ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams) fifth edition for Africa Region, Côte d'Ivoire Grand-Bassam, 01st -05th October 2018

Présentation: La gestion des risques cybernétiques

Par: Laïcana COULIBALY, AfricaCERT

I- GÉNÉRALITÉS

- Les organisations utilisent aujourd'hui les outils technologiques dans leurs activités quotidiennes pour accomplir leur stratégies: être plus performants, délivrer les services, augmenter leur rentabilité, promouvoir les ventes, stimuler l'innovation, accroître l'efficacité, et faciliter la gestion et l'analyse des données.

- Les risques pour la sécurité financière et les dommages à la réputation associés à cette révolution technologique nécessitent des indicateurs, des processus et des bonnes pratiques; en d'autre terme une stratégie efficace pour les aider à comprendre leurs systèmes d'information et à déterminer le niveau de sécurité et de contrôle qui est nécessaire pour protéger leur entreprise.

- À mesure que le monde devient plus en plus branché, les cyberattaques continuent de croître en ampleur et en gravité. Ces attaques constituent des menaces entrainant des incidents qui doivent êtres gérés.

AfricaCERT
United in promoting cyber security in Africa

II- DÉFINITIONS

- **Risque:** Le guide 73 de l'ISO définit un risque par la combinaison de la probabilité d'un événement et de ses conséquences. Il est souvent caractérisé en référence à des événements et des conséquences potentiels ou à une combinaison des deux. Cette définition est généralement étendue et on définit un risque à l'aide de ce que l'on nomme « l'équation du risque » :

  RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

- **Gestion des risques:** La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

- Améliorer la sécurisation des systèmes d'information.
- Justifier le budget alloué à la sécurisation du système d'information.
- Prouver la crédibilité du système d'information à l'aide des analyses effectuées

AfricaCERT
United in promoting cyber security in Africa

III-1- Concepts de la gestion des risques (1/3)

La gestion des risques, « dans son plus simple appareil », se compose de trois blocs interdépendants:

- l'organisation cible de l'étude, définie par les biens (assets) et ses besoins de sécurité,
- les risques pesant sur les biens
- et enfin les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité

III-1- Concepts de la gestion des risques (2/3)

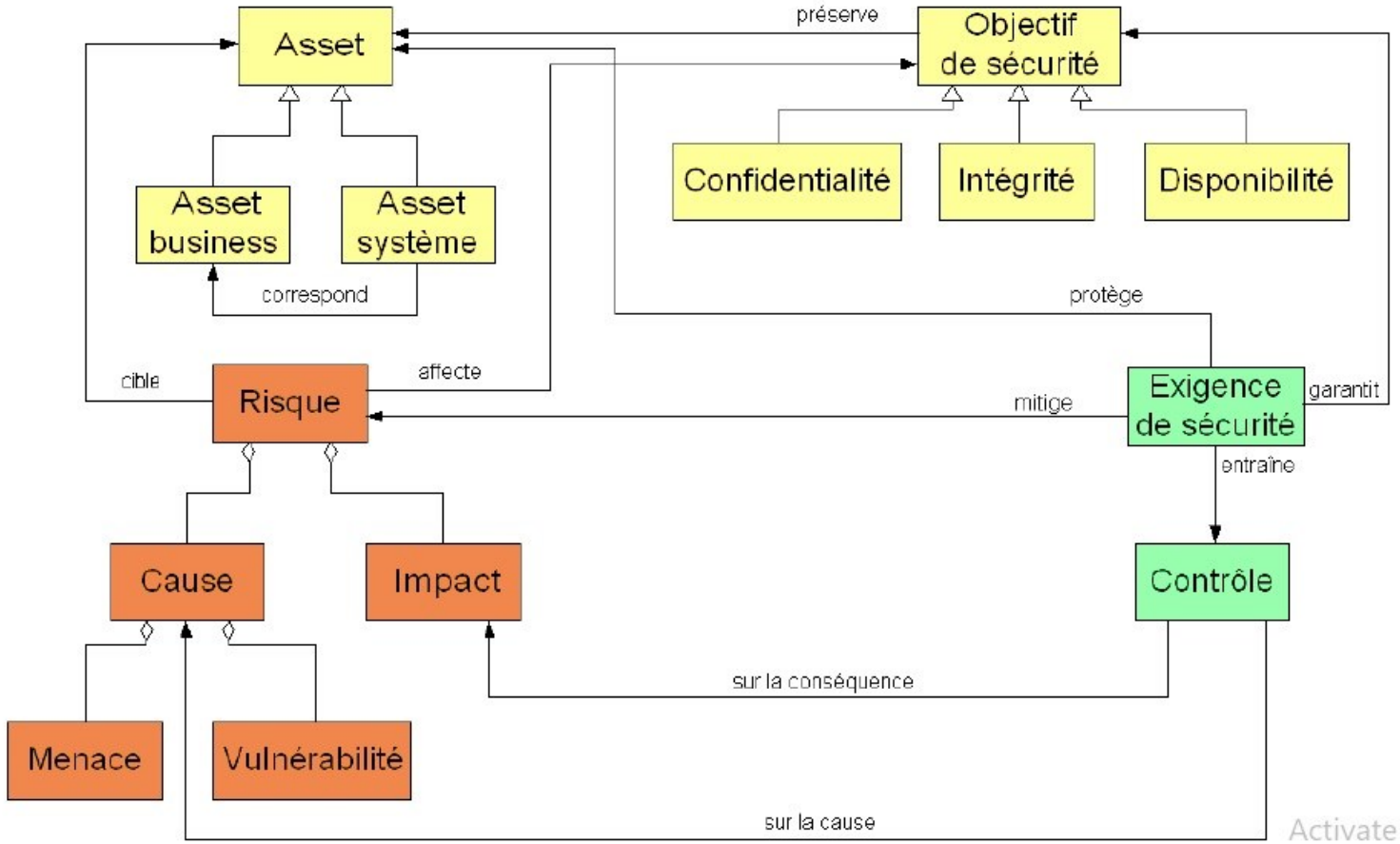

Figure 1: Les concepts de la gestion des risques

AfricaCERT
United in promoting cyber security in Africa

III-1- Concepts de la gestion des risques (3/3)

- Les Biens (assets) : l'ensemble des actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement.
  - informations (par exemple des numéros de carte bancaire);
  - processus (comme la gestion des transactions ou l'administration des comptes).
- Ces biens sont soumis à des risques de sécurité
- Mitiger ces risques et de protéger les biens = Mettre en place une politique de traitement des risques:
  - exigences de sécurité permettant de répondre aux risques. Ces exigences de sécurité vont ensuite entraîner la mise en place de contrôles (ou contre-mesures) de sécurité à implémenter, afin de satisfaire aux exigences.

AfricaCERT
United in promoting cyber security in Africa

III-1- Concepts de la gestion des risques (3/3)

- Les contrôles sont de deux types :
  - Sur la menace ou la vulnérabilité, afin de limiter la cause du risque ;
  - Sur l'impact, afin de limiter la conséquence du risque.

III-2- Le processus de gestion des risques

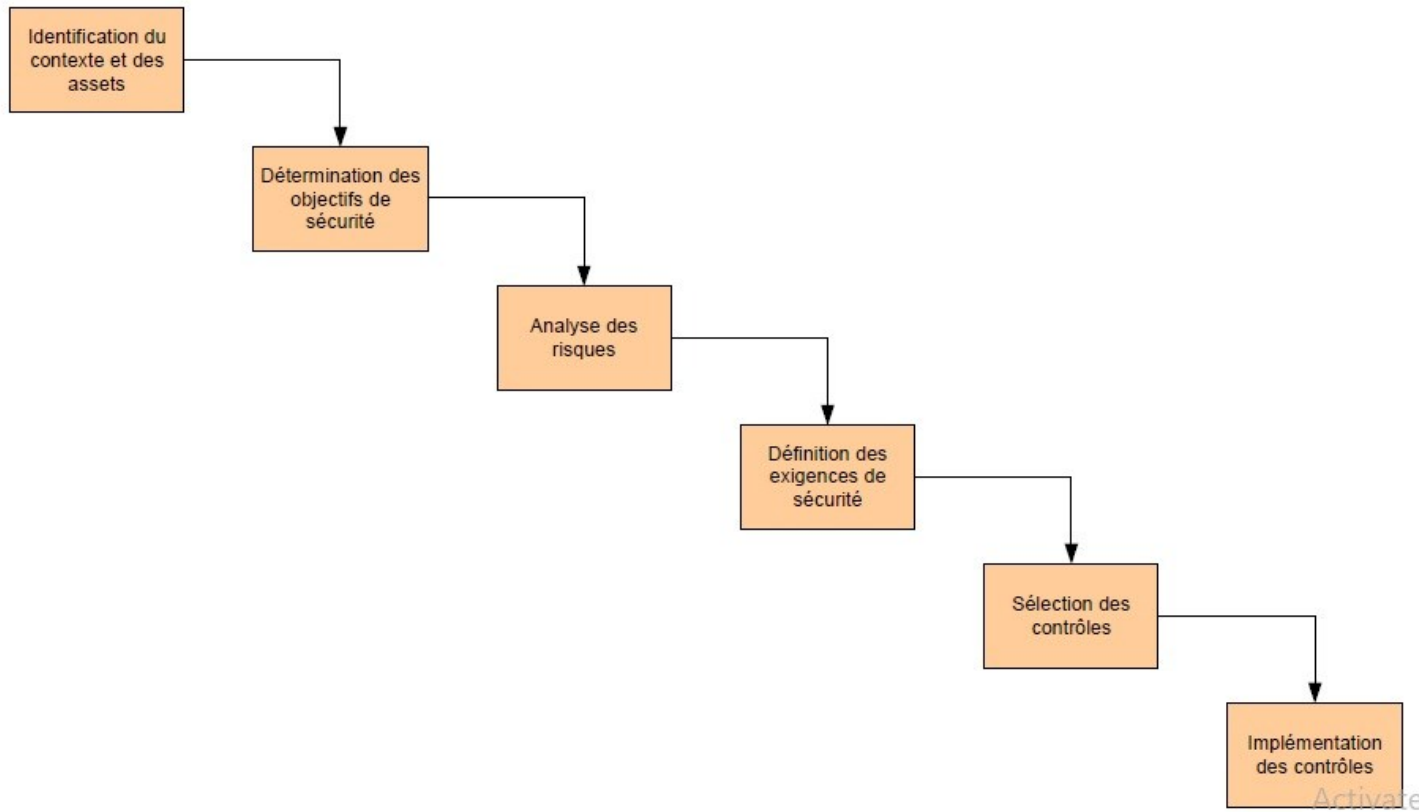

Figure 2: Le processus de gestion des risques

III-3- Le processus de gestion des risques (3/3)

- Dans la 1ère partie, il est question de prendre connaissance avec l'organisation, son environnement, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques
- La détermination des objectifs de sécurité vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets, en particulier au niveau business.
- L'analyse des risques constitue le cœur de la démarche de gestion des risques. Elle a pour finalité l'identification et l'estimation de chaque composante du risque (menace/vulnérabilité/impact), afin d'évaluer le risque et d'apprécier son niveau, dans le but de prendre des mesures adéquates. Aussi appelée, « Appréciation du risque ».

AfricaCERT
United in promoting cyber security in Africa

III-3- Le processus de gestion des risques (3/4)

- Une fois l'analyse des risques effectuée, la définition des exigences de sécurité permettra de réduire les risques identifiés
- Ici sont définis les choix techniques des solutions de sécurité, influencés par le système déjà en place, les compétences disponibles, les coûts de mise en œuvre
- Une fois les contrôles sélectionnés, il reste alors à les implémenter dans le SI et à éventuellement les tester et les évaluer
- Une fois les contrôles mis en place; l'étape suivante est la préparation a la gestion des incidents engendrés par les risques afin de maintenir le système d'information dans son état optimal.

AfricaCERT
United in promoting cyber security in Africa

IV- En Pratique (1)

- Les fonctions de haut niveau de la Gestion des risques dans une organisation est généralement assumée par un dirigent et implique toute la hiérarchie de l'Organisation.
- La Gestion des risques et les fonctions associées font partie d'un ensemble de documents qui constituent « la Stratégie de Cyber sécurité »
- Les éléments de la stratégie incluent la Gestion des Incidents de sécurité.
- Un incident de sécurité est la concrétisation d'un risque. Autrement dit c'est un évènement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien.

AfricaCERT
United in promoting cyber security in Africa

IV- En Pratique (2)

- La Vitesse a laquelle une organisation reconnait, analyse et répond aux incidents limite les dommages et réduits les couts de reprise d' activité.
- C'est pourquoi après avoir misé sur la prévention et la protection, il est necessaire d'investir dans la detection, la reaction et la gestion des incidents.
- Les fonctions de gestion d'incident sont généralement confiées a une équipe spécialisée qui peut être au sein de l'Equipe Informatique.
- Depuis l'avènement du Vers Morris, on assiste a la mise en place de Centres d'Alerte et de Réponse aux incidents Cybernétiques ou CSIRTs.
- Le CSIRT est une **équipe de sécurité opérationnelle**, composée d'experts de différents domaines (malwares, test d'intrusion, veille, lutte contre la cybercriminalité, forensics…). Elle est chargée de **prévenir** et de **réagir** en cas d'incidents de sécurité informatique.

AfricaCERT
United in promoting cyber security in Africa

V. Les Missions du CSIRT

Un CSIRT accomplit généralement 5 grandes missions :

- Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CSIRT, contribution à des études techniques spécifiques ;
- Etablissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CSIRT nationaux et internationaux.

AfricaCERT
United in promoting cyber security in Africa

V- La coopération comme indicateur de performance et de maturité.

- L'avantage d'un CSIRT est de centraliser la réponse à incident mais également de servir de relai vers l'intérieur de l'organisation (pour prévenir les menaces en informant, sensibilisant pour le réajustement des contrôles) et surtout vers l'extérieur à destinations des autres CSIRT et de la communauté sécurité en général.
- Des initiatives ont été rapidement lancées pour regrouper les CSIRT du monde entier et leur permettre de **coopérer** :

➢ L'AfricaCERT, qui a pour mission piloter de mettre en place un cercle de confiance, une plateforme d'échange d'expériences pour la communauté africaine et d'aider à la création de nouveaux CSIRT.

➢ Le FIRST (Forum of Incident Response and Security Teams), qui est une organisation mondiale qui regroupe plusieurs. Il s'agit avant tout d'un **cercle de confiance** dans lequel les différentes équipes de réponse peuvent partager de l'information et des bonnes pratiques. Le FIRST organise également une conférence annuelle internationale.

AfricaCERT
United in promoting cyber security in Africa

V- CONCLUSION

- La notion de risque, qui demeure intangible, reste difficile à appréhender : « Les risques désignent un futur qu'il s'agit d'empêcher d'avenir »
- L'incident est la concrétisation du risque
- Des équipes sont mis en place pour gérer les risques et donc diffèrent selon les secteurs et le type d'organisation. Ces équipes sont communément appelées CSIRT.
- La collaboration entre les CSIRTS comme nous le verrons cette après midi est un paramètre de maturité et de performance.

AfricaCERT
United in promoting cyber security in Africa

- Rendez-vous pour AfricaCERT 14 pendant AFRINIC-29 Hammamet, Tunisia, 26th - 30th Novembre 2018
  - CSIRT Création et Gestion
  - Gestion de Crises
  - Performance et Maturité
  - Comment conduire des Operations Anti Abuse
  - Journees AfricaCERT et visite de TunCERT

MERCI