ACTIVITE PSSI 4 – Socle de sécurité

Travail essentiellement basé sur:
https://cyber.gouv.fr/sites/default/files/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

1. Définir un cadre de gouvernance au risque numérique

Une bonne gouvernance du risque numérique passe par la mise en place d'un comité dédié et adapté aux réalités de l'organisation. Son rôle est de définir la **stratégie de sécurité numérique** de l'organisation, de s'assurer de sa mise en œuvre, de piloter la performance et de valoriser les investissements réalisés.
La gouvernance du risque numérique s'inscrit dans une démarche de long terme et doit pouvoir trouver sa place dans le fonctionnement habituel de l'organisation. Elle s'appuie sur trois «lignes de maîtrise»:

- Les fonctions opérationnelles et les responsables métiers
- Les spécialistes des risques (y compris numériques) à même d'assister les fonctions opérationnelles dans l'identification et l'évaluation de leurs risques
- La fonction d'audit (interne ou externe selon la taille de l'organisation) indépendante et liée au plus haut niveau de l'organisation

Dans le cadre de la gouvernance des risques fondée sur les "trois lignes de maîtrise", adaptée à TechNova, voici comment cela pourrait être mis en œuvre:

1. Première ligne de maîtrise (Opérationnelle):
- Les équipes opérationnelles, y compris les développeurs, les administrateurs système, les responsables des applications mobiles et des plateformes cloud, sont responsables de la mise en œuvre des contrôles de sécurité au niveau opérationnel.
- Ils sont chargés de s'assurer que les applications et les plateformes sont conçues et configurées de manière sécurisée, en mettant en œuvre des mesures de sécurité telles que le chiffrement des données, l'authentification multi-facteurs, et la surveillance des journaux d'audit.

2. Deuxième ligne de maîtrise (Spécialistes des risques):
- Les spécialistes des risques, y compris les experts en cybersécurité, les spécialistes de la conformité réglementaire et les responsables de la gestion des risques, fournissent un soutien et une expertise aux équipes opérationnelles dans l'identification, l'évaluation et la gestion des risques liés à la sécurité de l'information.
- Ils développent des politiques de sécurité, des procédures et des normes pour guider les pratiques de sécurité de l'entreprise, en tenant compte des menaces émergentes telles que les attaques par phishing et les violations de données.

3. Troisième ligne de maîtrise (Fonction d'audit):
- Une fonction d'audit interne ou externe, indépendante de l'exploitation quotidienne de l'entreprise, est chargée d'évaluer l'efficacité des contrôles de sécurité et des processus de gestion des risques.
- Ils réalisent des audits de conformité pour vérifier si les pratiques de sécurité de l'entreprise sont conformes aux normes et réglementations applicables, et identifient les domaines d'amélioration potentiels.

Ce modèle de gouvernance des risques basé sur les "trois lignes de maîtrise" permet à TechNova de bénéficier d'une approche holistique de la gestion des risques, en intégrant les responsabilités et

l'expertise à différents niveaux de l'organisation pour garantir une sécurité efficace des données et des systèmes.

2. Bâtir son seuil d’acceptation des risques en l’argumentant

L’appétence aux risques est fortement liée à la culture de l’organisation, à son secteur économique, ses implantations et à sa stratégie de développement. Elle formalise les attentes des instances dirigeantes en matière de prise de risques. Fruit d'échanges avec les parties prenantes de l’organisation (banques, assurances, partenaires, clients ou fournisseurs, etc...), l’appétence aux risques définit le seuil d’acceptation des risques de l’organisation.
Pour être efficace, l’appétence aux risques doit être régulièrement réévaluée au moyen d’indicateurs de performance et à la lumière des évolutions que connaît l'environnement (sociales, techniques, économiques, environnementales et politiques).

Définir des seuils d'acceptation des risques est crucial pour aider une organisation à décider quels risques elle est prête à accepter, à atténuer ou à transférer. Voici quelques exemples de seuils d'acceptation des risques pour TechNova, ainsi que des arguments pour chaque seuil:

1. Taux de réussite des attaques par phishing:
   - Seuil : Accepter un taux de réussite des attaques par phishing inférieur à 5%.
   - Argument : Un taux de réussite des attaques par phishing inférieur à 5% indiquerait une sensibilisation adéquate à la sécurité parmi les employés et une capacité à reconnaître et à signaler les e-mails de phishing, réduisant ainsi le risque d'intrusion dans le système.

2. Nombre de violations de données par an:
   - Seuil : Accepter moins de deux violations de données par an.
   - Argument : Un nombre limité de violations de données par an indique une bonne gestion des risques et une robustesse des contrôles de sécurité, ce qui renforce la confiance des clients et protège la réputation de l'entreprise.

3. Délai de détection des incidents de sécurité:
   - Seuil : Détecter les incidents de sécurité dans les 24 heures suivant leur survenance.
   - Argument : Une détection rapide des incidents de sécurité permet une réponse proactive et une minimisation des dommages potentiels, réduisant ainsi l'impact financier et la perte de données sensibles.

4. Conformité aux réglementations de protection des données:
   - Seuil : Maintenir un niveau de conformité de 95% ou plus avec les réglementations de protection des données telles que le RGPD.
   - Argument : Un niveau élevé de conformité aux réglementations de protection des données est essentiel pour éviter les amendes et les sanctions réglementaires, ainsi que pour maintenir la confiance des clients dans la sécurité de leurs données.

5. Nombre de contrôles de sécurité non conformes lors des audits internes:
   - Seuil : Maintenir moins de 5% de contrôles de sécurité non conformes lors des audits internes.
   - Argument : Un faible pourcentage de contrôles de sécurité non conformes indique une bonne gouvernance des risques et une attention constante à l'efficacité des contrôles de sécurité, réduisant ainsi le risque d'incidents de sécurité.

En définissant des seuils d'acceptation des risques clairs et en les alignant sur les objectifs stratégiques et les priorités de l'entreprise, TechNova peut prendre des décisions éclairées pour gérer efficacement les risques liés à la sécurité de l'information.

3. Construire ses pires scénarios de risque

Adopter une approche par conformité aux risques les plus vraisemblables: Le respect de normes et de bonnes pratiques en matière de sécurité des SI permet d'anticiper la survenance des cyberattaques les plus vraisemblables. En prenant ainsi connaissance des mesures de sécurité numériques indispensables à la construction du socle de sécurité, l'organisation devient capable de recentrer son analyse de risque en s'intéressant aux scénarios les plus critiques pour son activité. Identifier les scénarios de cyberattaque critiques: Le comité des risques numériques élabore des scénarios de cyberattaque susceptibles d'impacter une ou plusieurs activités vitales pour l'organisation. Ces impacts peuvent être numériques, physiques, financiers, liés à la réputation ou encore juridiques. Le niveau de risque est ensuite défini en fonction de la gravité de ces impacts et de la vraisemblance de ces scénarios. La vraisemblance reflète le degré de faisabilité ou de possibilité qu'un attaquant aboutisse à son objectif.

Voici quelques-uns des pires scénarios de risque auxquels TechNova pourrait être confrontée en termes de cybersécurité:

1. Violation massive des données clients:
   - Scénario : Une faille de sécurité importante dans les systèmes de TechNova conduit à une violation massive des données clients, exposant des informations sensibles telles que les identifiants personnels, les informations financières et les données de paiement.
   - Impact : Perte de confiance des clients, dommages à la réputation de TechNova, amendes réglementaires importantes, poursuites judiciaires, perte de revenus et de clients.

2. Arrêt prolongé des services cloud:
   - Scénario : Une attaque par déni de service distribué (DDoS) cible les serveurs cloud de TechNova, entraînant un arrêt prolongé des services pour les clients.
   - Impact : Perte de revenus, insatisfaction des clients, perte de confiance dans la disponibilité des services de TechNova, dommages à la réputation.

3. Vol de propriété intellectuelle:
   - Scénario : Des cybercriminels réussissent à accéder aux données sensibles de TechNova, y compris des informations sur la propriété intellectuelle, telles que des codes sources, des plans de produits et des secrets commerciaux.
   - Impact : Perte de compétitivité sur le marché, réduction de la valeur de TechNova, litiges pour violation de la propriété intellectuelle, dommages à long terme à la rentabilité et à la croissance de l'entreprise.

4. Ransomwares sur les systèmes critiques:
   - Scénario : Les systèmes informatiques critiques de TechNova sont infectés par un logiciel de rançon, paralysant les opérations commerciales et empêchant l'accès aux données essentielles.
   - Impact : Perturbation majeure des opérations commerciales, perte de données critiques, coûts élevés de récupération des données ou de paiement de la rançon, perte de confiance des clients et des investisseurs.

5. Compromission des identifiants administratifs:
   - Scénario : Les identifiants administratifs de haut niveau sont compromis, permettant à des attaquants d'accéder et de modifier les systèmes, les données sensibles et les paramètres de sécurité de TechNova.

- Impact : Perte de contrôle sur les systèmes et les données, compromission de la confidentialité et de l'intégrité des données, perturbation des opérations commerciales, dommages à la réputation et perte de confiance des parties prenantes.

En anticipant et en planifiant la réponse à ces pires scénarios de risque, TechNova peut mieux se préparer à faire face à des situations critiques et à réduire leur impact potentiel sur ses activités et sa réputation.

4. Définir sa stratégie de sécurité numérique

Analyse des risques numériques: La phase d'analyse des risques correspond aux choix et arbitrages faits par le dirigeant au regard des enjeux et objectifs de son organisation. Ces choix doivent s'appuyer sur:

- la vraisemblance d'exploitation des chemins d'attaques et l'impact des pires scénarios sur l'organisation
- la capacité des mesures de sécurité en place à empêcher la survenance des scénarios
- les ressources financières, humaines et techniques disponibles.

En tenant compte de ces critères, le dirigeant sera en mesure de choisir les options de traitement des risques à retenir telles que la mise en œuvre de mesures de sécurité, l'évolution des processus métiers ou encore le transfert contractuel des risques vers des tiers externes (sous-traitants, assurances, etc.)

Stratégie de sécurité numérique: Les options de traitement des risques sont déclinées dans la stratégie de sécurité numérique qui sera pilotée par le comité des risques numériques.
Cette stratégie comprend quatre axes :

- l'implémentation progressive du socle de sécurité afin de faire converger celui-ci avec la politique de sécurité des systèmes d'information (PSSI)
- la mise en œuvre d'une réponse aux scénarios de cyberattaque critiques. Cette réponse se traduit par l'établissement d'un plan d'amélioration continue de la sécurité (PACS) incluant une démarche d'homologation
- la valorisation de la sécurité numérique par la communication en vue de développer un avantage concurrentiel
- une politique de transfert de risque efficace vers le marché de l'assurance pour compléter le schéma de gestion de risque. Cette politique doit être pensée de façon globale mais détaillée par une équipe spécifique incluant le risk manager, le courtier et l'assureur

En élaborant une stratégie de sécurité numérique pour TechNova, il est essentiel de prendre en compte la vraisemblance d'exploitation des chemins d'attaques, l'impact des pires scénarios sur l'organisation, la capacité des mesures de sécurité en place à empêcher la survenance des scénarios, ainsi que les ressources financières, humaines et techniques disponibles. Voici comment cette stratégie pourrait être construite:

1. Évaluation des risques et priorisation:
   - Effectuer une évaluation approfondie des risques en identifiant les vulnérabilités potentielles dans les systèmes, les applications et les processus métier.
   - Prioriser les risques en fonction de leur vraisemblance d'exploitation et de leur impact sur l'organisation, en se concentrant sur les pires scénarios qui présentent le plus grand risque.

2. Renforcement des mesures de sécurité existantes:
- Examiner et renforcer les mesures de sécurité existantes pour s'assurer qu'elles sont adéquates pour prévenir les scénarios de risque identifiés.
- Mettre en œuvre des contrôles de sécurité supplémentaires, tels que l'authentification multi-facteurs, le chiffrement des données, la surveillance des journaux d'audit et les pare-feu de nouvelle génération.

3. Mise en place de solutions de détection et de réponse aux incidents:
- Mettre en place des outils de détection des menaces pour surveiller en permanence les activités suspectes et les indicateurs de compromission dans les systèmes et les réseaux.
- Élaborer et tester des plans de réponse aux incidents pour savoir comment réagir rapidement et efficacement en cas d'incident de sécurité.

4. Formation et sensibilisation des employés:
- Fournir une formation régulière sur la sécurité de l'information pour sensibiliser les employés aux menaces potentielles, y compris les attaques par phishing et les violations de données.
- Encourager les pratiques de sécurité telles que la création de mots de passe forts, la mise à jour régulière des logiciels et le signalement des incidents de sécurité.

5. Allocation efficace des ressources:
- Allouer les ressources financières, humaines et techniques de manière efficace en fonction des priorités de sécurité identifiées lors de l'évaluation des risques.
- Identifier les domaines où des investissements supplémentaires sont nécessaires pour renforcer la sécurité de l'organisation, tout en maximisant l'utilisation des ressources existantes.

En suivant cette stratégie de sécurité numérique, TechNova peut améliorer sa posture de sécurité, réduire les risques liés aux pires scénarios identifiés, et protéger efficacement ses données, ses systèmes et sa réputation contre les menaces potentielles.

5. Argumentez que doivent contenir les polices d’assurance adaptés

Faire l’inventaire des couvertures existantes: Avant de se mettre en quête d'une assurance spécifique, l’organisation doit d'abord faire un état des lieux de ses polices d’assurance dans le cas où l’une d’elle prévoirait la couverture d’incidents numériques. En effet, il est tout à fait possible que le risque numérique soit partiellement couvert au titre de dommages ou en termes de responsabilité civile.
Aujourd’hui toutefois, les couvertures classiques ne couvrent que très partiellement le risque numérique. S’il est parfois possible d’interpréter certaines clauses en faveur d’une prise en charge de ce type de risque, les assureurs sont généralement peu enclins à les couvrir. Ainsi, on tend de plus en plus vers une exclusion explicite du risque numérique des contrats d'assurance classiques, au profit de polices d’assurance plus spécifiques.

Les quatre piliers d'une politique d'assurance cyber:

- Prévention : l'assureur va aider l’organisation à mettre en place ou améliorer la gestion de son risque numérique, en lui apportant son support dans l’application des démarches décrites dans cet ouvrage. Ainsi, la mise en place d'une police peut permettre à l’organisation d'améliorer sa gestion du risque numérique grâce, notamment, au diagnostic et recommandations émis par l’assureur.
- Assistance : en cas d'événement, l'assureur entrera en jeu pour apporter son expertise et permettre ainsi de sortir plus vite de la crise. En aidant au redémarrage rapide de l’activité, il peut permettre de

réduire le montant des pertes.

- Couverture des opérations : l'assureur couvre les pertes financières directement subies par l'organisation : pertes d'exploitation, de revenus et dépenses supportées pour faire face à la crise.
- Couverture de la responsabilité : l'assureur va couvrir le coût des recours et dommages éventuellement subis par des tiers.

Pour assurer une couverture complète des risques liés à la cybersécurité, les polices d'assurance cyber doivent généralement contenir des éléments qui couvrent les quatre piliers d'une politique d'assurance cyber : prévention, assistance, opérations et responsabilité. Voici comment chacun de ces piliers peut être argumenté dans le contexte des polices d'assurance adaptées:

1. Prévention:
   - Argument : Les mesures de prévention sont essentielles pour réduire la probabilité d'occurrence d'incidents de sécurité. Une police d'assurance cyber devrait inclure des incitations financières pour encourager les assurés à mettre en œuvre des mesures de sécurité préventives telles que la formation des employés, la mise à jour des logiciels, la gestion des vulnérabilités et la surveillance continue des réseaux.

2. Assistance:
   - Argument : En cas d'incident de sécurité, il est crucial d'avoir accès à une assistance immédiate et spécialisée pour atténuer les dommages potentiels et reprendre les opérations normales. Une police d'assurance cyber devrait inclure des services d'assistance 24/7 pour fournir une réponse rapide, des conseils d'experts en gestion des incidents et des services de restauration des données et des systèmes.

3. Opérations:
   - Argument : Les opérations de sécurité efficaces sont nécessaires pour détecter, analyser et répondre aux menaces de manière proactive. Une police d'assurance cyber devrait inclure des clauses couvrant les coûts associés aux opérations de sécurité, tels que les frais de surveillance des réseaux, les analyses de sécurité régulières et les tests de pénétration.

4. Responsabilité:
   - Argument : En cas de violation de données ou d'autres incidents de sécurité, une entreprise peut être tenue responsable des dommages causés aux tiers, tels que les clients, les partenaires commerciaux et les régulateurs. Une police d'assurance cyber devrait inclure une couverture de responsabilité civile pour indemniser les tiers pour les pertes financières et les frais juridiques résultant d'une violation de données ou d'autres incidents de sécurité.

En incluant ces quatre piliers dans les polices d'assurance cyber, TechNova pourra bénéficier d'une protection complète contre les risques liés à la cybersécurité, tout en étant mieux préparée à faire face aux conséquences financières et opérationnelles des incidents de sécurité.