La gestion du risque

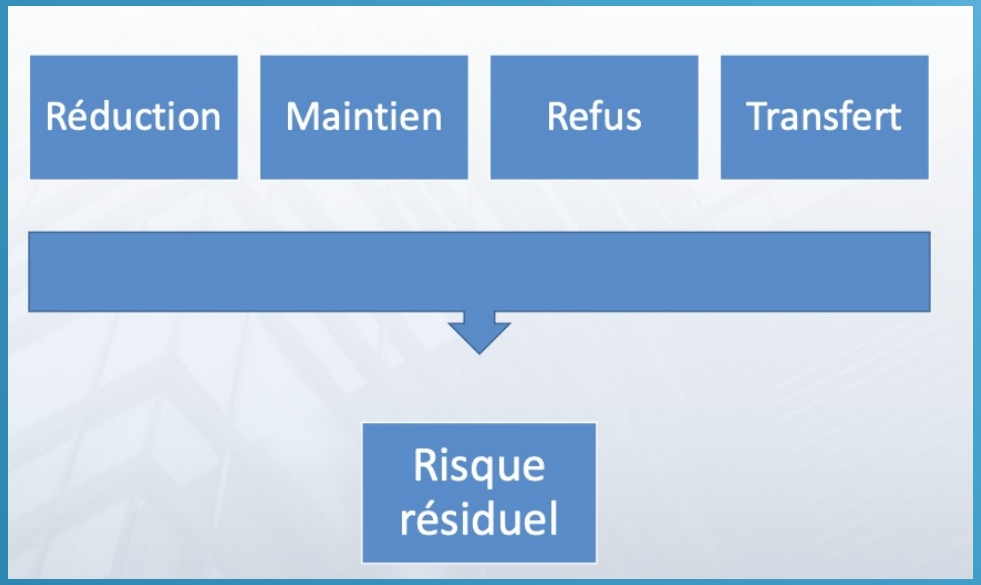
ANDN SERVICES

Définition du risque

- Un risque est la vraisemblance qu'une menace exploite une vulnérabilité afin d'impacter un actif.
- RISQUE = MENACE x VULNERABILITES x VRAISEMBLANCE x IMPACT
- Un risque se formule sous forme de scénario afin qu'il soit compréhensible du management.
- L'exécution du scénario de risque amène à une conséquence pour le propriétaire de l'actif.

Traitement du risque

- Il y a quatre options de traitement de risque



ANDN SERVICES

Risque résiduel

- Un risque résiduel est un risque qui persiste après un traitement du risque.
- S'il n'est pas acceptable, vous devez repartir dans un cycle d'évaluation et de traitement jusqu'à ce que le niveau de ce risque devienne acceptable.

Risque induit

- Un risque induit est un risque introduit suite à la mise en œuvre d'une mesure de sécurité

Espérance de perte unique

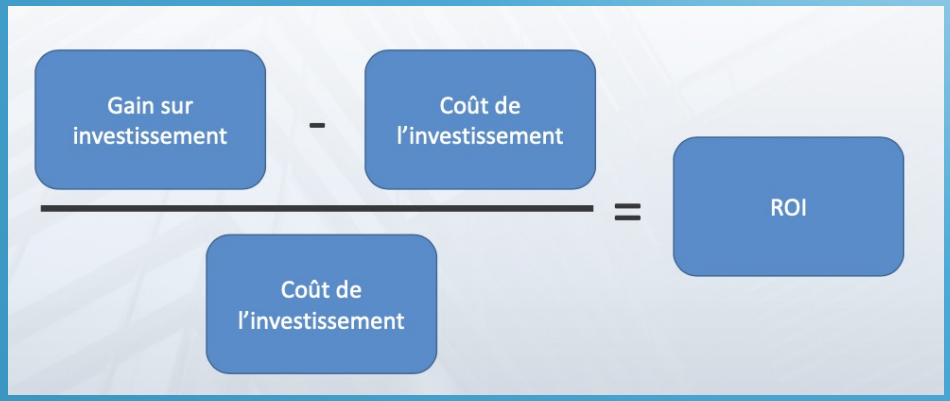
- Espérance de Perte Unique (EPU) : Correspond à une perte suite à un évènement unitaire
- La Valeur de l'Actif (VA) x Facteur d'Exposition (FE) = Espérance de Perte Unique (EPU)
- Exemple : 60% du chiffre d'affaire journalier est impacté en cas d'attaque sur les services web e-commerce de l'entreprise.
  - La valeur du chiffre d'affaire journalier est de 100 000 €
  - 60% correspond au Facteur d'Exposition
  - Chiffre d'affaire journalier x Facteur d'Exposition = 100 000 € x 0,6 = 60 000 €
  - Espérance de Perte Unique = 60 000 €
- Terme anglophone : Single Loss Expectancy (SLE)

Espérance de perte annuelle

- Espérance de Perte Annuelle (EPA) : Correspond à la perte sur un an
- Espérance de Perte Unique (EPU) x Taux d'Occurrence Annuel (TOA) = Espérance de Perte Annuelle (EPA)
- Exemple : 60% du chiffre d'affaire journalier est impacté en cas d'attaque sur les services web e-commerce de l'entreprise. L' évènement se produit 1 journée par trimestre.
  - Chiffre d'affaire journalier = 100 000 €
  - Espérance de Perte Unique = 60 000 €
  - Taux d'Occurrence Annuel : 4
  - Espérance de Perte Unique x Taux d'Occurrence Annuel = 60 000 € x 4 = **240 000 €**
  - Espérance de Perte Annuelle = **240 000 €**
- Terme anglophone : Annualized Loss Expectancy (ALE)

Return of investment (ROI)

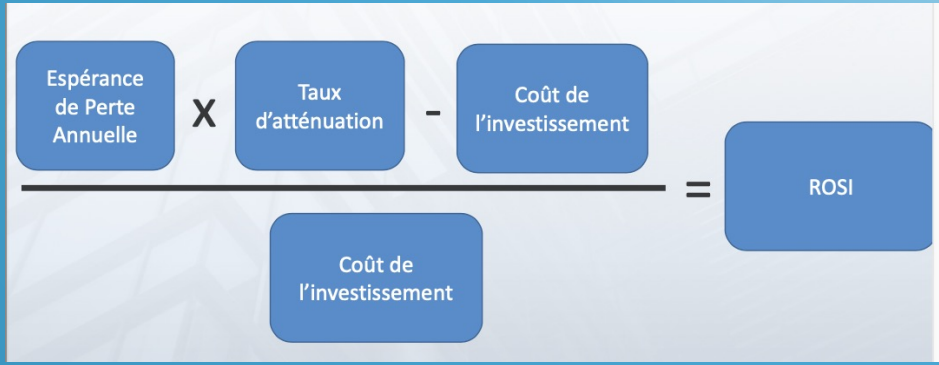
- Retour sur investissement
- Terme Anglophone: Return Of Investment (ROI)



ANDN SERVICES

Return of security investment (ROSI)

- Retour sur l'investissement sécurité
- Taux d'atténuation: Capacité de la solution à atténuer la perte annuelle
- Terme Anglophone: Return Of Security Investment (ROSI)



ANDN SERVICES

Return of security investment (ROSI)

- Hypothèse: Scénario solution Anti-DDOS
- 1 incident par mois
- Espérance de Perte Unique (EPU) = 20 000€
- Taux d'Atténuation (TA): La solution sélectionnée bloque 80% des attaques DDOS
- Le coût de la solution est de 50 000€ par an

Return of security investment (ROSI)

- ROSI = ((Espérance de Perte Annuel x Taux d'atténuation) – Coût de l'investissement)/ Coût de l'investissement
- ROSI = (((Espérance de Perte Unique x Taux d'Occurrence Annuel) x Taux d'atténuation) – Coût de l'investissement) / Coût de l'investissement
- ROSI = ((20 000 € x 12) x 0,8) – 50 000 €) / 50 000 € = 2,84%
- L'investissement réalisé est de 50 000 € et permet d'économiser142 000 € par an.
- On ne parle pas de gain mais d'économie réalisée

Return of security investment (ROSI)

- Exemple: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment