matrice de responsabilités utilise généralement le modèle RACI (Responsable, Autorité, Consulté, Informé), qui est un excellent moyen d'attribuer et de clarifier les rôles de chaque équipe ou individu pour les tâches spécifiques.

Tâche / Activité	**Responsable (R)**	**Autorité (A)**	**Consulté (C)**	**Informé (I)**
Identification des Risques	Analyste Risques	Directeur SI	Équipe IT	Responsable Sécurité
Analyse des Risques	Analyste Risques	Directeur SI	Équipe IT	Responsable Sécurité
Définition des Contrôles	Responsable Sécurité	Directeur SI	Responsable IT	Équipe IT
Mise en œuvre des Contrôles	Équipe IT	Responsable Sécurité	Consultant Externe	Directeur SI
Surveillance des Risques	Analyste Risques	Responsable Sécurité	Responsable IT	Directeur SI
Audit de Sécurité	Auditeur	Directeur SI	Responsable Sécurité	Équipe IT

Explication des Colonnes :

- **Tâche / Activité** : Liste des tâches ou activités clés dans le cadre de la gestion de la sécurité.
- **Responsable (R)** : La personne ou l'équipe qui exécute la tâche. C'est l'acteur qui a la responsabilité directe de la réalisation de la tâche.
- **Autorité (A)** : La personne ayant le pouvoir de décision finale, souvent le sponsor ou le chef de projet.
- **Consulté (C)** : Les personnes ou équipes consultées pour avis et conseils avant ou pendant la réalisation de la tâche.
- **Informé (I)** : Les personnes ou équipes informées des progrès et des résultats de la tâche, sans être directement impliquées.