

# **Sécurité des Technologies Internet**

## **Chapitre 2. Développement sécurisé**

Abraham Rubinstein

[abraham.rubinstein@heig-vd.ch](mailto:abraham.rubinstein@heig-vd.ch)

Septembre 2019 - Février 2020

# Aperçu

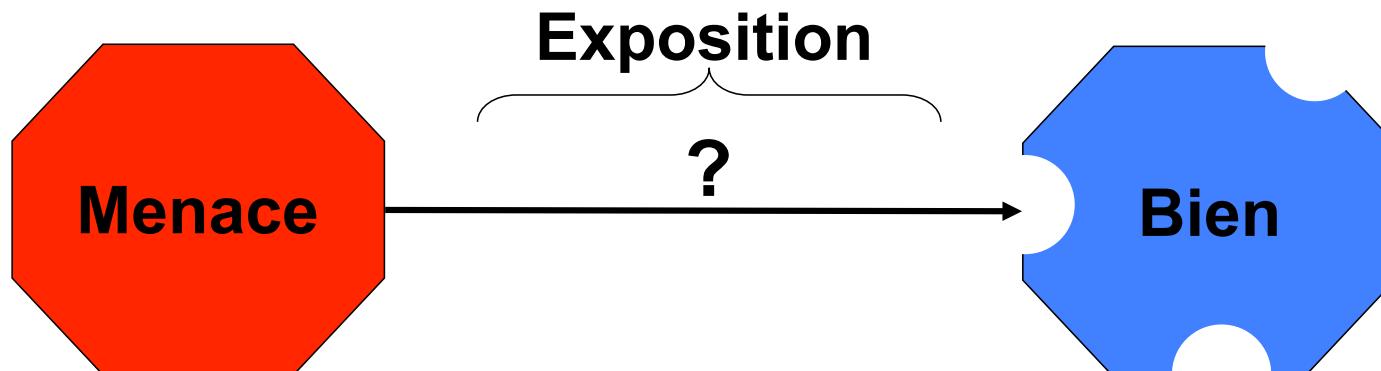
- 1 Introduction à la gestion des menaces/risques
- 2 Menaces des applications Web
- 3 Modélisation de menaces

# Aperçu

- 1 **Introduction à la gestion des menaces/risques**
- 2 Menaces des applications Web
- 3 Modélisation de menaces

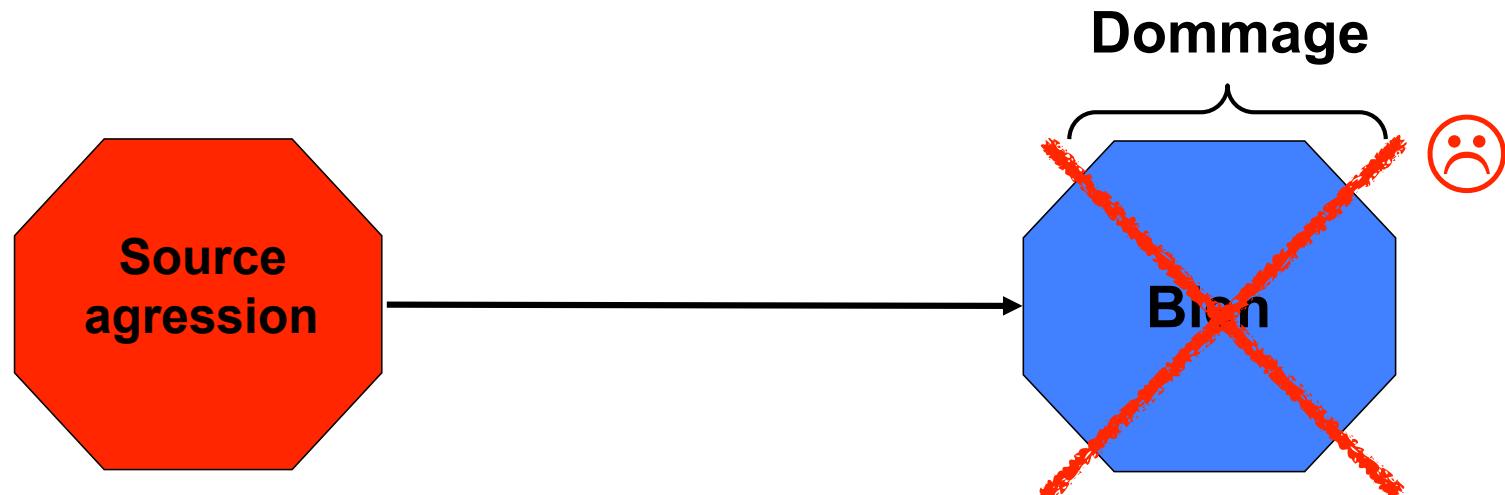
# Bien, vulnérabilités et menaces

- Un **bien** est une chose que l'on cherche à protéger.
- Un bien comporte (très probablement) des **vulnérabilités**.
- Une **menace** cherche à porter préjudice au bien.
- Le bien est donc **exposé** à des menaces (**exposition**).



# Risques et dommages

- Un **risque** exprime le fait qu'une menace puisse **exploiter** une vulnérabilité d'un bien en causant des **dommages** [27005].
- Le **risque** permet de **quantifier les chances** que les dommages surviennent (par rapport à cette menace).



# Conséquences d'un dommage

- Les **conséquences** sont évaluées en termes de :
  - (C) perte de confidentialité (et/ou)
  - (I) perte d'intégrité (et/ou)
  - (D) perte de disponibilité de l'information.
- Conséquences **directes** ~ conséquences **techniques**
  - typiquement perte de données, fuites, ...
- Conséquences **indirectes** ~ conséquences **business**
  - typiquement perte financière, perte d'image de marque, ...

# Vocabulaire

- **Bien, actif (asset)**
  - Quelque chose qui a de la valeur (aux yeux de la source de menace)
- Exemples :
  - argent, machine, objet, savoir, savoir faire, outil, ...
  - données privées, clés cryptographiques, droits, credentials, ...

# Vocabulaire

- **Menace (source)**
  - Quelque chose capable d'effectuer une action non-désirée ou non-autorisée contre un système
  - Une menace nécessite des ressources, compétences et des accès
- Exemples :
  - Evénements naturels :      inondation, séisme
  - Evénements physiques :      accident, poussière, corrosion, chaleur/feu
  - Pannes :                        air conditionnée, alimentation, télécommunications
  - Perturbations :                émissions électromagnétiques, lumière
  - Pannes techniques :         bug, saturation, malfonction
  - Menace humaine :
    - Mauvaises utilisations, distractions, erreurs
    - Hackers, cybercriminels, terroristes, insiders
    - espionnage industriel et étatique

# Vocabulaire

- **Impact**

- Modification de l'état de la cible
- Exemples :
  - Réputation, argent, savoir, savoir-faire
  - Perturbation de l'activité, fuite d'informations stratégiques
  - Mise en danger d'autrui
  - Destruction

# Vocabulaire

- **Scénario de menace**
  - *séquence d'évènements qui modifie un système*
- Exemples :
  - La source de menace a utilisé une cagoule et des gants pour être anonyme, puis un bulldozer pour entrer dans la banque, puis du scotch pour immobiliser le personnel, puis un chalumeau pour ouvrir le coffre, puis un hélicoptère pour s'enfuir.
  - La source de menace a utilisé une XSS pour piéger un utilisateur, puis une SQL injection pour éléver ses privilèges, ...

# Vocabulaire

- **Vulnérabilité**
  - Attribut d'un bien permettant d'exécuter un scénario non désiré.
- Exemples :
  - Le papier est vulnérable au feu et aux fuites d'informations
  - Un serveur est vulnérable aux inondations.
  - N'importe quel mot de passe ultra-sécurisé est vulnérable à un pistolet pointé sur la tempe du propriétaire

# Vocabulaire

- **Risque**
  - Potentialité qu'une menace exploite une fonctionnalité pour porter préjudice à un bien
  - Un risque nécessite :
    - une menace, un bien, une potentialité et un impact
    - Risque = potentialité x impact
- Exemples :
  - L'impact d'une inondation est de CHF100'000.-. La probabilité est de 1% sur la période concernée. Le risque est de CHF 1'000.-

# Risque...

- Est-ce que le chat est une source de menace ?
- Est-ce que l'oiseau est vulnérable ?
- Quel serait le scénario non-désiré ?
- Quel serait l'impact ?
- L'oiseau est-il actuellement à risque ?



# Risk analysis vs. threat analysis

## Threat analysis:

« The examination of threat-sources against system vulnerabilities to **determine the threats for a particular system** in a particular environment. »

## Risk analysis:

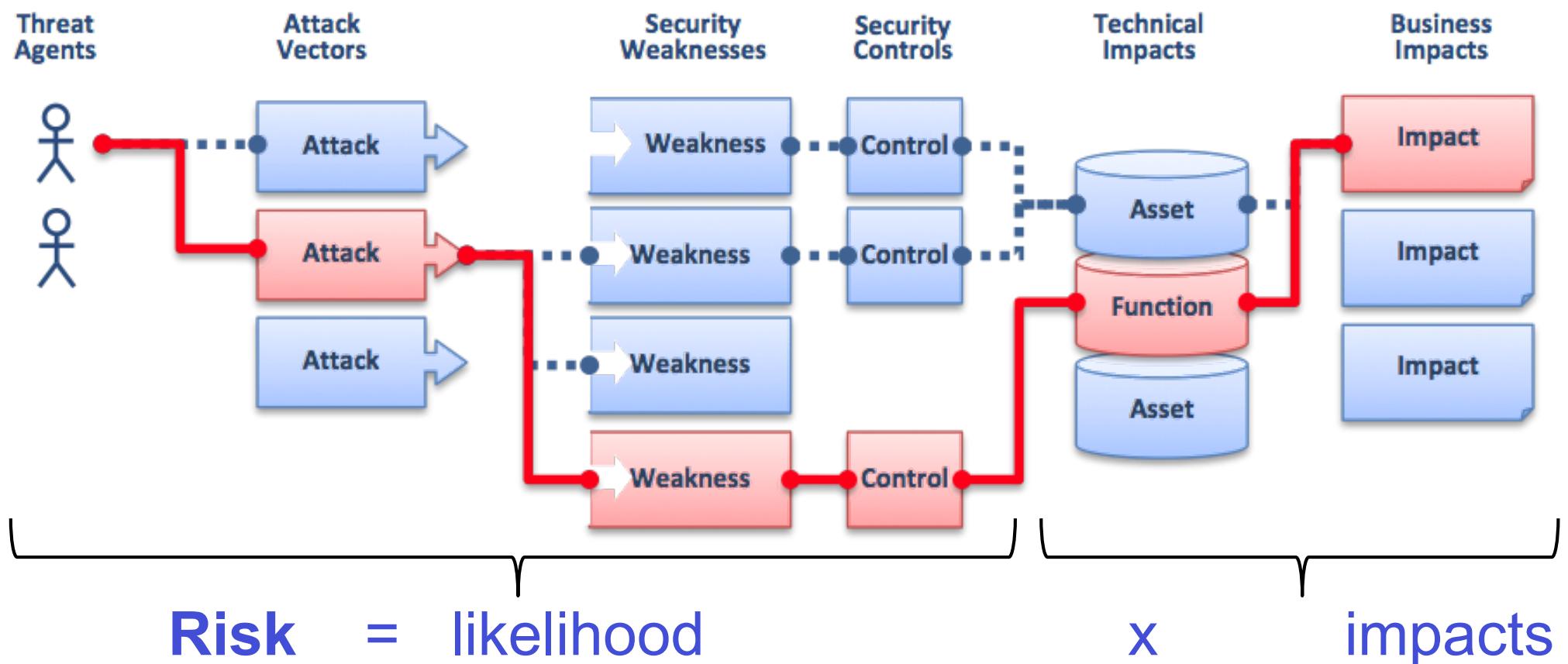
« The identification of risks to a system's security and **determination of the probability of occurrence**, the resulting impact and additional safeguards that would mitigate this impact. » (*NIST SP-500-30*)

# Information Security Risk Management

## Outils et méthodes disponibles

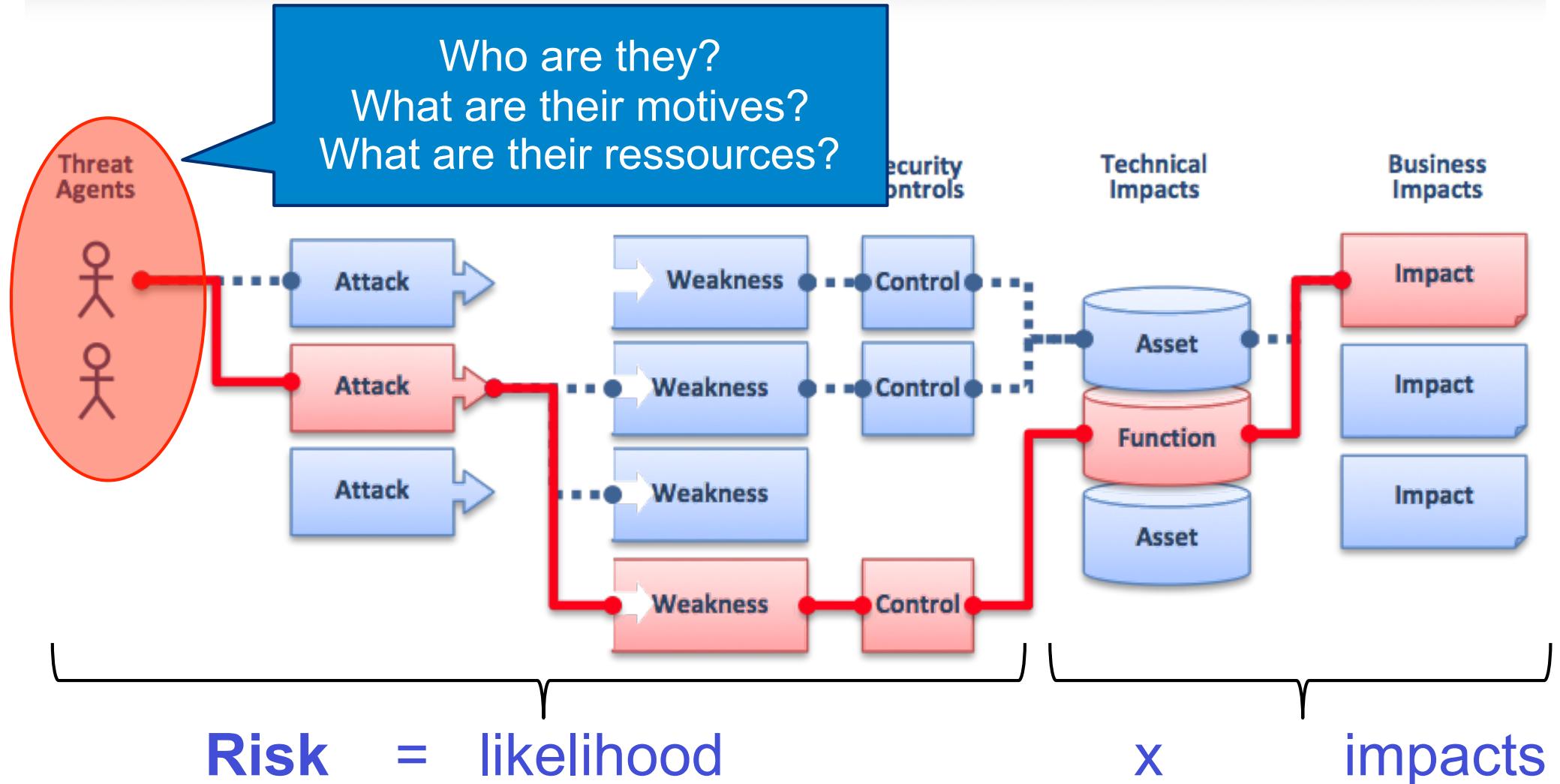
- ISO/IEC 27005: Information security risk management (commercial ressource)  
[http://www.iso.org/iso/catalogue\\_detail?csnumber=56742](http://www.iso.org/iso/catalogue_detail?csnumber=56742)
- NIST SP-800-30: Risk management guide for information security systems  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- OWASP Risk Rating methodology  
[https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)

# OWASP Risk rating methodology



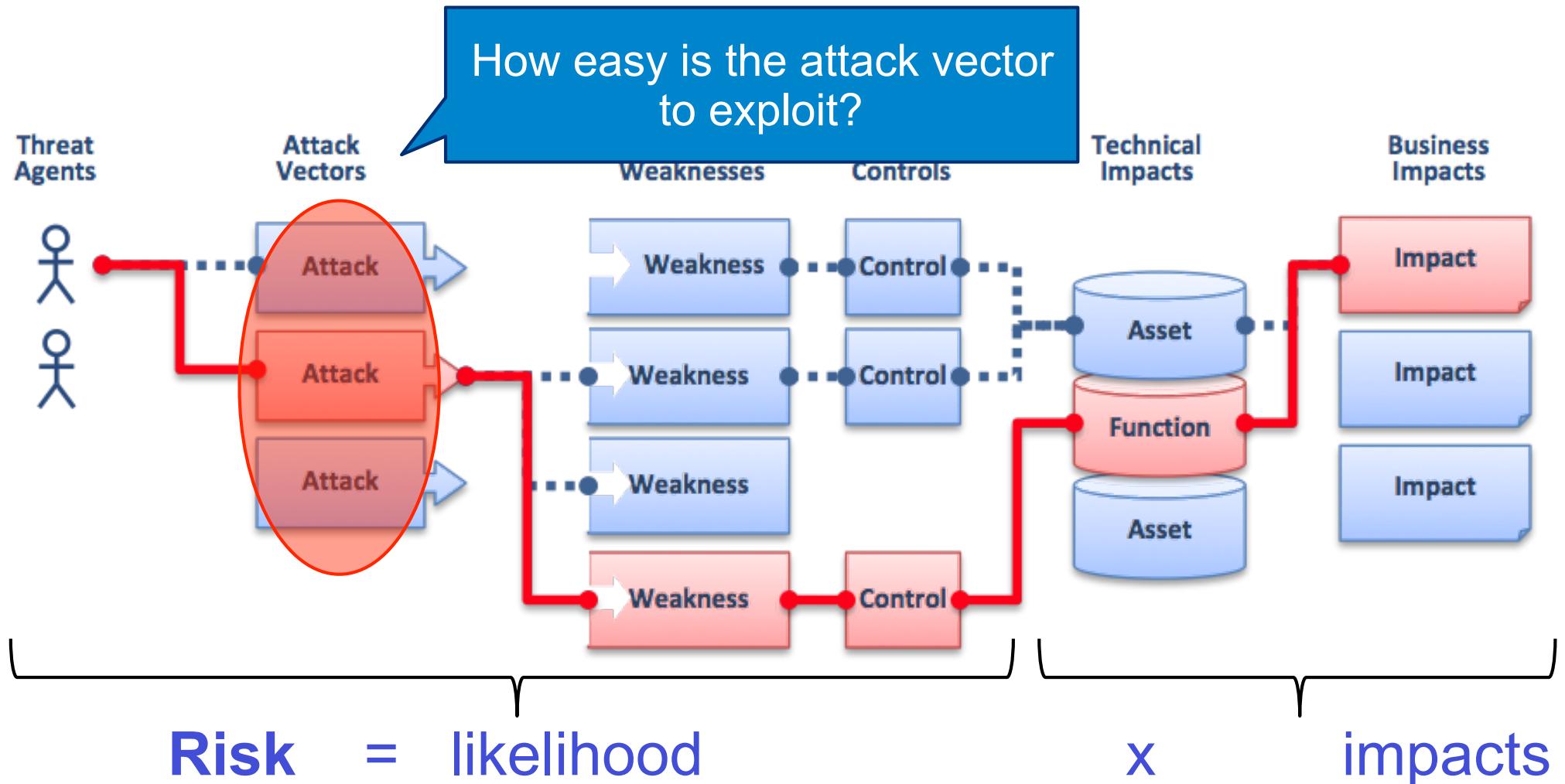
source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



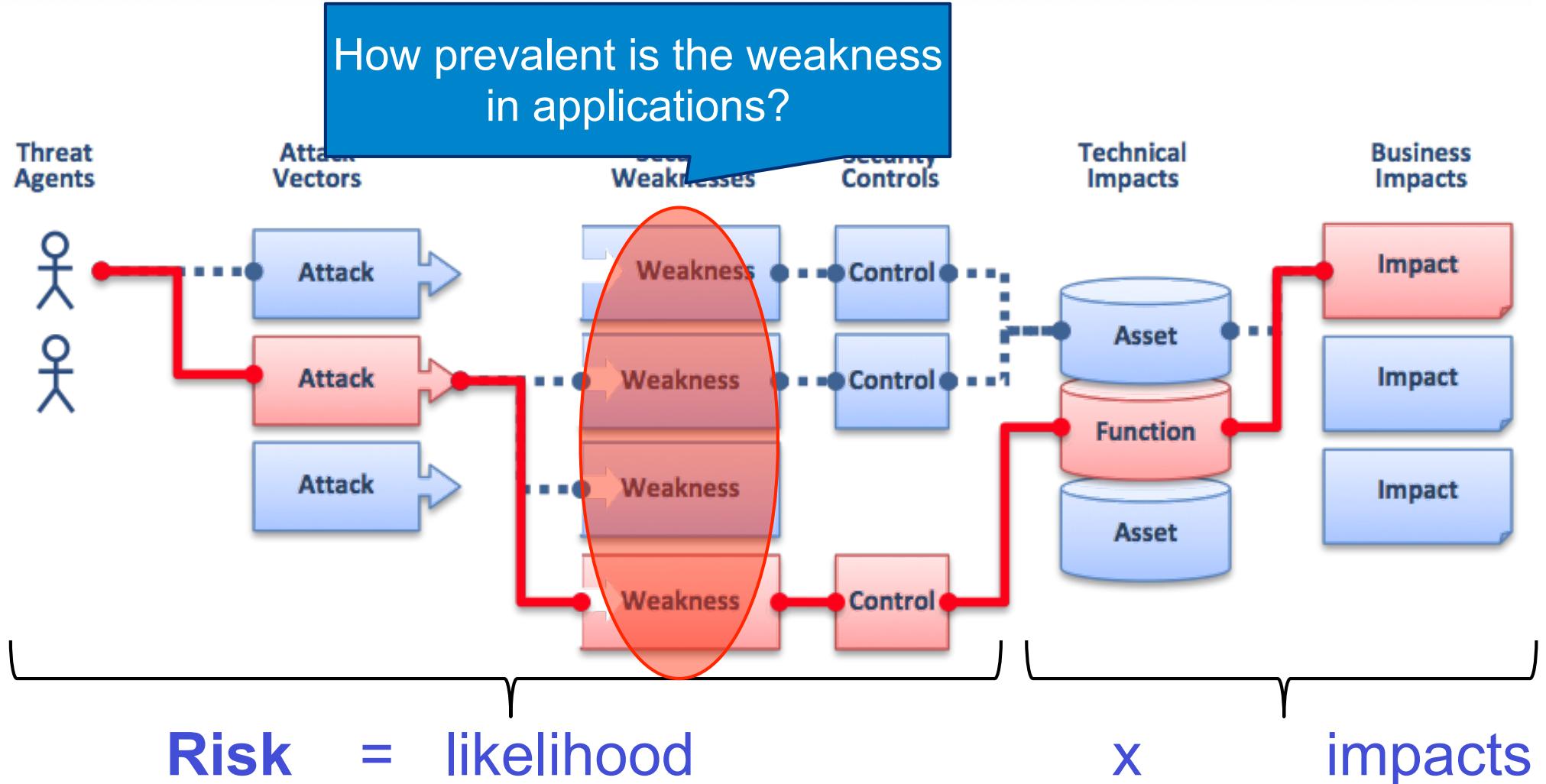
source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



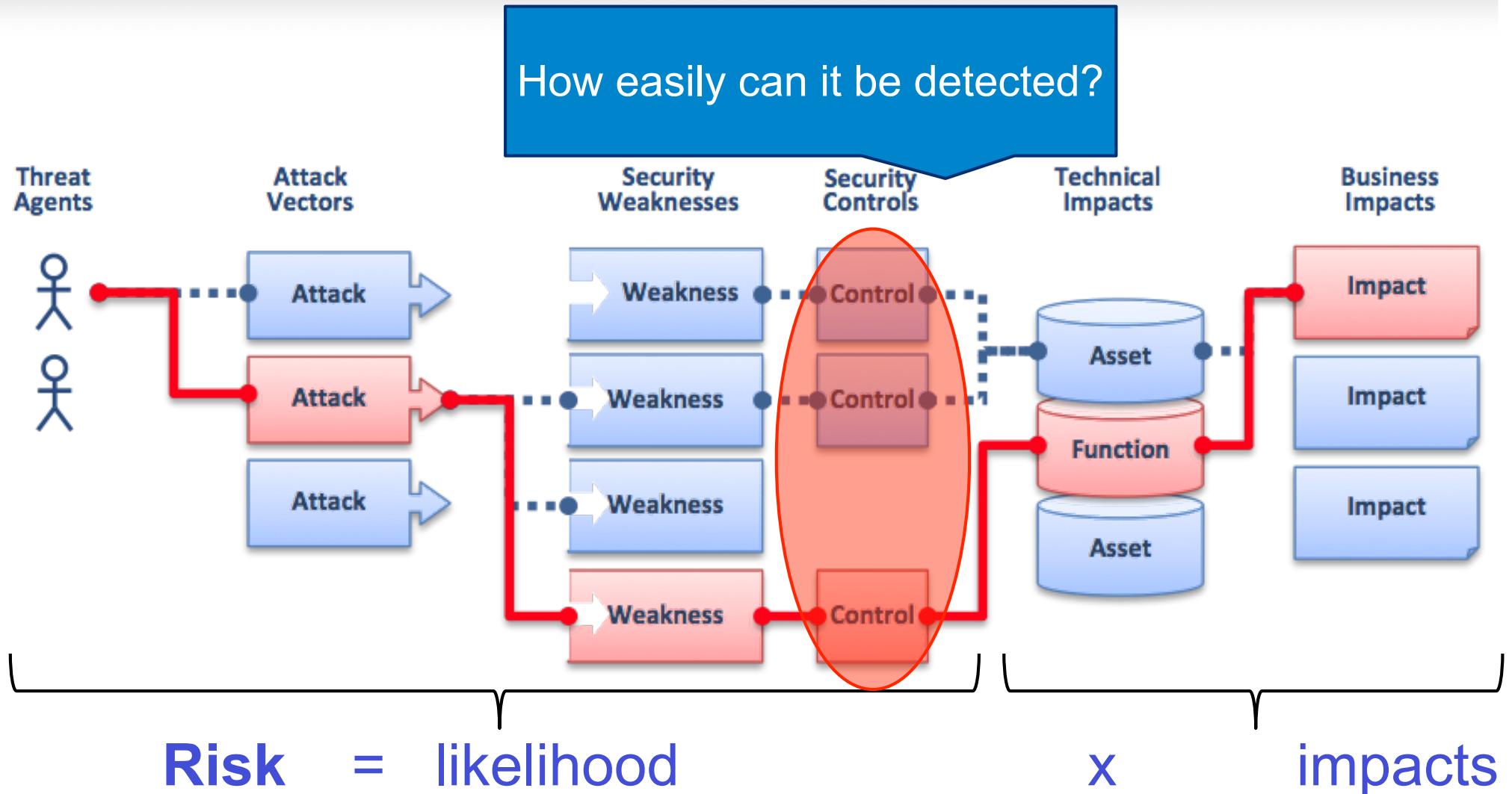
source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



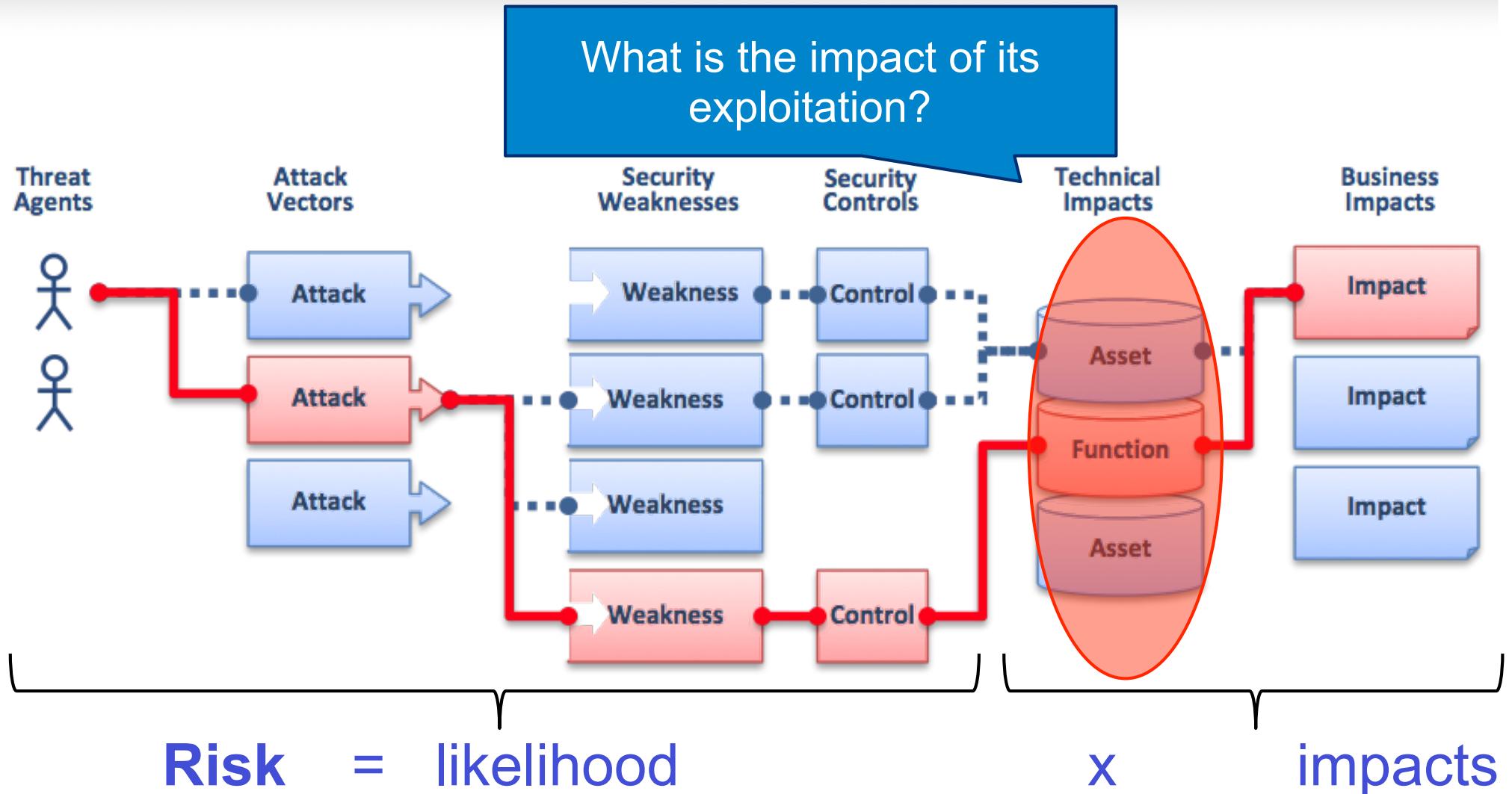
source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



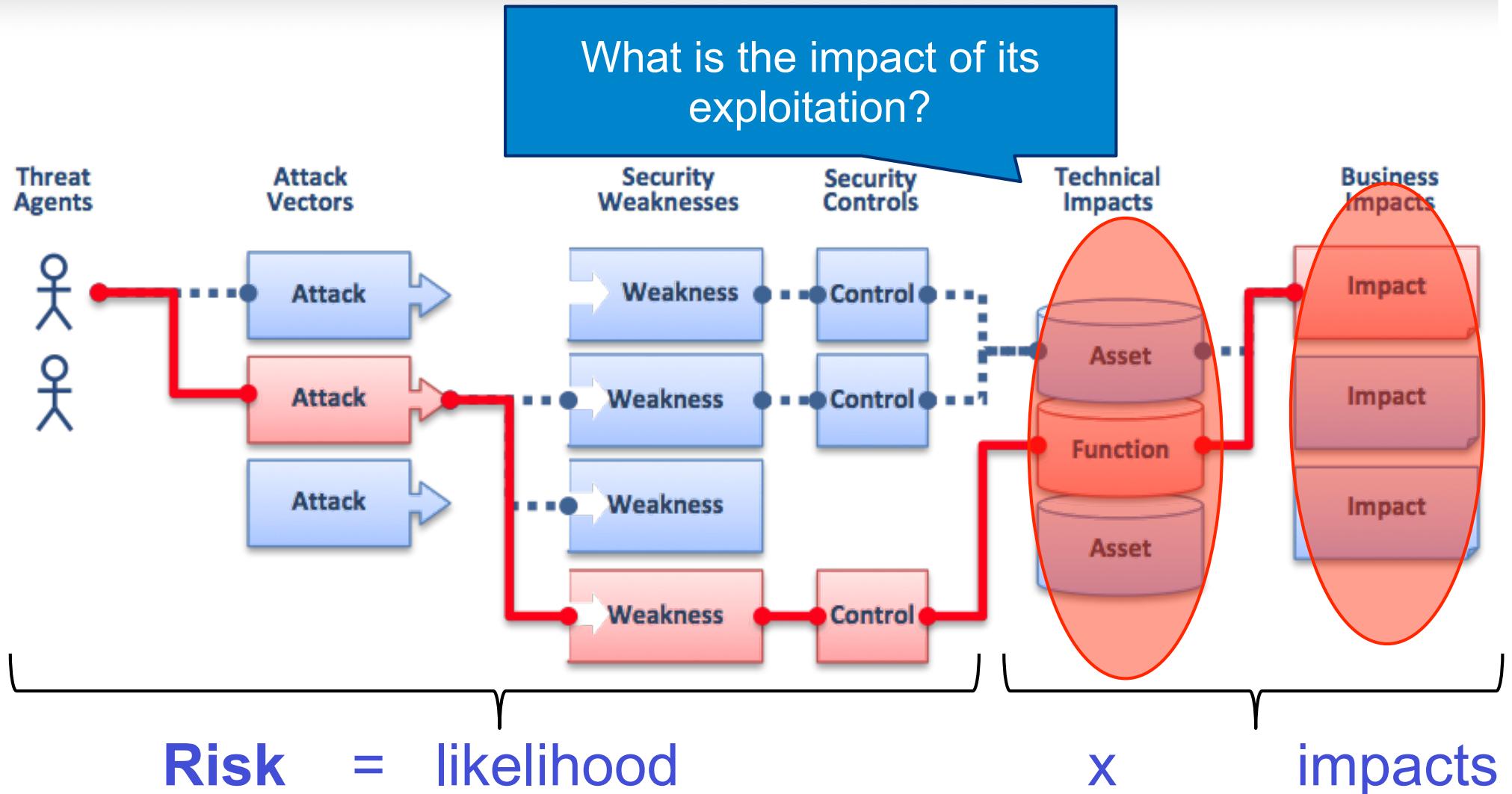
source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



source: [http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

# OWASP Risk rating methodology



# OWASP Risk Rating Methodology

This Risk Rating Calculator is based on [OWASP's Risk Rating Methodology](#). We hope you find it useful.

Description :

Likelihood factors	Impact factors																			
<i>Threat Agent Factors</i>	<i>Technical Impact Factors</i>																			
Skills required	Select an option																			
Motive	Select an option																			
Opportunity	Select an option																			
Population Size	Select an option																			
<i>Vulnerability Factors</i>	<i>Business Impact Factors</i>																			
Easy of Discovery	Select an option																			
Ease of Exploit	Select an option																			
Awareness	Select an option																			
Intrusion Detection	Select an option																			
All factors require a selection.																				
<input type="button" value="Calculate"/>	<input type="button" value="Calculate"/>																			
Overall Risk Severity : <i>Note</i>																				
<table border="1"><thead><tr><th>Likelihood</th><th colspan="3">Impact</th></tr><tr><th>-&gt; Low</th><th>-&gt; Note &lt;-</th><th>Low</th><th>Medium</th></tr></thead><tbody><tr><td>-&gt; Low</td><td>-&gt; Note &lt;-</td><td>Low</td><td>Medium</td></tr><tr><td>Medium</td><td>Low</td><td>Medium</td><td>High</td></tr><tr><td>High</td><td>Medium</td><td>High</td><td>Critical</td></tr></tbody></table>	Likelihood	Impact			-> Low	-> Note <-	Low	Medium	-> Low	-> Note <-	Low	Medium	Medium	Low	Medium	High	High	Medium	High	Critical
Likelihood	Impact																			
-> Low	-> Note <-	Low	Medium																	
-> Low	-> Note <-	Low	Medium																	
Medium	Low	Medium	High																	
High	Medium	High	Critical																	
Copy/paste <b>THIS URL</b> (<CTRL>+D) and all factors are selected as the current settings. This might save you time for future use.																				
Delicious <a href="#">Bookmark this page on Delicious</a>																				
Feedback is welcome. Let us know at <a href="mailto:info@paradoslabs.nl">info@paradoslabs.nl</a> .																				

- Resources:
  - [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)
  - <https://www.security-net.biz/files/owaspriskcalc.html>

# Aperçu

- 1 Introduction à la gestion des menaces/risques
- 2 **Menaces des applications Web**
- 3 Modélisation de menaces

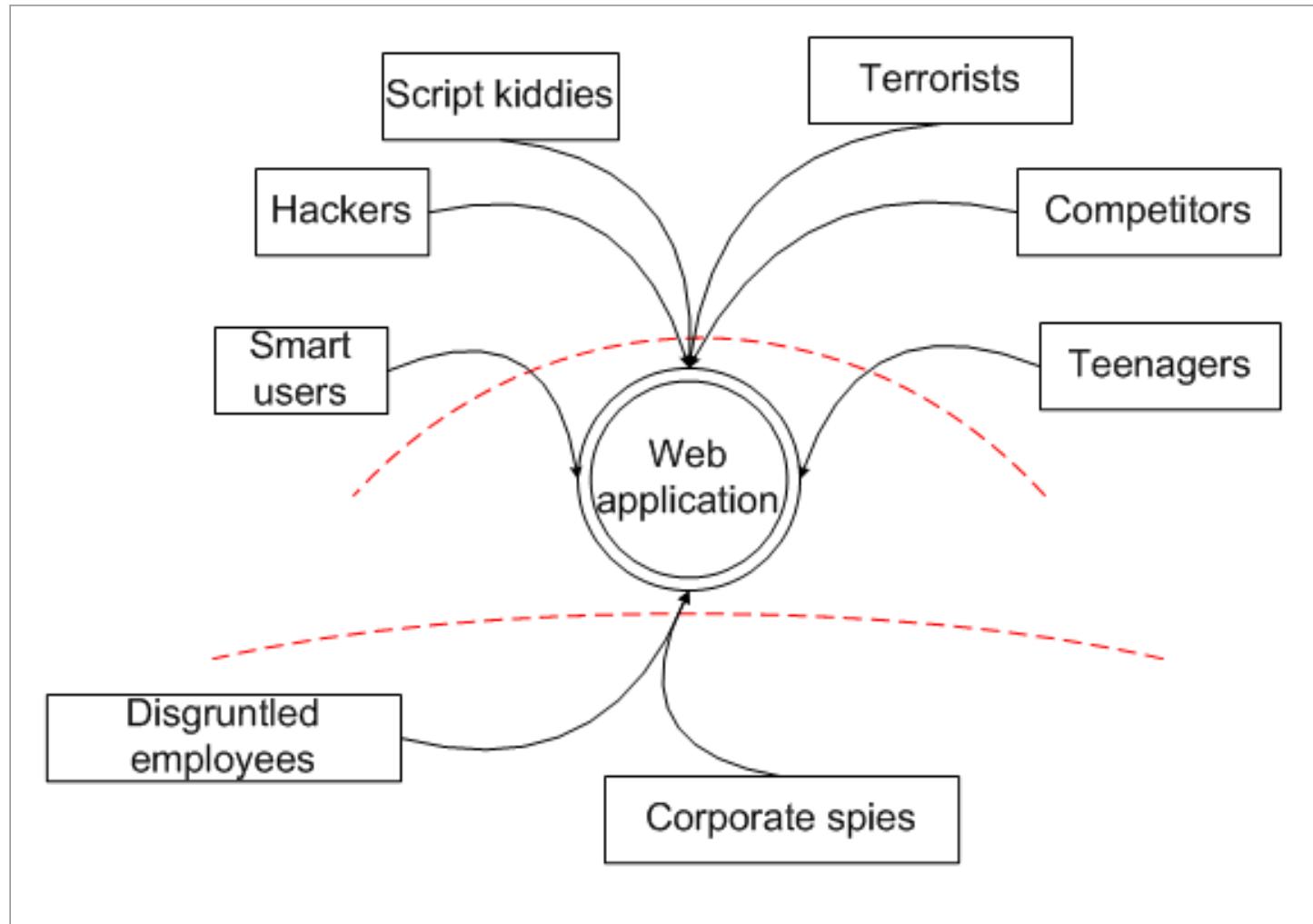
# Trois risques majeurs

- Perte de **confidentialité**
  - Données sensibles
  - Jetons financiers
  - Secrets politiques / gouvernementaux / industriels
- Perte d'**intégrité** (service, information)
  - Infection par un cheval de Troie (Client-side ou server-side)
  - Intrusion dans un système de transactions
  - Corruption de la traçabilité (logs)
- Perte de **disponibilité** (service, information)
  - DoS (résultat d'un problème d'implémentation/configuration)
  - DDoS (pas au niveau de l'application Web)

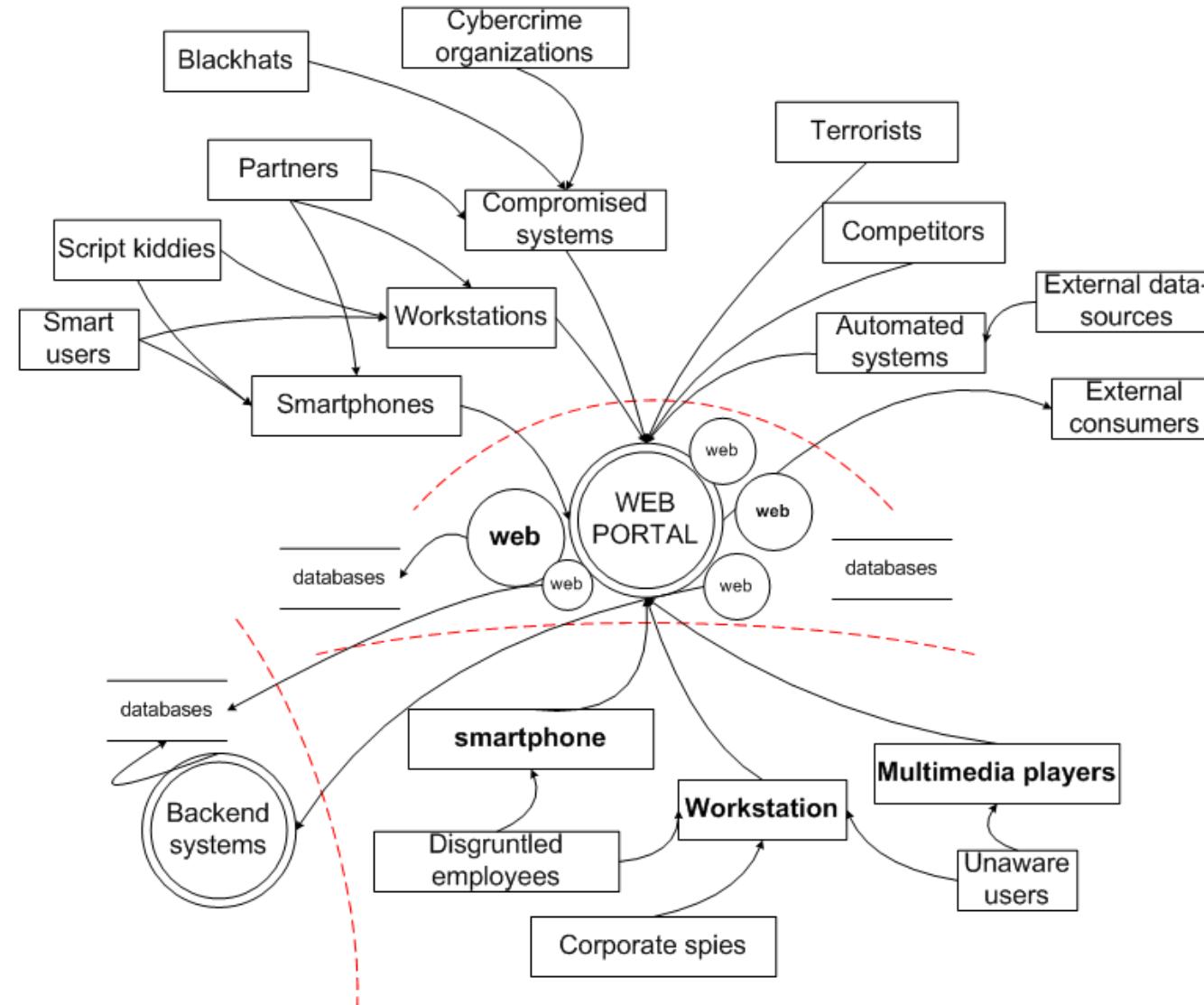
# La jungle !!!

- Sources de menaces variées
- Chemins d'attaques variés
- Compétences variées
- Motivations variées

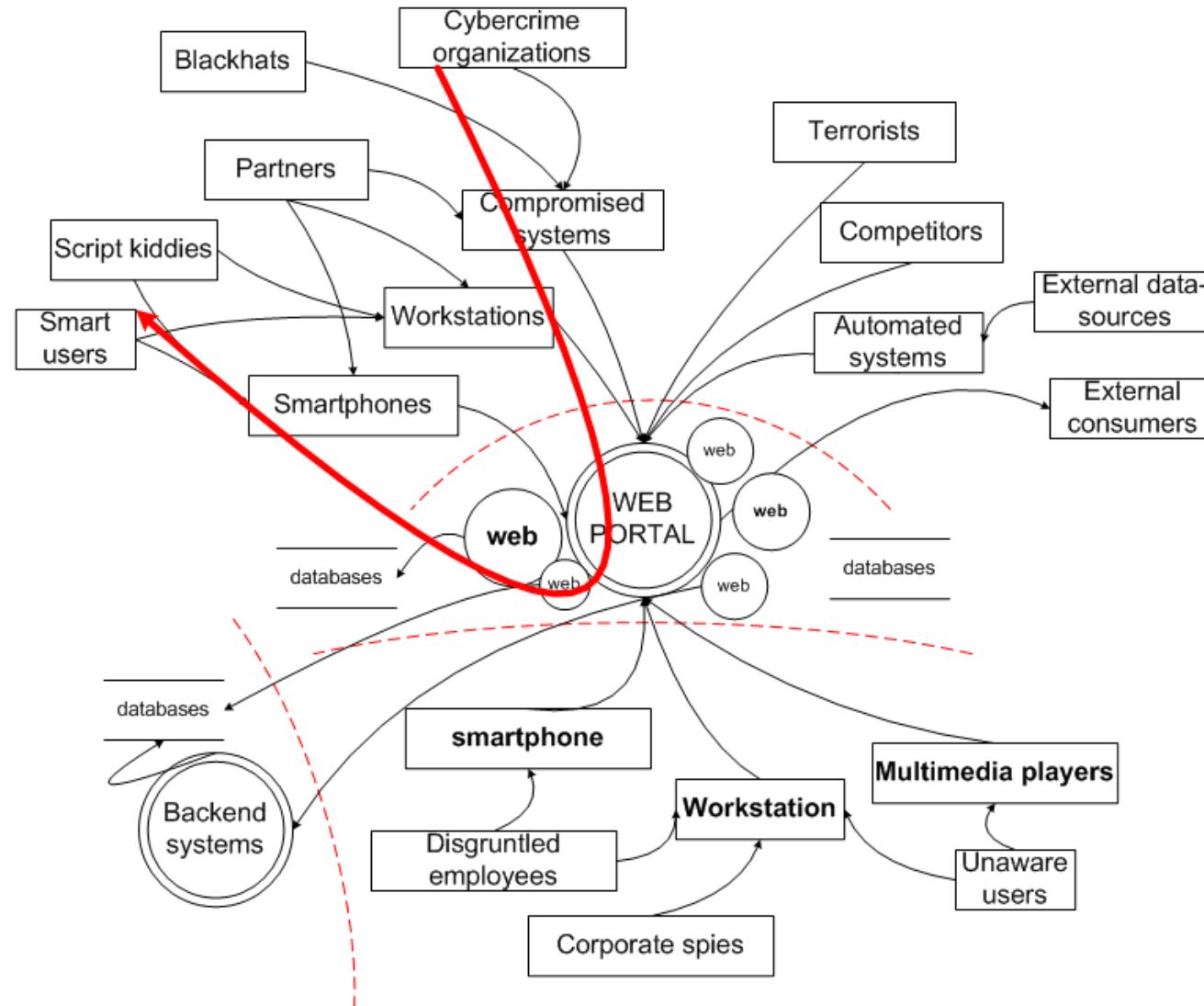
# Sources de menaces variées



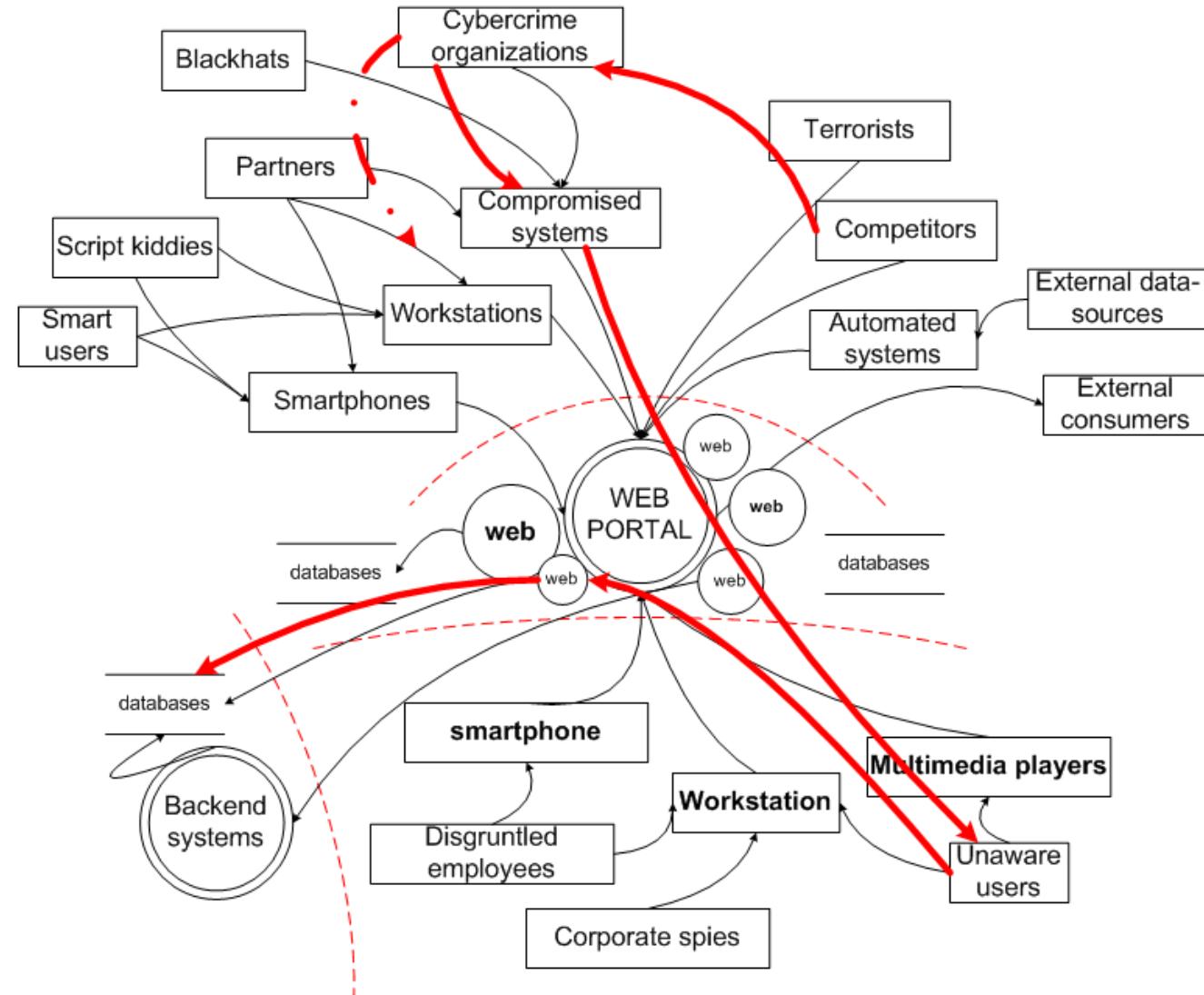
# Chemins d'attaques variés



# Chemins d'attaques variés



# Chemins d'attaques variés



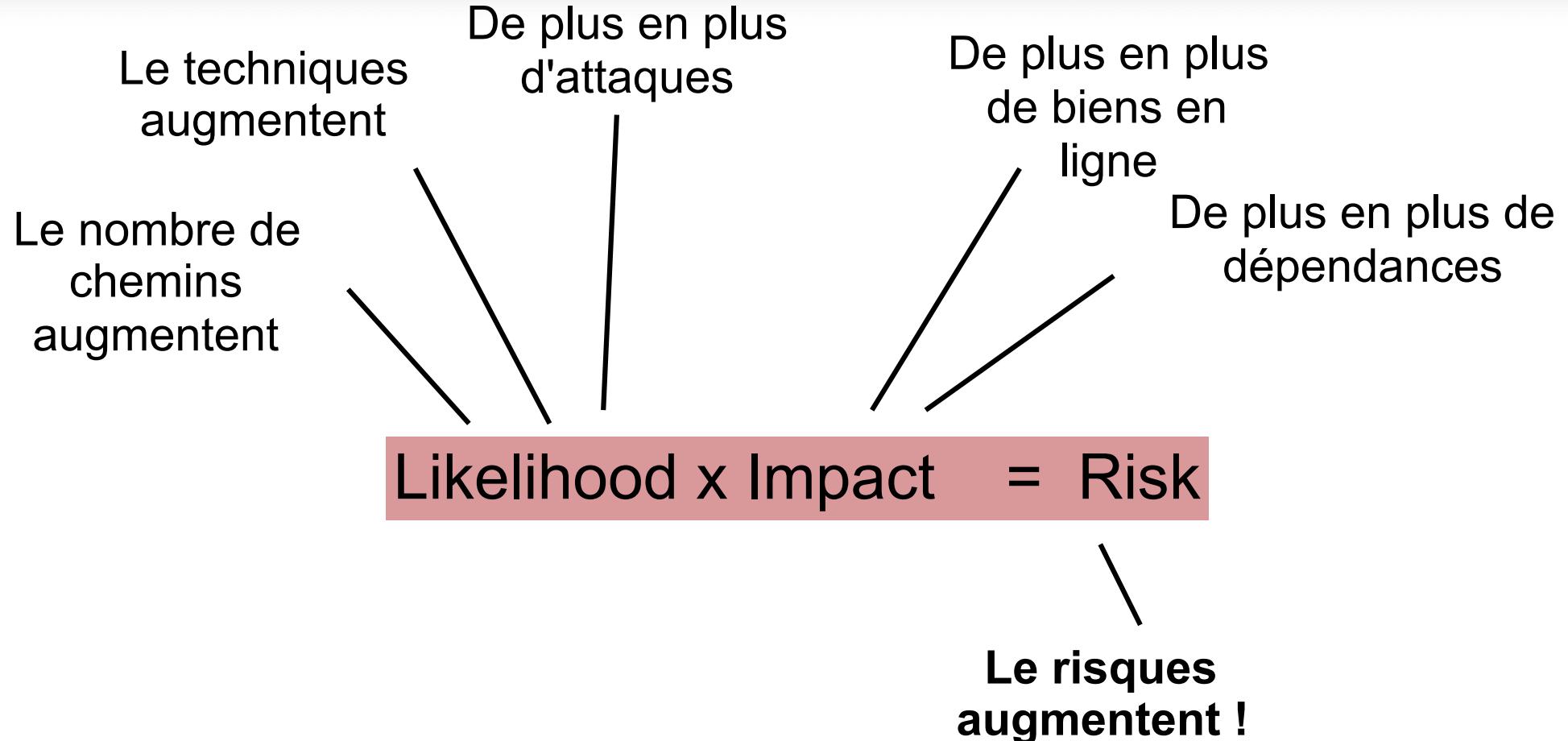
# Compétences variées

- Utilisateurs malins
  - Ils savent comment contourner les protections de l'application
- Script kiddies
  - Ils savent télécharger et utiliser des outils
- Les autorités de réglementation
  - Ils essaient de faire respecter les règles en réalisant des audits
- Blackhats
  - Ils connaissent des techniques pour s'introduire
- High-skilled blackhats
  - Ils inventent des techniques pour s'introduire

# Motivations variées

- Motivations :
  - S'amuser (souvent sans autre but).
  - Prise de contrôle, pouvoir, ego.
  - Acquérir des connaissances techniques.
  - Morales : politique, écologie, social, "robin des bois", etc.
  - Ressources gratuites : accès, machines, etc.
  - Argent, escroqueries, espionnage industriel/économique.
  - Terrorisme, espionnage, guerre informatique.

# De plus en plus de risques !



# Les défis !

- Une organisation fait des compromis entre
  - temps
  - finances
  - technologies
  - culture
  - éthique
  - environnement
  - lois
  - facilité/confort d'utilisation
  - compétences

# Conclusion

- Les entreprises ne peuvent pas toutes engager des équipes de sécurité
  - pourtant leur surface d'attaque augmente
- Les défis de la gestion des risques
  - Est-ce que **chaque partie de l'application doit être sécurisée ?**
  - Qu'en est-il si l'application **part en production la semaine prochaine** ?
    - Que devons-nous faire en **priorité** ?
  - Qu'est-ce qu'il se passe si une **menace a été oubliée** ?
  - Comment garantir un niveau de **sécurité** même si le système est déployé puis **hacké** ?
    - Où est la frontière entre “nous n'avons pas fait notre travail” et “nous avons fait ce que nous pensions légitime” ?

# Aperçu

- 1 Introduction à la gestion des menaces/risques
- 2 Menaces des applications Web
- 3 **Modélisation de menaces**

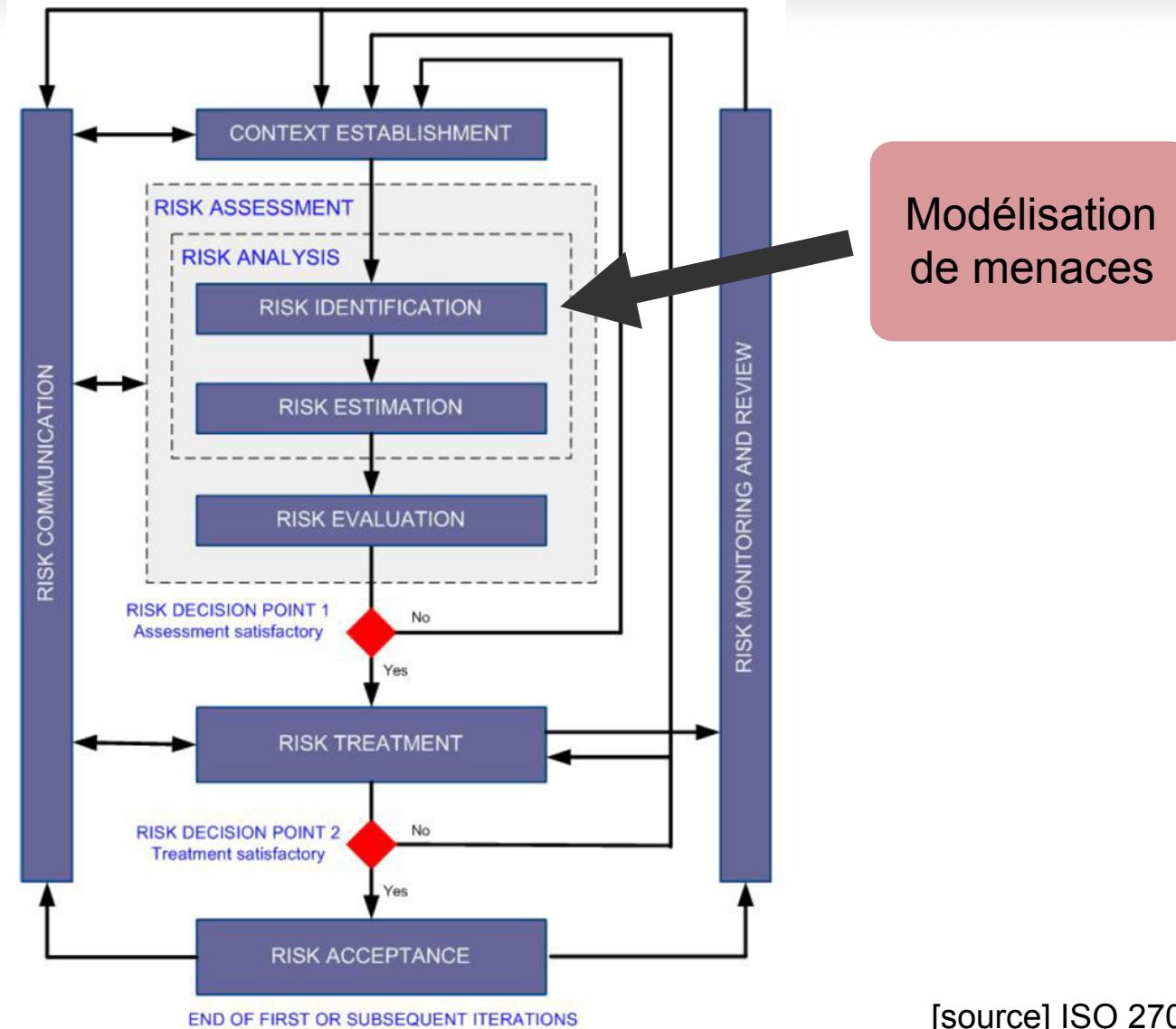
# Mais qu'est-ce qu'une application sécurisée ?

- Elle respecte les **lois** auxquelles elle est sujette.
  - Conformité
- L'application **protège elle-même** ainsi que **tous les systèmes** avec lesquels elle interagit contre toute action non autorisée.
  - Confidentialité / intégrité
- Elle doit garantir un niveau de **performance** acceptable.
  - Disponibilité
- Les utilisateurs ne peuvent nier leurs actions.
  - **Non-réputation**

# Mais qu'est-ce qu'une application sécurisée ?

- Chacun a sa propre vision de la sécurité :
  - site Web personnel
  - forum
  - communauté
  - réseau social
  - commerce électronique
  - e-banking
  - infrastructure critique (pour la nation)
- Modélisation de menaces :
  - identifier et comprendre les **menaces**
  - identifier les **mesures adaptées**

# Gestion des risques (cf SSP)



[source] ISO 27005 - Information Security Risk Management

# Modélisation de menaces

- Permet de rendre **visible** 3 choses :
  - les menaces
  - les expositions actuelles du systèmes à ces menaces (niveau de risque)
  - les opportunités de réduire le risque (contremesures)
- Permet de fixer des **priorités**
  - Quelles sont les parties absolument sensibles ?
  - Quels risques peuvent être supprimés/diminués ?
  - Quels sont les risques acceptables ?
- Permet de créer de la **confiance**
  - visibilité des risques + priorités = confiance

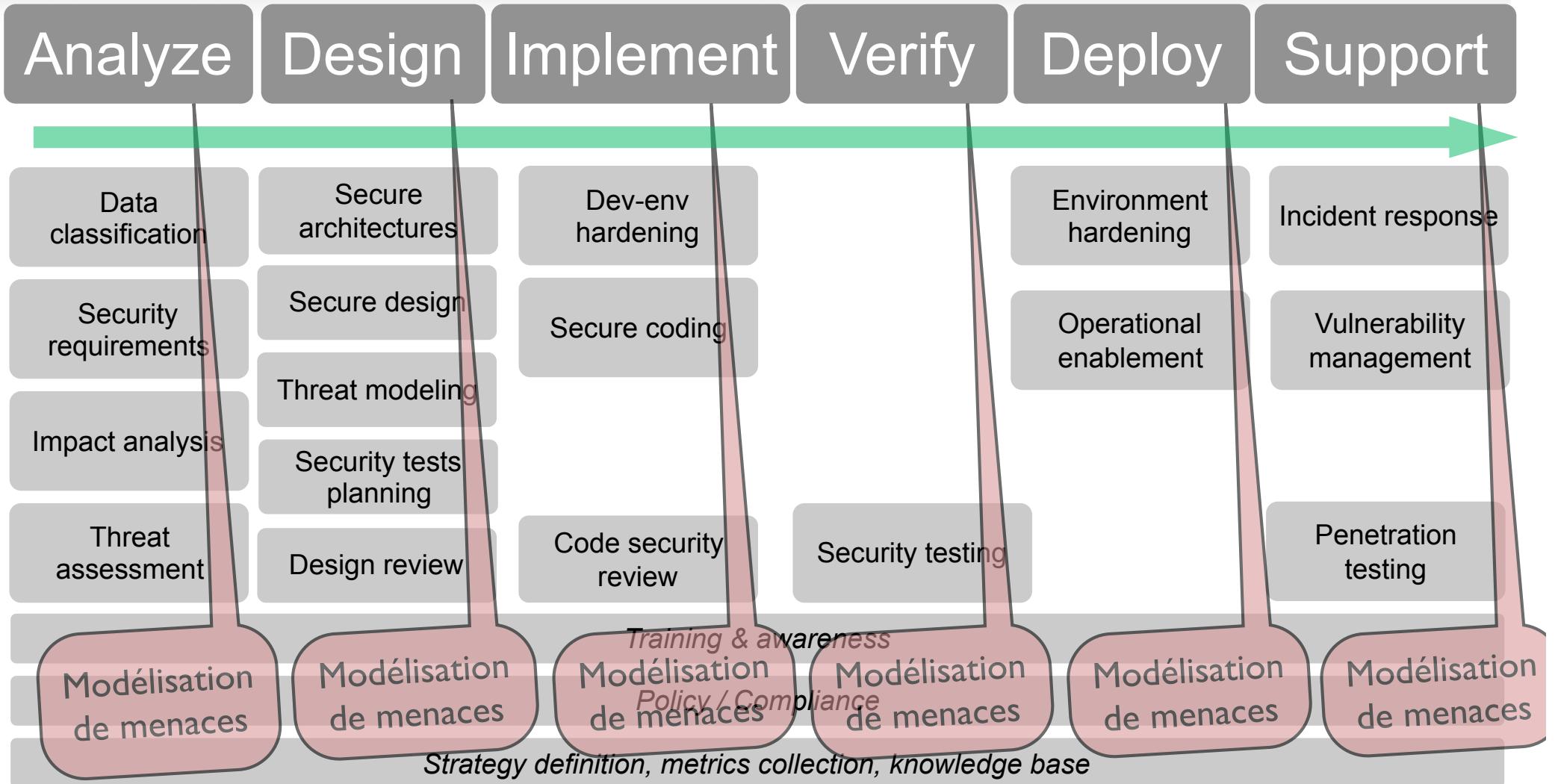
# Modélisation de menaces

- Le modèle de menaces est **non certain**
  - Il augmente la confiance, mais ne garanti rien !
  - On peut oublier des menaces, des biens, des contremesures, ...
- C'est un **art** plutôt qu'une science
  - Il y a beaucoup de méthodes différentes
  - Rien de technique défini la documentation et sa formalisation
- C'est un **processus agile**
  - Un modèle de menaces évolue au cours du temps.
  - Il n'est jamais terminé.
  - Il contient ce que vous pensez nécessaire.

# Modélisation de menaces

- C'est un élément **viral**
  - Il se propage au long du cycle SDLC
    - Phase d'implémentation : détermine les contremesures
    - Phases de vérification/test : vérification des parties à haut risque
    - Phase de déploiement : analyse de risques
- Difficile à justifier
  - Moins démonstratif qu'un test d'intrusion

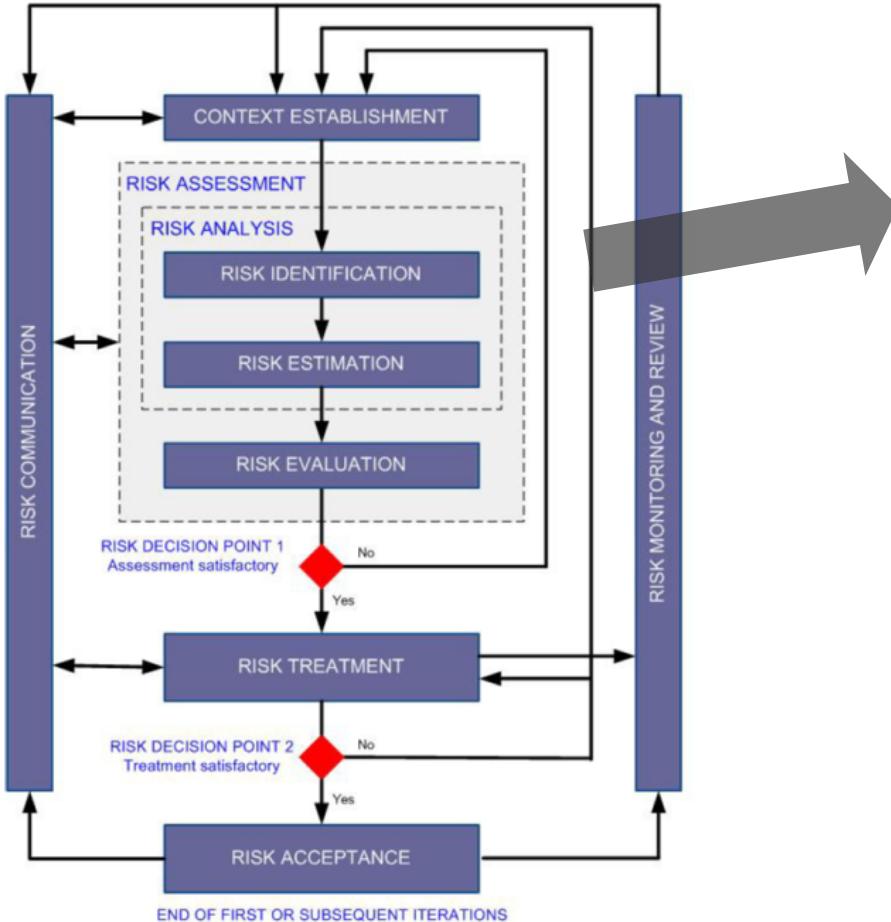
# SDLC - Modélisation de menaces



# Modélisation de menaces

- Comment ça se pratique ?
  - Sur du papier !
  - Papier - crayon - beaucoup de réflexion sont suffisants
  - Pas besoin de code, d'implémentation, d'architecture définie

# Le processus



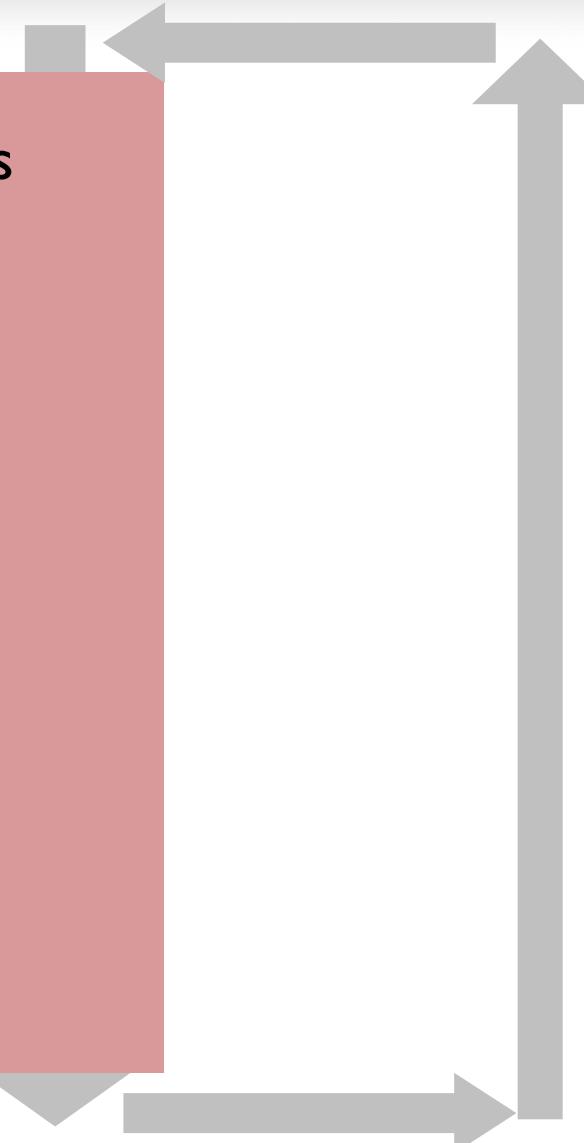
ISO 27005  
Gestion des risques

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle

Processus de modélisation de menaces

# Processus de modélisation

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle



# Processus de modélisation

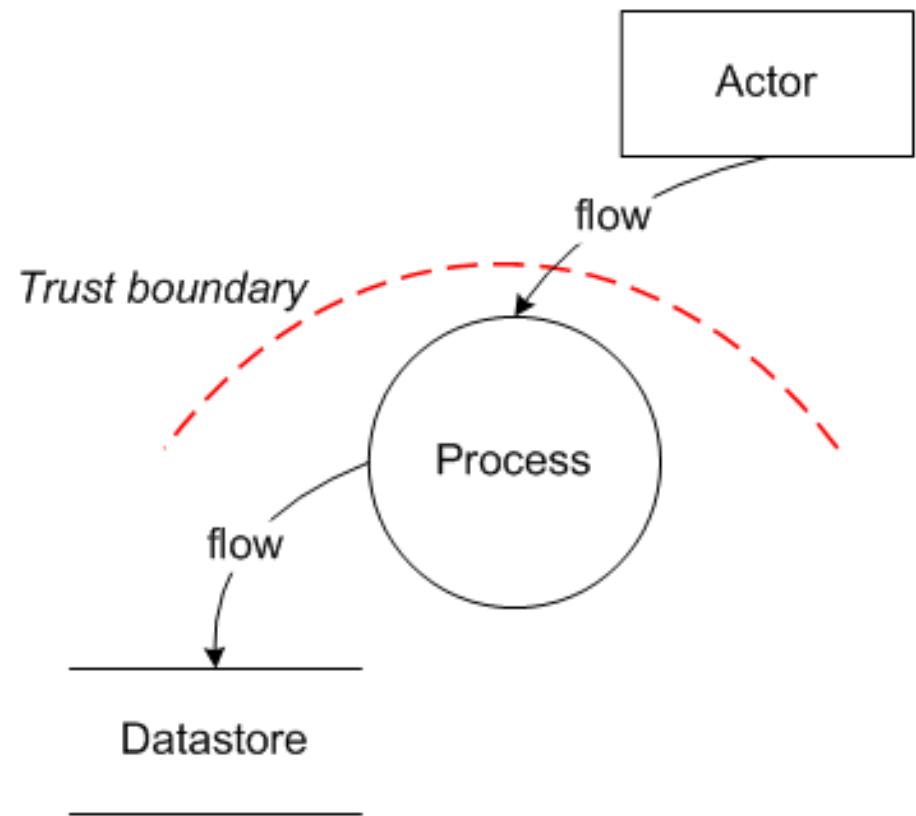
- 
- ```
graph TD; A[1. Décrire le système, identifier ses actifs] --> B[2. Identifier les sources de menaces]; B --> C[3. Identifier les scénarios d'attaques]; C --> D[4. Identifier les contremesures]; D --> E[5. Documenter]; E --> F[6. Diffuser le modèle]; F -- feedback --> A;
```
1. Décrire le système, identifier ses actifs
  2. Identifier les sources de menaces
  3. Identifier les scénarios d'attaques
  4. Identifier les contremesures
  5. Documenter
  6. Diffuser le modèle

# Description du système

- Quels sont les **objectifs** du système
- Quelles sont les **exigences** du système
- Comment est **constitué** le système
  - utilisateurs, machines, flux, ...

# Décomposition du système

- Data-flow diagrams (DFDs)
- 4 types de composants
  - Processes
    - Business decisions
  - Flows
    - Data transport
  - Data stores
    - Data persistence
  - Trust boundary
    - Indicate different security levels
  - Actors
    - Event triggers



- Limite de confiance
  - confiance aux administrateurs, confiance aux autres machines, interception réseau, ...
  - exemples : processus, système de fichiers, réseaux, ...
- Sources de données
  - que faut-il protéger ? vol, vente, lecture, destruction, modification
  - que peut-on stocker ? lois ?
  - exemples : base de données, fichiers de config, registre, mémoire, ...
- Programme
  - modification de la logique, arrêt, ...
  - exemples : composant, service, librairie, exécutable, ...
- Acteur
  - usurpation, nier ses actions, équipement source compromis, équipement source intéressant à compromettre, ...
  - exemples : utilisateur, autre système, partenaire, ...
- Flux
  - interception, modification, direction, porte d'entrée, ...
  - exemples : appel, lien réseau, requêtes/réponses, ...

# Processus de modélisation

- 
- ```
graph TD; A[1. Décrire le système, identifier ses actifs] --> B[2. Identifier les sources de menaces]; B --> C[3. Identifier les scénarios d'attaques]; C --> D[4. Identifier les contremesures]; D --> E[5. Documenter]; E --> F[6. Diffuser le modèle]; F -- feedback --> A;
```
1. Décrire le système, identifier ses actifs
  2. Identifier les sources de menaces
  3. Identifier les scénarios d'attaques
  4. Identifier les contremesures
  5. Documenter
  6. Diffuser le modèle

# Exemple

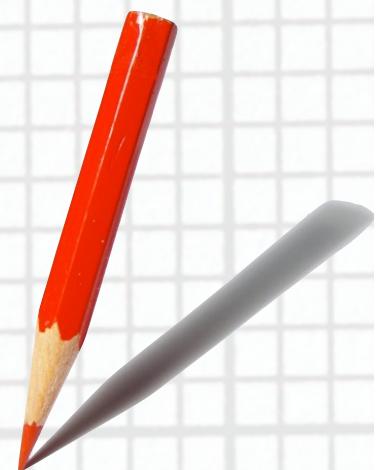
- Online news website :
  - Site d'actualité (news)

The screenshot shows the homepage of The New York Times. At the top, there are links for 'HOME PAGE', 'TODAY'S PAPER', 'VIDEO', 'MOST POPULAR', and 'U.S. Edition'. A banner at the top right says 'Try a Digital Subscription' and 'Register Now'. The main headline is 'Al Qaeda Plot Leak Has Hampered U.S. Intelligence' by Eric Schmitt and Michael S. Schmidt. Below it is another article, 'The House Rushes to a Shutdown' by the Editorial Board. On the right side, there's a sidebar for 'The Opinion Pages' with articles like 'Can Walter White Save Your Soul, if Not His?' and 'Op-Ed: Our Outlaw President'. The 'MARKETS' section shows stock prices for S&P 500, Dow, and Nasdaq. The 'MAGAZINE' section features an article about 'Fiction by Dave Eggers'. The bottom right corner has a graphic of a pencil.

- Contenu très dynamique
  - Editeurs peuvent poster du contenu très souvent
- Les utilisateurs non-inscrits (gratuit) peuvent consulter du contenu limité
- Les utilisateurs abonnés (payant) peuvent accéder aux articles premium,
- Le site maintient une forte réputation de part la fiabilité des informations diffusées

# Exemple: online news website

- Identifiez
  - les objectifs
  - les hypothèses sécuritaires
  - les exigences sécuritaires



# Exemple: online news website

- **Objectifs du système :**

- Diffuser de l'information aux utilisateurs
- Financier : gagner de l'argent grâce aux éditions payantes
- Réputation : avoir une bonne réputation grâce aux informations de haute fiabilité



- **Hypothèses de sécurité**

- réseau interne et administrateurs de confiance
- système d'exploitation et serveur Web de confiance

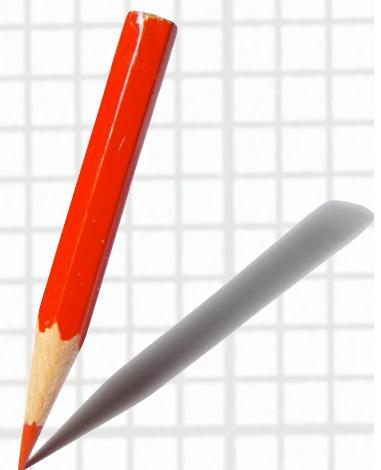
- **Exigences de sécurité :**

- Le contenu payant ne doit être accessible qu'aux abonnés (contrôle d'accès)
- Le contenu doit être protégé en intégrité, non modifiable (info fiable)
- Le site Web doit être disponible à 99% du temps (disponibilité)
- Les informations des utilisateurs doivent être scrupuleusement protégées (privacy)
- Les informations accédées par les utilisateurs ne doivent pas pouvoir être tracées (privacy)
- Un membre premium ne peut ouvrir qu'une connexion simultanément.
- Le contenu ne doit pas être réutilisable (copie, plagiat).



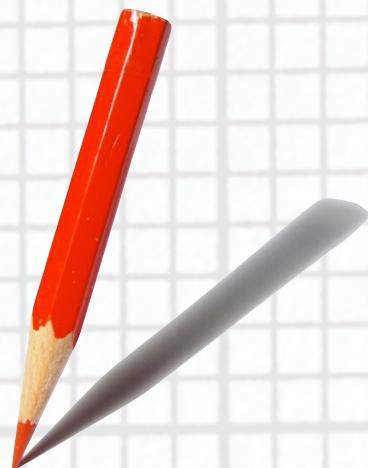
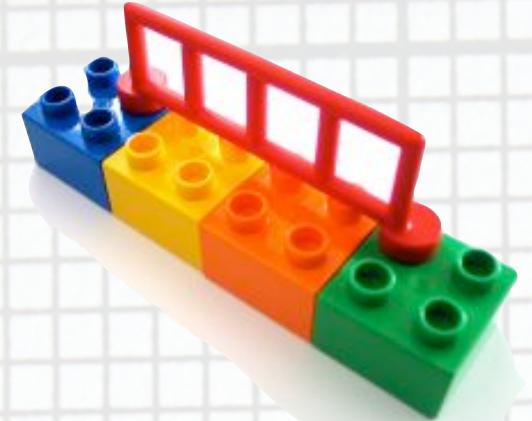
# Exemple: online news website

- Identifiez
  - les éléments du système
  - les rôles des utilisateurs



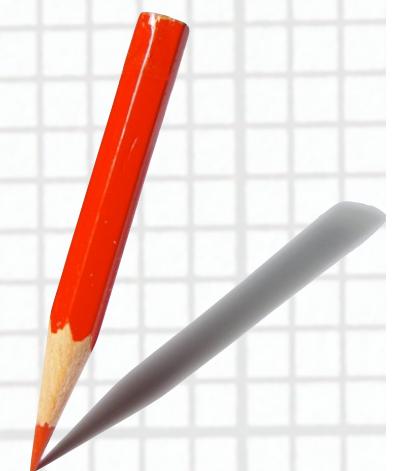
# Exemple: online news website

- **Eléments du système :**
  - Base de données des utilisateurs
  - Base de données des articles (premium ou non)
  - Application Web
- **Rôles des utilisateurs :**
  - Editeurs (contenu)
  - Webmasters (gestion du site)
  - Membres premium (payant)
  - Membres anonymes (petits articles)
  - Administrateurs des machines/réseaux



# Exemple: online news website

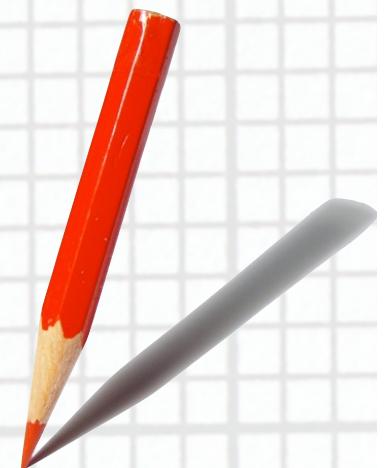
- Identifiez
  - les actifs (assets)



# Exemple: online news website

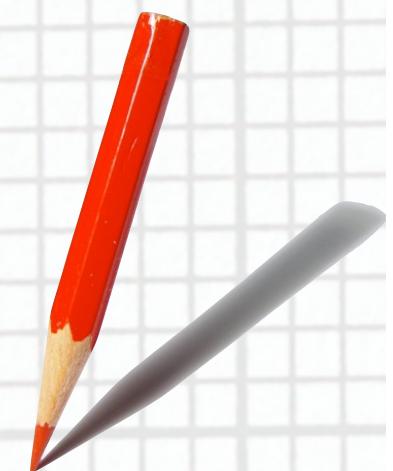
- **Actifs à haute valeur**

- Base de donnée des utilisateurs (données)
  - confidentialité, sphère privée
  - un incident nuirait à la réputation du site !
- Contenu payant (données)
  - confidentialité (uniquement les membres premium ont accès)
  - intégrité (une modification impliquerait une baisse de réputation)
  - un incident engendrerait une perte de revenu
- Base de données des logs (données)
  - confidentialité, sphère privée (possibilité de connaître la liste des accès)
  - intégrité (prouver les actions des utilisateurs, éditeurs de contenu)
  - en cas d'incident les utilisateurs ne peuvent répudier leurs actions
- Infrastructure
  - intégrité, disponibilité
  - un incident serait critique et nuirait à la disponibilité/réputation

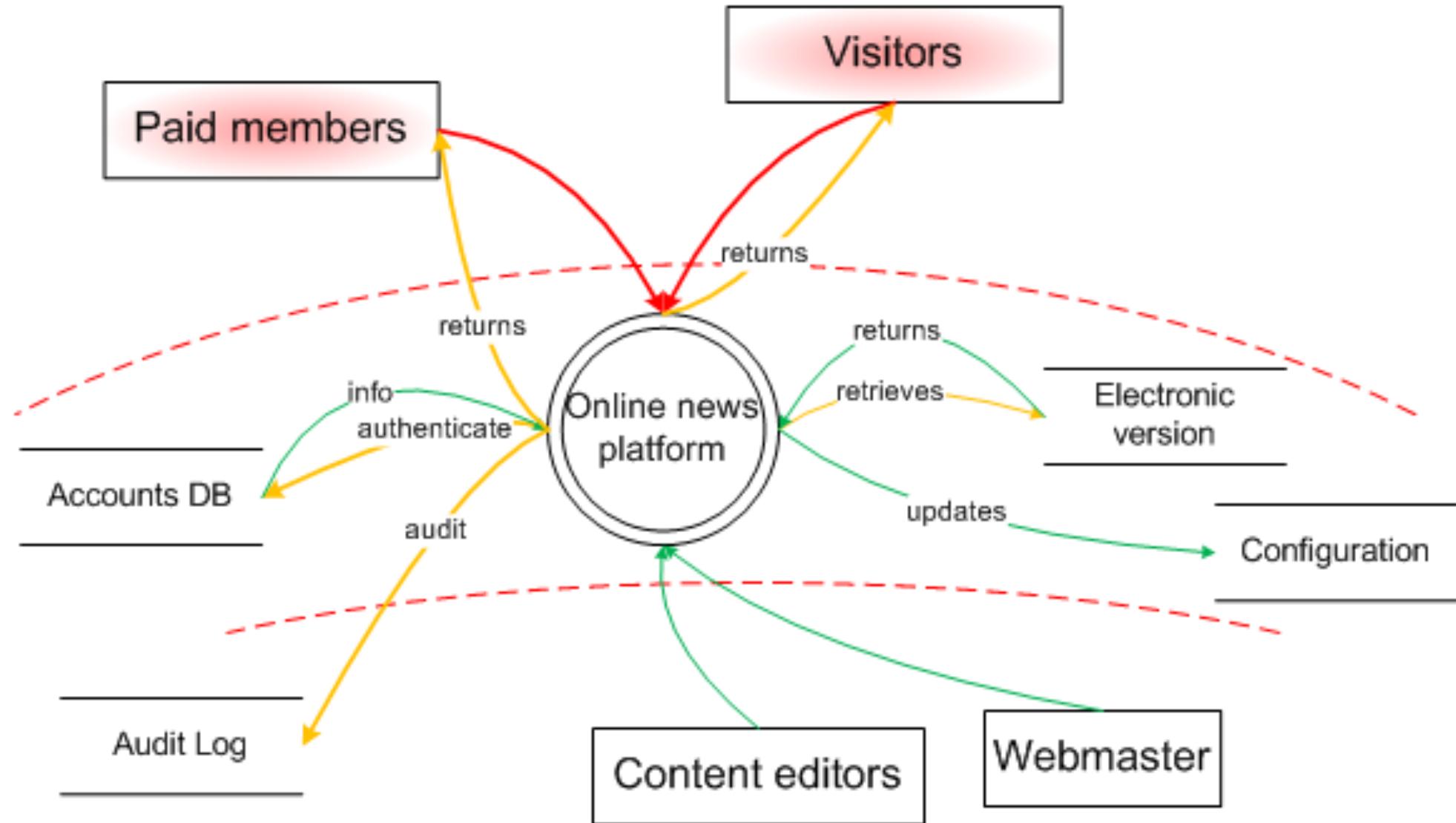


# Exemple: online news website

- Dessinez
  - un DFD



# Exemple: online news website



# Processus de modélisation

1 Décrire le système, identifier ses actifs

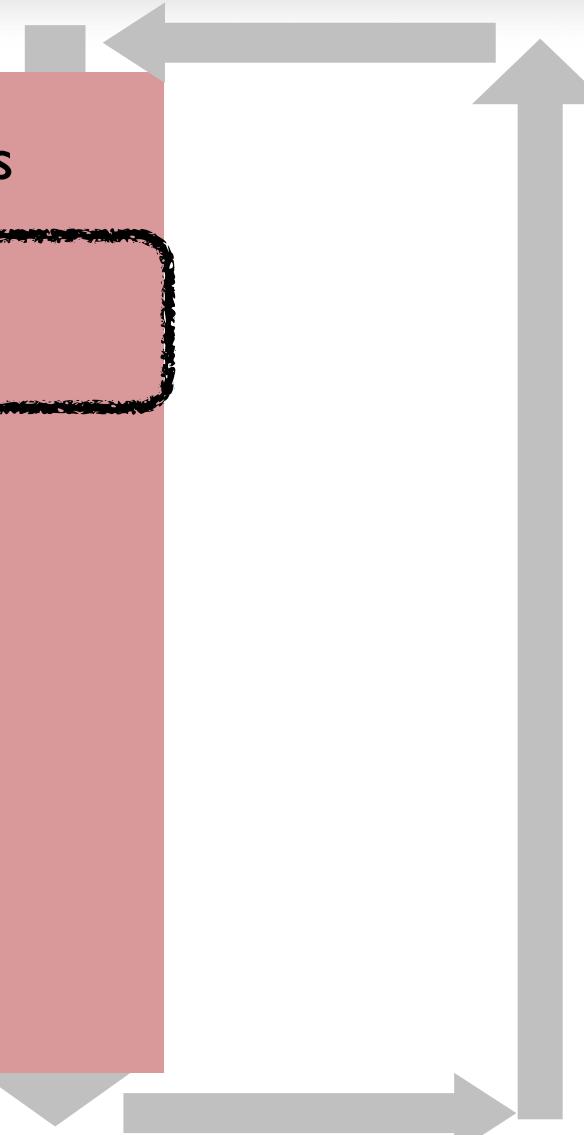
2 Identifier les sources de menaces

3 Identifier les scénarios d'attaques

4 Identifier les contremesures

5 Documenter

6 Diffuser le modèle

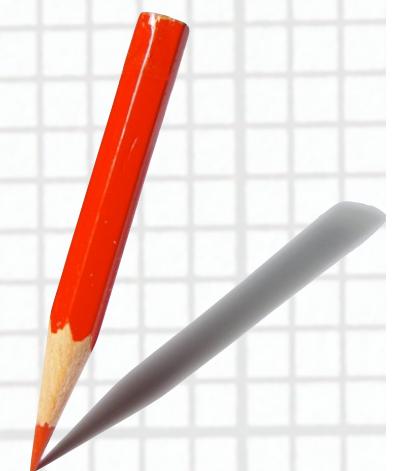


# Identification des sources de menaces

- Définir :
  - les sources potentielles d'agression
  - les cibles potentielles (le système ou rebonds)
  - les motivations
  - les compétences
  - ...

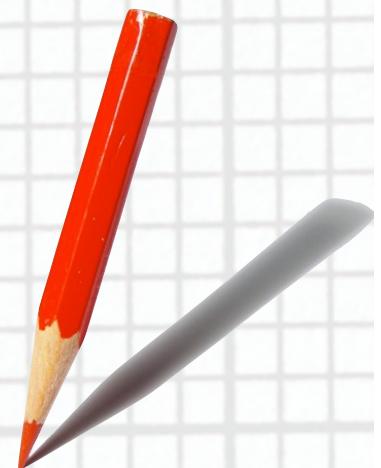
# Exemple: online news website

- Identifiez
  - quelques sources de menaces



# Exemple: online news website

- Hackers, script-kiddies
  - Motivation : s'amuser, gloire
  - Cible : n'importe quel élément / actif
  - Potentialité : haute
- Cybercrime (spam, maliciels)
  - Motivation : financières
  - Cible : vol de credentials du client, spam des clients  
modification d'informations
  - Potentialité : moyenne
- Utilisateurs malins
  - Motivation : accès gratuit aux services payants
  - Cible : contenu premium/payant
  - Potentialité : moyenne
- Concurrent
  - Motivation : réutilisation du contenu
  - Cible : contenu premium/payant
  - Potentialité : moyenne



# Processus de modélisation

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle

# Identification des scénarios

- Identifier les scénarios probables qui conduiront à un dommage
- Pensez typiquement à
  - Vols d'informations
    - confidentialité, compétition, ...
  - Destruction information
  - Modification information or systems
  - Arrêt de processus
  - Infection des systèmes des utilisateurs
  - Usurpations d'identités
  - Accès aux services payants

# STRIDE

- Spoofing vs. Authentication
- Tampering vs. Integrity
- Repudiation vs. Non-repudiation
- Information disclosure vs. Confidentiality
- Denial of service vs. Availability
- Elevation of privileges vs. Authorisation

# STRIDE

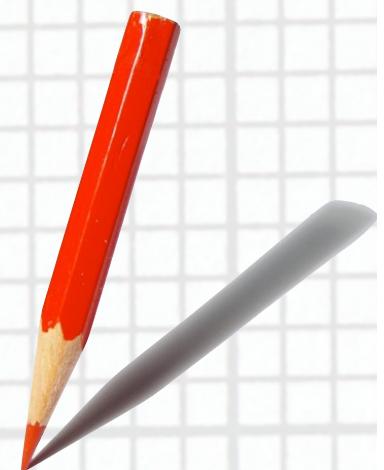
- Spoofing
  - Example: authenticating to the application using a stolen password
  - Countermeasure: strong authentication, secure data transport
- Tampering
  - Example: using SQL injection to modify or delete records of a data base
  - Countermeasure: use of prepared statements, escaping user input
- Repudiation
  - Example: Modify a user shipping address on an e-commerce
  - Countermeasure: request address confirmation and additional authentication to confirm
- Information disclosure
  - Example: intercept clear-text browser traffic in a public wifi
  - Countermeasures: traffic encryption
- Denial of service
  - Example: allocate session memory based on user provided values
  - Countermeasures: validate size before allocating (input validation)
- Elevation of privileges
  - Example: copy/paste an administrative URL within a normal user session
  - Countermeasures: authorization mechanism

# STRIDE et les DFDs

Component	S	T	R	I	D	E
External agent	★		★			
Data store	★	★	★	★	★	★
Process		★	★	★	★	
Data flow		★		★	★	

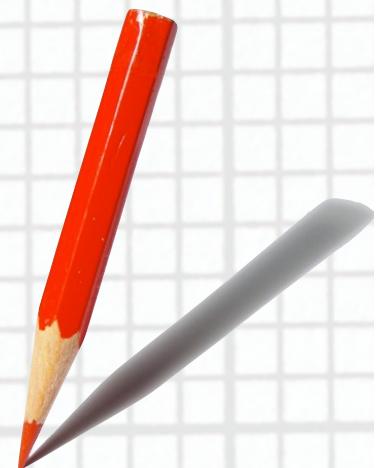
# Exemple: online news website

- Identifiez
  - quelques scénarios d'attaques



# Exemple: online news website

- Threat scenario 1: internal network intrusion (integrity breach)
  - Business impact: high (financial, cost of remediation)
  - Threat source: hackers
  - Motivation: curiosity, challenge
  - Targeted asset(s): internal network and systems
  - Attack scenario:
    - Code injection (request tampering or malicious file injection)
  - Controls:
    - Input validation
      - Use parameterized database queries
    - File input validation



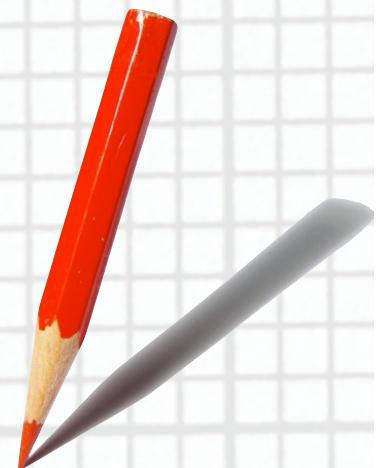
# Exemple: online news website

- Threat scenario 2: users database stealing
  - Business impact: medium (reputation, loss of assets)
  - Threat source: organized cybercrime, competition
  - Motivation: financial
  - Targeted asset(s): user accounts database
  - Attack scenario(s):
    - Code injection (request tampering or malicious file injection)
    - Authorization bypass (access to user profile details)
  - Control(s):
    - Input validation
    - File input validation
    - Strong access control to user details
    - Defense-in-depth: secure password storage, account data encryption



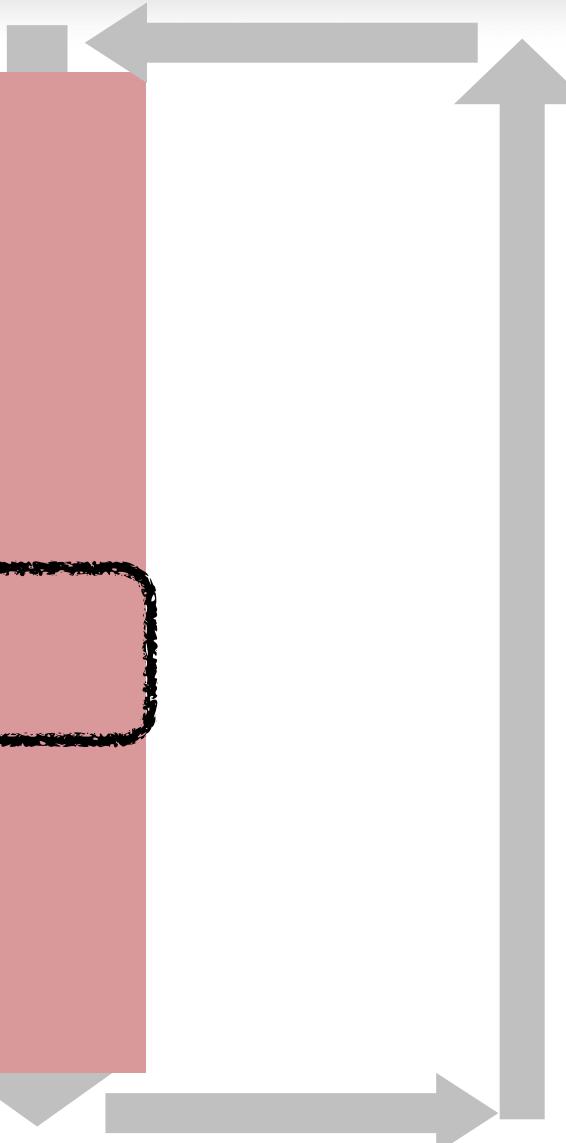
# Exemple: online news website

- Threat scenario 3: access to electronic editions
  - Business impact: medium (revenue loss)
  - Threat source: smart user
  - Motivation: fee avoidance
  - Targeted asset(s): electronic editions database
  - Attack scenario(s):
    - Direct URL access
  - Control(s):
    - Discretionary access control to electronic editions
    - Unguessable URL
    - Etc.



# Processus de modélisation

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle

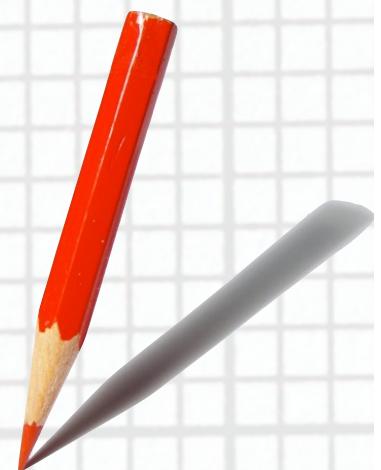


# Identifier les contremesures

- Pour chaque scénario d'attaque
  - Identifier les solutions et contremesures

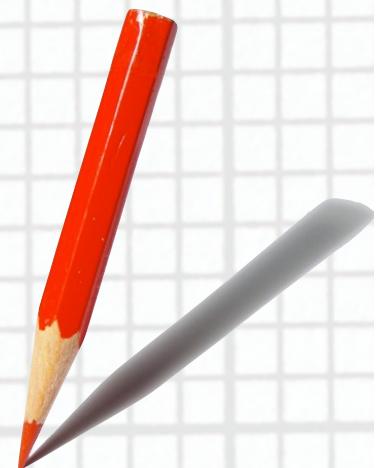
# Exemple: online news website

- Identifiez
  - quelques contrôles de sécurité



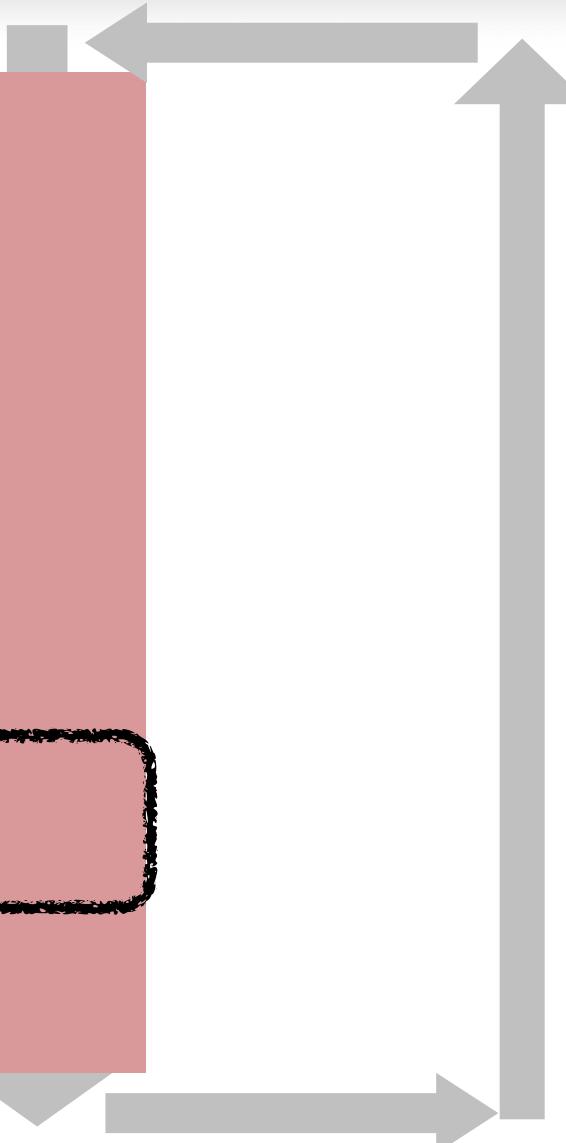
# Exemple: online news website

- Recommended controls for risk mitigation:
  - Validate input for all request parameters
  - Use parameterized SQL queries
  - Ensure access control when displaying user profiles
    - Prevent from request automation
  - Deploy random URLs for accessing the electronic edition
  - Access control when requesting the electronic edition



# Processus de modélisation

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle



# Un modèle de menaces

- Un modèle contient au moins :
  - La description du système
    - objectifs, hypothèses, exigences, rôles, éléments, ...
  - La liste des biens à protéger
  - La liste des sources de menaces
  - La liste des scénarios d'attaques
  - La liste des mécanismes pour diminuer les risques
- Par la suite :
  - Traduire les contremesures en spécifications de conception ou d'implémentation
  - Identifier les modifications dans la conception
  - Mettre à jour le modèle de menaces dès que nécessaire

# Processus de modélisation

- 1 Décrire le système, identifier ses actifs
- 2 Identifier les sources de menaces
- 3 Identifier les scénarios d'attaques
- 4 Identifier les contremesures
- 5 Documenter
- 6 Diffuser le modèle

# Conclusion

- Nous avons un moyen de créer des **modèles de menaces**
  - le **système** est décrit
  - les sources de **menaces** sont identifiées
  - les **scénarios** d'attaques sont identifiés
  - les **mécanismes de mitigation des risques** sont identifiés

# Conclusion

- La modélisation de menaces permet
  - d'identifier des menaces, détecter des scénarios d'attaques, déterminer des contremesures
  - d'accroître le niveau de confiance en terme de sécurité
  - créer un modèle réutilisable
- La modélisation de menaces ne permet pas :
  - d'avoir un modèle figé et universel
  - de couvrir 100% des risques
  - de réduire 100% des risques

# Autres lectures

- Guerilla threat modeling (Peter Torr)  
<http://blogs.msdn.com/b/ptorr/archive/2005/02/22/guerillathreatmodelling.aspx>
- Threat risk modeling (OWASP)  
[http://www.owasp.org/index.php/Threat\\_Risk\\_Modeling](http://www.owasp.org/index.php/Threat_Risk_Modeling)
- Application threat modeling (OWASP)  
[http://www.owasp.org/index.php/Application\\_Threat\\_Modeling](http://www.owasp.org/index.php/Application_Threat_Modeling)
- Threat modeling web applications (Microsoft)  
<http://msdn.microsoft.com/en-us/library/ff648006.aspx>
- Comments on threat modeling (in French, DLFP)  
<http://linuxfr.org/news/threat-modeling-savez-vous-quelles-sont-les-menaces-qui-guette>
- Modélisation de menaces par Antonio Fontes (ForumPHP, juin 2012)  
<http://fr.slideshare.net/starbuck3000/modliser-les-menaces-dune-application-web>