Sécurité du Système d'Information

Constats

- dans 80 % des cas, ce sont les maladresses internes, volontaires ou non, ou l'absence de sauvegardes fiables qui sont à l'origine de la perte ou de la destruction d'informations sensibles
- les 20 % restants sont imputables à des actes externes mal intentionnés

Pourquoi les risques ont-ils augmenté ?

- développement des nouvelles technologies
- augmentation du nombre d'utilisateurs
- augmentation des moyens d'accès à l'information
- augmentation spectaculaire du volume des données à sécuriser
- développement du travail à distance

Evaluation de la menace

- connaissons-nous réellement les menaces qui pèsent sur notre système d'information ?
- la réponse est : non
- nous avons donc besoin d'une méthode d'analyse pour procéder à un audit de notre organisation, interne ou avec aide externe

Audit de l'organisation en 3 points

1. Contexte commercial

- qualifier la valeur de nos produits : haute technologie, produits communs …
- connaitre la concurrence

2. Contexte technique

- déterminer le rôle et importance de notre SI : majeur, normal, mineur
- qualifier le matériel sur lequel fonctionne le SI
- qualifier les logiciels sur lesquels repose le SI
- déterminer le degré d'homogénéité des matériels et logiciels utilisés

Audit de l'organisation en 3 points

3. Contexte humain

- évaluer les décisionnaires
- évaluer les utilisateurs du SI : qualification, compétences, formation
- évaluer les équipes techniques en charge du SI (internes ou externes) : qualifications, compétences, formation, références (autres clients)
- évaluer la communication entre tous les acteurs, c'est-à-dire évaluer la qualité du système d'information qui est toujours le lien entre le système décisionnel et le système opérationnel

4 risques majeurs

- vols de données sensibles : fichiers clients, tarifs, salaires, brevets et licences, données personnelles etc.
- destruction de données ou de matériels
- captation d'informations
- indisponibilité du système

Que doit-on protéger ?

- les serveurs, les postes de travail, fixes et nomades, les smartphones …
- les applications : systèmes d'exploitation, suites bureautiques, logiciels métiers …
- les infrastructures de communication : modes d'accès au réseau de l'entreprise, liaisons intersites, réseau téléphonique, accès Internet, liaisons radio …
- les informations sensibles détenues par l'entreprise : ce sont celles dont la divulgation procurerait un avantage à la concurrence ou réduirait l'avantage dont dispose l'entreprise telles que la R&D, le savoir-faire technologique, la structure financière de l'entreprise, les fichiers clients, prospects, les tarifs produits, …

Mise en place d'une politique de sécurité

1. la gouvernance : pilotage de la politique de sécurité par une unité spéciale, la DSI : Direction des Systèmes d'Information

Il faut :

- s'assurer de formations régulières pour les membres de la DSI
- mettre en place d'une veille technologique à l'aide des outils les plus récents facilitant cette veille : l'objectif est de traquer les bonnes informations, celles relatives à notre contexte
- opérer un recrutement qualitatif, spécifique : faire appel à des spécialistes
- selon le contexte, nommer un DPO (Data Protection Officer, voir RGPD)

Mise en place d'une politique de sécurité

2. les comportements doivent changer ! Voyons comment …

Quel que soit leur niveau hiérarchique et leur niveau d'implication au sein du SI, les collaborateurs / utilisateurs sont au cœur du SI.

Il faut donc :

- les informer : communication entre les 3 systèmes, décisionnel, information et opérationnel
- les responsabiliser : management
- veiller à la fréquence et la qualité de leur formation
- instaurer le partage sur les problèmes techniques et humains rencontrés

Mise en place d'une politique de sécurité

- mettre en place des règles d'utilisation d'Internet : téléchargements, forums …
- sensibiliser en permanence les collaborateurs à la protection des informations sensibles
- engager la responsabilité des collaborateurs : charte d'utilisation annexée au règlement intérieur, mise en place de sanctions
- impliquer fortement la direction
- configurer les postes de travail par un spécialiste
- verrouiller des postes informatiques
- ne pas installer de nouveau logiciel sans autorisation

Mise en place d'une politique de sécurité

- déterminer des droits d'accès différenciés selon les responsabilités des salariés et les statuts des autres personnes pouvant avoir accès au système d'information : stagiaires, personnels temporaires, prestataires extérieurs …
- gérer des codes d'accès et des mots de passe : attribuer des mots de passe suffisamment sécurisés, les renouveler régulièrement, les supprimer lors du départ des collaborateurs

→ qui a le droit de faire quoi ? de savoir quoi ?

Mise en place d'une politique de sécurité

3. la sécurisation des données, les sauvegardes

- les systèmes d'exploitation doivent être mis à jour
- utiliser des logiciels : antivirus, anti-spyware, pare-feu, anti-spam, etc …
- sécurisation des échanges (Internet – Extranet – Wifi – Bluetooth …) par le chiffrement des données les plus sensibles
- pour les données très sensibles, utilisation de matériels non connectés au réseau
- gestion des courriers électroniques
- veille technologique : nouveaux virus, logiciels espions …

Mise en place d'une politique de sécurité

Les sauvegardes

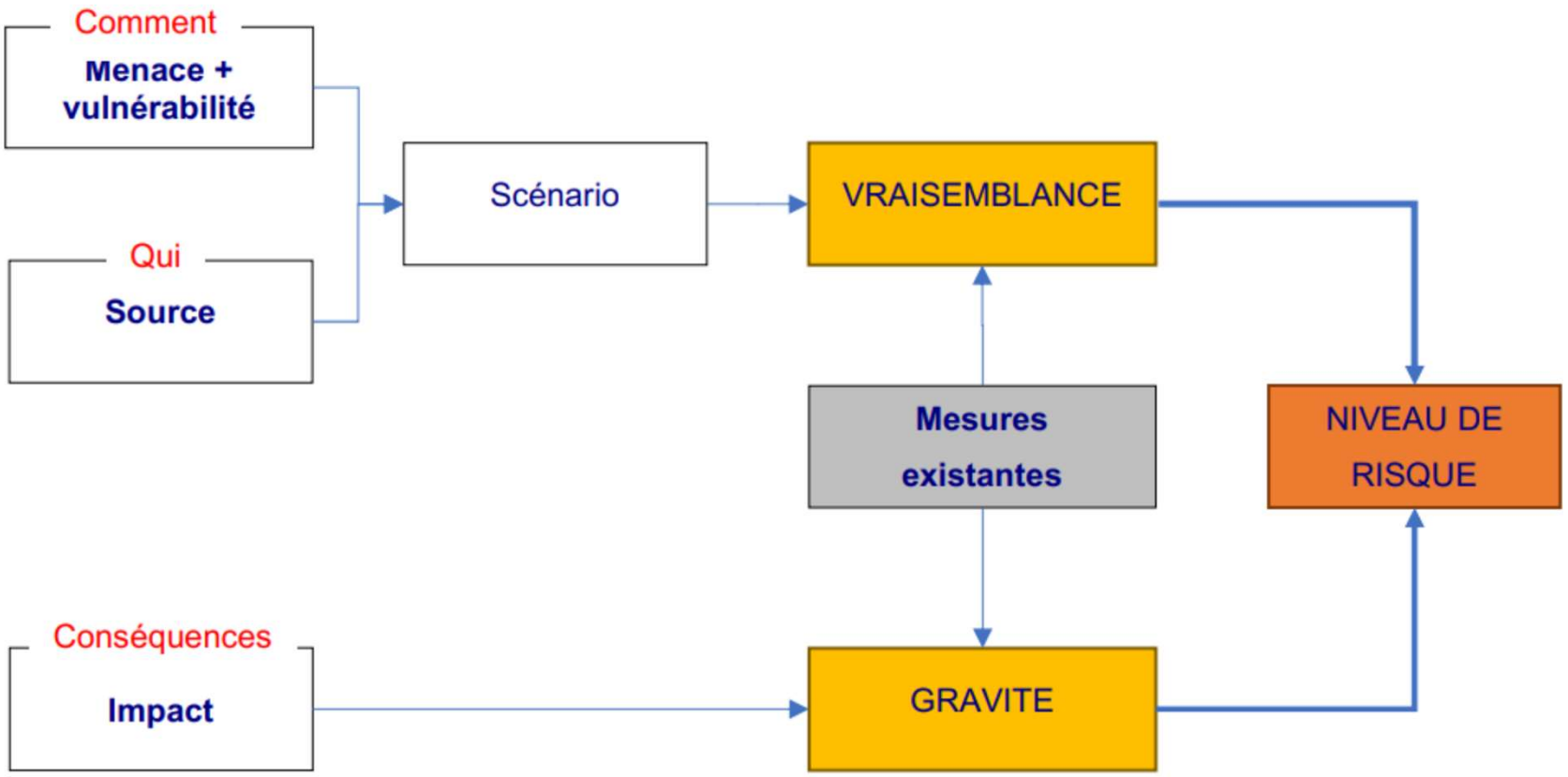
La règle du 3 – 2 – 1

- 3 copies de vos données
- 2 supports différents
- 1 copie hors site

Préconisations

- définir le type de données à sauvegarder, selon quelle périodicité, pour quelle durée (obligations légales de conserver certaines données)
- sécuriser les lieux de stockage des sauvegardes
- contrôler le bon fonctionnement des sauvegardes
- si sous-traitance à un prestataire : s'assurer du cryptage des données sauvegardées chez le prestataire

Détermination du niveau d'exposition au risque



Grilles d ’évaluation des risques

Détermination des risques potentiels

Numérotation du risque	Chemins d'attaques stratégiques	Vraisemblance
R 1	Mail avec fichier infecté en pièce jointe	V 4 - Quasi certain
R 2	Clé USB piégée installée sur un ordinateur	V 1 - Peu vraisemblable
R 3	Installation d'une porte dérobée (backdoor)	V 2 - Vraisemblable
R 4	Piratage du Wifi	V 4 - Quasi certain
R 5	Piratage d'un compte VPN	V 2 - Vraisemblable
R 6	Prise de contrôle des serveurs de fichiers	V 4 - Quasi certain
R 7	Attaque par DoS	V 2 - Vraisemblable
R 8	Phishing pour récupérer des identifiants	V 3 - Très vraisemblable
R 9	Attaque Injection SQL	V 2 - Vraisemblable
R 10	Attaque XSS	V 2 - Vraisemblable
R 11	Attaque par Brute force sur les mots de passe	V 2 - Vraisemblable
R 12	Installation de keyloggers	V 1 - Peu vraisemblable

Grilles d ’évaluation des risques

Niveaux de risque - Acceptabilité - Décisions

Niveau de risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action à entreprendre
Moyen	Tolérable sous contrôle	Suivi à mener - Actions à mettre en place dans le cadre d'une amélioration continue sur le moyen et le long terme
Elevé	Inacceptable	Mesures de réduction du risque à prendre impérativement sur le court terme

Gravité et vraisemblance

Gravité					
4	R 12	R 7	R 8	R 1	
3	R 2	R 3, R 10, R 9, R 11		R 4, R 6	
2		R 5			
1					
	1	2	3	4	**Vraisemblance**

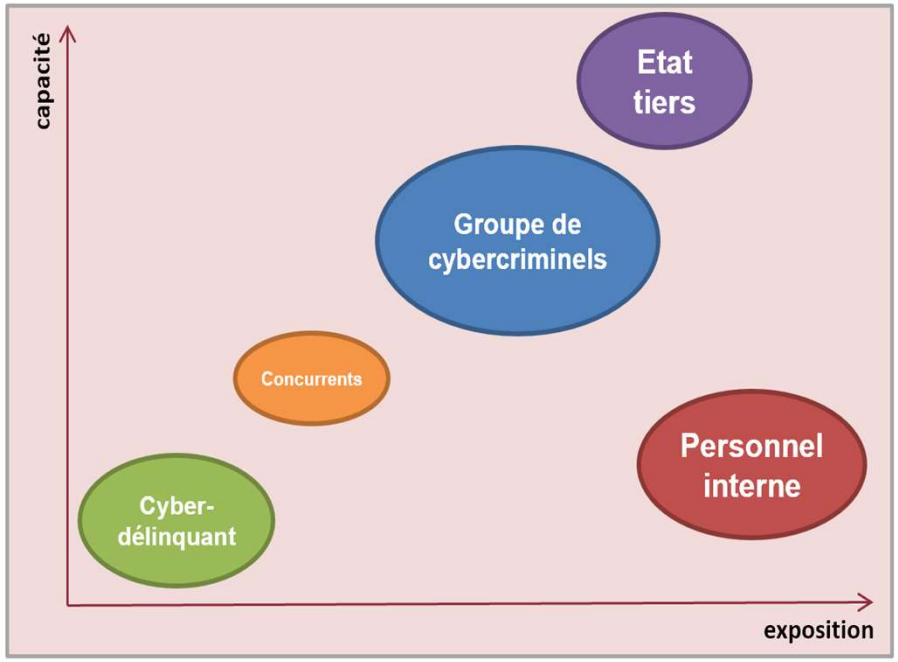
Exemple de synthèse des mesures de sécurité

Mesures de sécurité	Risques associés	Responsables	Freins et difficultés	Coût et complexité	Échéance	Statut
GOUVERNANCE						
Sensibilisation renforcée au phishing	R 1, R 7, R 8, R 9	RSSI	Validation du CHSCT	++	6 mois	A faire
Entraînement aux risques cyber	R 1, R 8, R 9, R 10, R 11, R 12	DSI		+	6 mois	A faire
Audit de sécurité technique et audit organisationnel	R 2, R 4, R 11, R 12	PASSI		+++	9 mois	A faire
Veille technologique	R 6, R 9, R 10, R 11	RSSI	Reflexion sur le mode de diffusion	++	6 mois	En cours
Mise en place de procédures de signalement d'incident	R 6, R 9, R 10, R 11	Equipe juridique		+++	12 mois	En cours
PROTECTION						
Renforcement des droits sur les données partagées	R 6, R 9	RSSI		+	3 mois	En cours
Renforcement des mots de passe (préconisations ANSSI)	R 4, R 5, R 6, R 9, R 10, R 11	RSSI	Utilisateurs	+++	3 mois	En cours
Protection des données (chiffrement, VPN ...)	R 6, R 10, R 11	RSSI, DSI	Revoir l'architecture du SI	++	9 mois	En cours
Renforcement des accès physiques	R 2, R 12	Equipe sécurité		++	3 mois	En cours
Gestion de l'obsolescence	R 6, R 9	RSSI, DSI	Budget	+++	9 mois	A faire
Mise en place d'une politique de sauvegardes	R 1, R 2	Administrateur	Budget	+++	6 mois	A faire
Segmentation des droits des utilisateurs	R 6, R 9, R 10	Administrateur		+	1 mois	Terminé
DEFENSE						
Surveillance renforcée des flux entrants et sortants	R 6, R 9, R 10	RSSI, Administrateur	Achat d'un logiciel	++++	6 mois	A faire
Système de surveillance des équipements sensibles	R 6, R 9	Equipe sécurité	Achat d'un logiciel	++++	6 mois	A faire
RESILIENCE						
Gestion de crise	R 4, R 6, R 7, R 9	RSSI, DSI, Direction		++++	6 mois	A faire
Mise en place d'un plan de continuité des activités (PCA)	R 1, R 2, R7, R 9	RSSI, DSI, Direction	Budget	++++	6 mois	A faire
Mise en place d'un plan de reprise des activités (PRA)	R 1, R 2, R7, R 9	RSSI, DSI, Direction	Budget	++++	6 mois	A faire

RSSI = Responsable Sécurité du Système d'Information
DSI = Direction des Systèmes d'Information
PASSI = Prestataire d'Audit de la Sécurité du Système d'Information

Cartographie des sources de menaces

Il est aussi possible de classer les sources de menaces selon leurs capacités et l'exposition de l'organisation



Exemple d'une cartographie des principales sources de menaces qui pèsent sur un S.I.

Capacité
degré d'expertise et ressources de la source de menaces

Exposition
opportunités et intérêts de la source de menaces

EBIOS

Méthode d'analyse proposée par l'ANSSI

La méthode EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité

- Cette méthode se décompose en 5 ateliers :
  - **ATELIER 1** – CADRAGE ET SOCLE DE SÉCURITÉ
  - **ATELIER 2** – SOURCES DE RISQUE
  - **ATELIER 3** – SCÉNARIOS STRATÉGIQUES
  - **ATELIER 4** – SCÉNARIOS OPÉRATIONNELS
  - **ATELIER 5** – TRAITEMENT DU RISQUE

  - A retrouver sur le site de l'ANSSI

Les enjeux juridiques

Responsabilité de l'entreprise

- elle est responsable de la protection de son SI et met en place des procédures :
  - transparentes et connues de tous
  - qui font l'objet d'une discussion collective
  - précises et mesurées, notamment celles qui concernent les messages privés

Les enjeux juridiques

Responsabilité de l'entreprise

- elle est responsable de la protection de son SI et met en place des procédures :
  - transparentes et connues de tous
  - qui font l'objet d'une discussion collective
  - précises et mesurées, notamment celles qui concernent les messages privés

Les enjeux juridiques

Il y a des risques de mise en cause civile ou pénale de l'entreprise induite par le comportement des salariés, par exemple :

- l'utilisation malveillante des moyens informatiques et de communications électroniques (messagerie, forums), contenus diffamatoires à l'égard de tiers
- le téléchargement de documents ouvrant droit à des poursuites pénales : pédophilie, incitation à la haine, incitation au racisme …
- la contrefaçon : utilisation de copies illicites de logiciels ou d'œuvres protégées sans autorisation des ayants droits, reproductions physiques interdites (imprimantes 3D)
- le non respect du secret des correspondances privées

Les enjeux juridiques

- en cas de défaut de protection de son SI, la responsabilité de l'entreprise peut également être engagée :
  - par ses partenaires extérieurs : atteinte à leur système d'information, non respect des engagements de confidentialité
  - par ses actionnaires et ses salariés : mise en cause du dirigeant pour faute de gestion

Les enjeux juridiques

- la responsabilité du chef d'entreprise peut aussi être mise en cause en cas de non respect des procédures de mise en place d'un processus de cyber surveillance des salariés
- l'entreprise est soumise à l'obligation de veiller à l'intégrité, la confidentialité, la disponibilité, et la traçabilité de ses informations → RGPD
- elle doit mettre en place les moyens adaptés, techniques et organisationnels
- détection des vulnérabilités et anomalies le plus en amont possible

Gestion des incidents

Prévoir des solutions de secours en cas d'indisponibilité du système informatique :

- assistance
- dépannage
- mise à disposition de matériel de secours
- PCA = plan de continuité des activités
- PRA = plan de reprise des activités

Quelques instances à contacter

- En France, voici quelques instances en charge de la cybersécurité et de la cybercriminalité :
  - la DGSI : Direction Générale de la Sécurité Intérieure (https://www.dgsi.interieur.gouv.fr)
  - l'OCLCTIC : Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication (https://www.police-nationale.interieur.gouv.fr/Archives/Archivage-articles-Police-Nationale/Plateforme-Signalement-sur-Internet)
  - la CNIL : Commission Nationale de l'Informatique et des Libertés (https://www.cnil.fr)