cadre management et organisationnelle d'un CERT

3.1 Qu'est-ce qu'un CSIRT

L'acronyme CSIRT qui signifie Computer Security Incident Response Team, est principalement utilisé comme synonyme du terme protégé CERT (Computer Emergency Response Team), déposé aux Etats-Unis par CERT Coordinateur Center (CERT/CC). La première apparition d'un ver dans l'infrastructure informatique mondiale remonte à la fin des années 1980 avec Morris, qui s'est rapidement propagé pour contaminer de très nombreux systèmes IT dans le monde entier.

Cet incident a été un véritable signal d'alarme, dans la mesure où il a fait prendre conscience de la nécessité impérative d'une coopération et d'une coordination au niveau des administrateurs systèmes et des responsables informatiques pour lutter contre ce type de phénomène. Le temps étant un facteur critique, il convenait d'adopter une approche davantage organisée et structurée de la gestion des incidents de sécurité informatique. Aussi, quelques jours à peine après « l'incident de Morris », l'DARPA (Defense Advanced Research Projects Agency) créait-elle le premier CSIRT, en l'occurrence CERT, implanté à la Carnegie Mellon University de Pittsburgh (Pennsylvanie).

Un CSIRT est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La plupart des CSIRT offrent également à leurs parties prenantes, dans le but d'atténuer les risques et de minimiser le nombre d'interventions requises, des services à caractère préventif et éducatif. Ils publient des bulletins et avis de vulnérabilités concernant les logiciels et matériels en usage, et informent les utilisateurs des exploits et virus tirant parti des failles constatées. Les parties prenantes sont dès lors en mesure de procéder rapidement à l'application de correctifs et à la mise à jour de leurs systèmes.

- **Les avantages d'un CSIRT**

Disposer d'une équipe spécialisée en sécurité informatique aide toute entreprise à réduire, voire à prévenir, les incidents majeurs et à protéger un patrimoine précieux.

Le CSIRT peut offrir en autre les avantages suivants

- La centralisation de la coordination en matière de sécurité informatique au sein de l'entreprise ;
- La centralisation et la spécialisation du traitement et de la réponse aux incidents informatiques ;
- La disponibilité d'une expertise permettant de soutenir les utilisateurs et de les aider à la restauration de leurs systèmes après un incident de sécurité ;
- La gestion des aspects juridiques et la protection des preuves en cas d'action en justice ;
- Le suivi des évolutions dans le domaine de la sécurité ;
- La sensibilisation des parties prenantes en matière de sécurité informatique

- **Les services d'un CSIRT**

Un CSIRT peut proposer un très large éventail de services, mais aucun CSIRT n'en propose actuellement la gamme complète. La sélection des services les mieux adaptés apparaît donc comme une décision essentielle.

Services réactifs	Services proactifs	Traitement des artefacts
Alertes et avertissements Traitement des incidents Analyse des incidents Appui à la réponse aux incidents Coordination de la réponse aux incidents Traitement des vulnérabilités Analyse des vulnérabilités Réponse aux vulnérabilités Coordination des réponses aux vulnérabilités	Veille technologique Audits ou évaluations de la sécurité Configuration et maintenance de la sécurité Développement des outils de sécurité Services de détection des intrusions Diffusion d'information relatives à la sécurité	Analyse des artefacts Réponse aux artefacts Coordination des réponses aux artefacts

Tableau 1: Les services d'un CSIRT

3.2 Types et rôle d'un CSIRT

✓ Types

Il existe trois (3) principaux types de CSIRT à savoir :

- Public
  - CSIRT Gouvernemental : en charge des institutions gouvernementales
  - CSIRT d'Infrastructure Critique : en charge des infrastructure critique
  - CSIRT National : en charge de tous les intérêts de la nation (institution, gouvernementales, grand public, entreprises …)
- Public-Privé
  - CSIRT Sectoriel : en charge d'un secteur d'activité (défense, santé…)
  - CSIRT Universitaire : en charge d'un réseau universitaire
- ✓ Privé :
  - CSIRT Sectoriel : en charge d'un secteur d'activité (finance, énergie…)
  - CSIRT Privé : en charge de la réponse à incident pour une entreprise privée

✓ Rôle

Dans le processus d'identification et gestion des incidents, les équipe de réponse aux incidents de sécurité informatique (CSIRT) jouent un rôle d'assistance auprès des victimes. Grâce à leur expérience et à leur savoir-faire, elles sont en mesures aider les personnes ou les organisations en difficulté, de manière efficace, rapide et à bas coût. Un CSIRT aide les organisations à juguler et à réparer les failles de sécurité et les menaces informatique. Cette fonction réactive est appelée gestion des incidents. En général, elle comprend trois aspects principaux :

1. La fonction « signalement des incidents » (incident reporting) qui permet à un CSRIT de servir de point de contact centralisé pour signaler des problèmes locaux. Tous les rapports d'incident sont collectés dans un lieu unique où l'information peut être analysée ;
2. La fonction « analyse de l'incident » (incident analysis) cette fonction est utilisée pour déterminer les tendances et modes intrusion et pour recommander des stratégies de prévention adaptées à l'organisation. Une analyse de l'incident implique également une étude en profondeur du rapport ou de l'activité d'incident afin d'en déterminer la portée, la priorité et la menace, ainsi que la recherche de réponse possibles et de stratégies d'atténuation ;

3. La fonction « réponse aux incident » (incident response) qui peut prendre leurs formes. Un CSIRT peut envoyer des recommandations pour la récupération, le confinement ou la prévention à l'organisation ou effectuer ces étapes lui-même.

Un autre rôle des CSIRT dans le processus de gestion des incidents consiste à collecter des informations sur les incidents afin d'établir des statistiques permettant d'avoir une vue complète sur la cybersécurité et de prendre les décisions politiques adaptées.

3.3 Gestion des incidents en cybersécurité

Comme illustré dans la norme de gestion des incidents de sécurité de l'information ISO 27035, la chaine d'incident de cybersécurité se présente comme suit ;

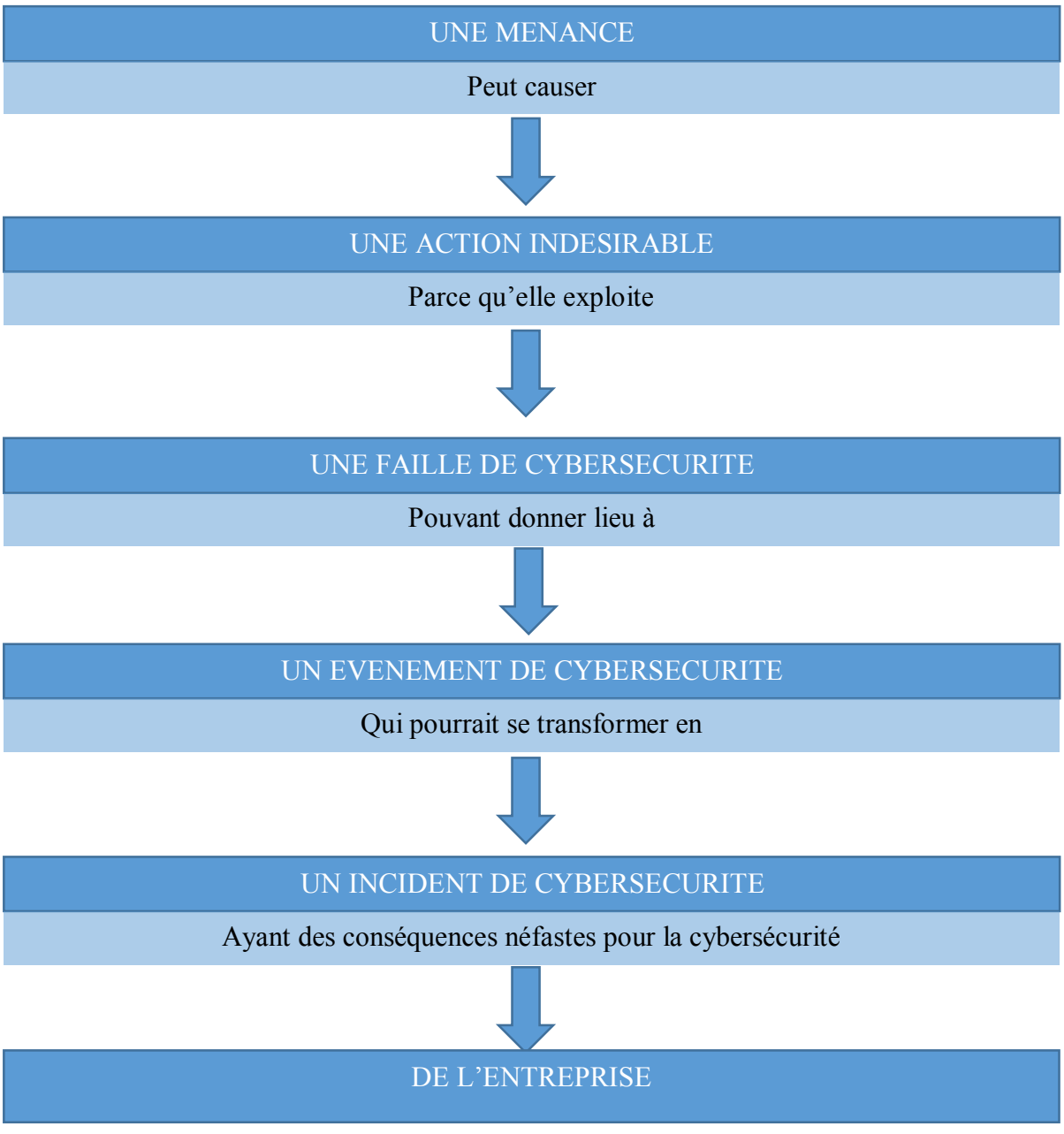

Figure 8:chaine d'incident de cybersécurité

- ✓ **Faille de cybersécurité :**

C'est une vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient.

- ✓ **Evénement de cybersécurité :**

C'est l'occurrence identifiée de l'état d'un service, d'un système ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.

- ✓ **Incident de cybersécurité :**

Un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus présentant une probabilité forte de compromettre les activités de l'entreprise et de menacer la sécurité de l'information. De ce fait, il a des impacts sur l'un des critères de la sécurité : Confidentialité, Intégrité, Disponibilité, Authentification.

La gestion d'un incident de sécurité ne s'improvise pas. Il est donc important de procéder de façon structurée afin de concilier efficacité et rapidité, tout en conservant une démarche d'amélioration continue.

Comme les atteintes à la sécurité sont de plus en plus sophistiquées, il est estimé qu'un nombre important des incidents demeure non décelé. Ceci est dû, d'une part, à l'absence de déploiement de méthodes de prévention avérées et moyens de détection et de contrôle en matière de cybersécurité, et d'autres part, au manque de compétences techniques.

Ainsi ; planifier et préparer une politique et un plan de gestion d'incident de cybersécurité s'avère indispensable pour une détection et une réponse efficaces aux incidents. La politique de gestion des incidents de cybersécurité doit fournir les principales démarches formellement documentées pour assurer une mise en œuvre cohérente et appropriée des processus et procédures. Elle doit faire partie de la stratégie de sécurité de l'information de chaque entité et doit être conforme à la politique et aux procédures appliquées par l'entreprise.

Pendant la phase de préparation, chaque entreprise vise également à limiter le nombre d'incidents qui pourraient se produire en sélectionnant et en mettant en œuvre un ensemble de contrôles et mesures basés sur les résultats des évaluations des risques. Le but est d'être en

mesure de prévenir les incidents tout en gardant les systèmes, les réseaux et les applications suffisamment sécurisés.

Par ailleurs, garder le nombre d'incidents raisonnablement bas est très important pour protéger les processus métiers de l'entreprise. Si les contrôles de sécurité sont insuffisants, un nombre important et élevé d'incident peuvent se produire, mettant à mal l'équipe de réponse aux incidents. Cela peut conduire à des réponses lentes et incomplètes, qui se traduisent par un impact négatif plus important. Bien que les équipes de réponse aux incidents ne soient généralement pas responsables de la sécurisation des ressources, elles peuvent émettre et faire valoir les bonnes pratiques de sécurité suite à l'identification des défaillances et des problèmes que l'entreprise ignore.

3.4 Détecter et identifier les incidents en cybersécurité

La phase de détection consiste à déceler un événement susceptible de constituer un incident de cybersécurité et d'en informer les responsables des systèmes touchés et de déclencher le processus de réponse à l'incident

De façon générale, lors de la phase de détection l'entreprise doit entreprendre les actions clés suivantes :

- Journaliser l'activité système et réseau de l'entreprise ;
- Collecter des informations permettant d'assurer une connaissance de la situation à partir de source de données internes et externes ;
- Disposer des outils de détection et les configurer selon les risques et menaces qui pèsent sur l'entreprise ;
- Assurer un suivi et monitoring permanent par l'équipe de sécurité ;
- Détecter et signaler l'occurrence d'un événement de sécurité de l'information ou l'existence d'une vulnérabilité, que ce soit manuellement ou automatiquement ;
- Surveiller les alertes transmises par les systèmes de sécurité internes ;
- Surveiller l'information communiquée et les alertes diffusées par les organismes spécialisés dans la détection des incidents de cybersécurité et la réponse aux attaques informatique ;

Pour pouvoir mette en place les recommandations susvisées et réussir la phase de détection, il est primordial pour chaque entreprise de comprendre les signes d'un incident et pouvoir les

collecter à partir des différentes sources disponibles au sein de l'entreprise en fonction de son secteur d'activité.

La phase d'identification repose sur l'évaluation des événements de cybersécurité décelés pendant la phase de détection. Cette évaluation vise à déterminer s'il s'agit réellement d'un incident de cybersécurité, de déterminer son incidence et son envergure, son impact ainsi que la cause probable de l'incident. Les tâches à accomplir lors de cette phase se présentent comme suit :

- Evaluer l'événement et confirmer qu'il s'agit d'un incident ;
- Désigner les personnes responsables de l'incident ;
- Déterminer le type de l'incident ;
- Déterminer le vecteur d'attaque susceptible ;
- Déterminer les données, systèmes ou réseaux touchés ;
- Cerner l'impact sur la confidentialité, l'intégrité et la disponibilité ;
- Aviser les personnes compétentes

3.5 Réponse aux incidents en cybersécurité

Conformément aux actions menées durant la phase de détection et d'identification, cette étape consiste à apporter les réponses adéquates aux incidents de cybersécurité détectés. Une fois qu'un incident de cybersécurité est confirmé, les activités suivantes doivent être exécutées :

- Attribuer les responsabilités et les rôles aux différents membres de l'équipe d'intervention interne ou externe ou mixte ;
- Elaborer des procédures formelles à suivre pour chaque personne impliquée dans l'incident ;

La première phase d'une réponse à incident est l'acquisition des preuves de compromission. Les analystes doivent reconstituer le scénario complet d'attaque (Exploitation d'une vulnérabilité, élévation de privilèges, exfiltration de données …). Les évidences collectées doivent être stockées en toute sécurité. L'acquisition des données peut se faire :

- ✓ **À chaud :** sur un système en marche (on parle de « live forensics ») la réponse à chaud permet de mener des investigations en collectant des « artefacts » sur des systèmes en marche. A ce stade, les détails de la menace sont toujours inconnus, il faut donc commencer par identifier et quantifier la menace à travers la collecte des informations à savoir :

- La mémoire volatile ;
- Les « prefetch files » ;
- Les clés de registre ;
- Les connexions réseau ouvertes ;
- Les comptes système :
- Etc

✓ **À froid :** sur un système éteint cette manière d'acquisition des évidences est très couteuse en termes de temps. Elle repose sur la création d'une image du disque authentique à celle utilisé par le système compromis. Cette action est primordiale dans le cas où on est sûr que la machine cible est compromise.

Après analyse des informations relatives à l'incident, il faut lancer la procédure de restauration et d'éradication qui consiste à

- Supprimer tous les éléments et évidences associés à l'incident :
- Corriger toutes les vulnérabilités exploitées par l'attaquant :
- Restaurer à partir d'une sauvegarde saine ou réinstaller le système en entier :
- Déterminer la source du problème pour sécuriser d'avantage

Après le traitement d'un incident, un rapport de synthèse des résultats de l'investigation doit être rédigé et doit être communiqué à toutes les parties concernées.

3.6 La communication des incidents en cybersécurité

La gestion des incidents de cybersécurité nécessite une coordination minutieuse au sein de l'équipe de réponse, mais également avec diverses parties prenantes internes autant qu'externes. Un plan de communication dédie est alors essentiel : il fournit conseils et orientation à ces efforts de communication. Comme pour les éléments du plan de réponse à incident, il est nécessaire d'élaborer le plan de communication au préalable pour assurer une prise de décision saine et sereine, malgré la forte pression qui s'exerce inéluctablement sur les équipes dans un contexte de crise.

3.7 Suivi et clôture des incidents en cybersécurité

Après le traitement d'un incident, l'entreprise doit passer en revue l'ensemble des décisions prises et les étapes suivies tout au long du cycle de traitement de l'incident afin de déterminer les points à l'égard desquels des améliorations devraient être apportées.

En outre, des réunions périodiques doivent être programmées pour identifier et corriger les faiblesses systémiques et les lacunes identifiées dans les politiques et les procédures adoptées. Enfin, les rapports de suivi pour chaque incident résolu doivent être exploités pour mieux traiter les futurs incidents et utilisés comme cas d'études dans la formation des nouvelles recrues.