
CYBERDÉFENSE: QUELLE STRATÉGIE POUR LES ENTREPRISES ?
D D

PLAN

- Explications des terms clefs
- Les attaques et les attaquants
- Comment mettre en place une strategie de cyberdefense
- Les technologies de sécurité emergentes
- Q&R

LA TERMINOLOGIE

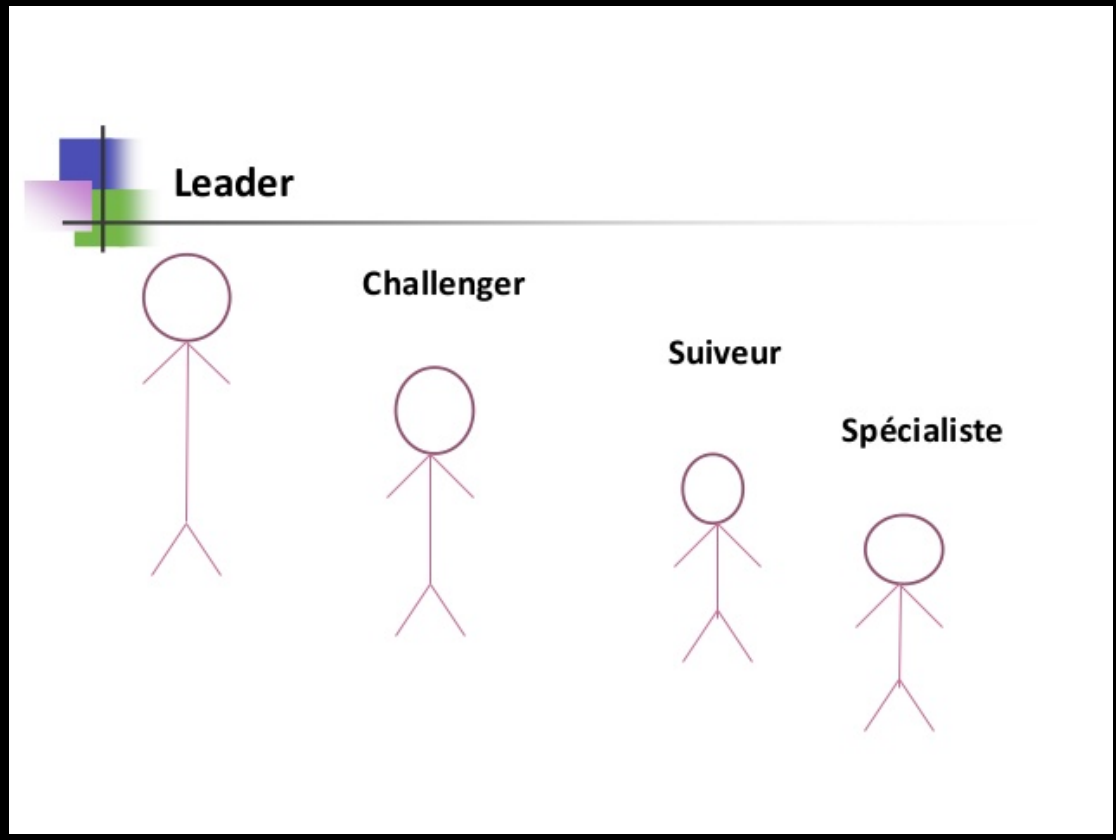
Stratégie

« Le ciment qui permet de construire et d'offrir une proposition de valeur constante et distinctive à votre marché cible.

Pour reprendre la mise en garde de Bruce Henderson, fondateur du Boston Consulting Group : une entreprise qui n'a pas un avantage spécifique sur ces concurrents n'a aucune raison d'exister ».

L'encyclopédie du marketing /Jean-Marc Lehu

STRATEGIE DU:



CYBERDÉFENSE : TENTATIVES DE DÉFINITIONS ?

Dans le contexte du monde purement académique du terme, la **cyberdéfense** désigne « un ensemble de mesures techniques, et non techniques, permettant à un État de défendre dans le cyberspace les systèmes d'information jugés essentiels contre les **attaques informatiques** ».

Dans le contexte du monde de l'entreprise, « le terme pourrait être traduit par une stratégie de défense ciblée du système d'information permettant de protéger les ressources sensibles de l'entreprise contre une attaque informatique".

Cette stratégie met en œuvre des moyens techniques, organisationnels et humains. On parle alors de « **Cybersécurité** ».

La différence avec la sécurité dite « traditionnelle » réside dans la proposition d'une approche stratégique de défense ciblée visant les actifs essentiels au fonctionnement de l'entreprise.

EVOLUTION DES ECOSYSTEMES DES MENACES ET ATTAQUES INFORMATIQUES

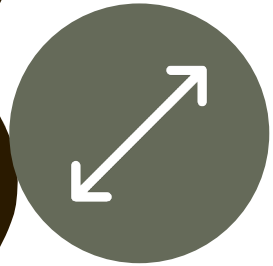
HISTORIQUE DES ATTAQUANTS

Curiosité, compétition…

Arsenal technologique de guerre

Entreprise: offre et demande

CONTEXTE: LES ATTAQUES



Attaques sur mesures et professionnelles

Guerre numérique intelligente.

Objectif des cybercriminels: une occupation durable du terrain invisibles des radars de technologiques de détection.

Expansion exponentielle des maillons vulnérables:

Un périmètre à surveiller de plus en plus vaste, et de plus en plus difficile à maîtriser

CYBERDÉFENSE : LA MENACE INFORMATIQUE IMPACTE LE MONDE DU BUSINESS

- La visée des menaces et des attaques n'est plus seulement informatique mais plutôt l'activité de celle-ci (business, production, image de marque de l'entreprise, etc.).
- Les impacts sont donc multiples, notamment :
  - La Réputation (= défacing site web / déni de service)
  - Le Savoir (malware furtifs / interception et exfiltration de données)
  - L'Intégrité des processus industriels (compromission des accès, infection des systèmes industriels, arrêt de la production, etc.)
- L'activité des cibles est aujourd'hui de plus liée à la bonne santé du SI. De la ,on comprend aisément le lien entre la menace informatique et l'impact final sur l'activité de l'entreprise.
- L'enjeu des SI est donc d'assurer la préservation du patrimoine de l'entreprise, tout en répondant aux enjeux métiers, sans oublier de garantir la conformité aux obligations légales (législature nationale & internationale).

CYBERDÉFENSE : PRÉVENIR, DÉTECTER ET RÉAGIR EST VITAL POUR L'ENTREPRISE

- Pas de risque zéro dans le monde numérique.
- Donc se préparer à subir l'attaque - parce qu'elle arrivera forcément tôt ou tard.
- Contrer, et non pas empêcher.
- « La **cybersécurité** est ainsi une stratégie de défense ciblée des biens sensibles de l'entreprise.».
- Cette organisation repose sur une méthodologie, une expertise et un outillage continuellement revus et améliorés.

COMMENT METTRE EN PLACE UNE STRATEGIE DE CYBERDEFENSE AU SEIN DE L ENTREPRISE?

CONTEXTE

La **cybercriminalité** menace tous les domaines de l organisation de l espace humaine.

Réaction: création d une **stratégie de cyberdéfense**

STRATÉGIE DE CYBERDÉFENSE :

ANTICIPER LES MENACES ET PROTÉGER LES SYSTÈMES D'INFORMATION

Le quid pro quo de la mise en œuvre d'une stratégie de cyberdéfense cohérente et fiable, est d'identifier en amont les différentes phases du processus.

PHASE 1 :

PROTÉGER LE SOCLE DE L'ENTREPRISE

- Définir une stratégie de défense proactive
- Cibler ce qui est essentiel à l'activité de l'entreprise
- Réaliser des audits de vulnérabilité et tests d'intrusion
- Réaliser des analyses de risques et déterminer les impacts d'une attaque (BIA : Business Impact Analysis)
- Définir un schéma directeur pour renforcer les mécanismes existants

PHASE 2 :

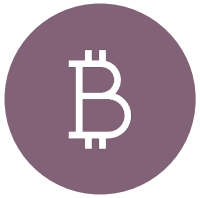
METTRE EN PLACE DES TECHNOLOGIES DE SÉCURITÉ STATIQUES ET DYNAMIQUES

DÉFINIR DES SOLUTIONS ADAPTÉES, ET ÉVITER LA FUITE EN AVANT TECHNOLOGIQUE

SÉLECTIONNER LES SOLUTIONS PERTINENTES

LIMITER LES RISQUES OPÉRATIONNELS

RENFORCER LES TECHNOLOGIES DÉJÀ EN PLACE, ET LES INCLURE DANS LE SYSTÈME DE SURVEILLANCE



MESURER LE RISQUE INDUIT PAR L'INTRODUCTION D'UNE NOUVELLE SOLUTION

PHASE 3 :

GARANTIR LA SÉCURITÉ OPÉRATIONNELLE ET FONCTIONNELLE

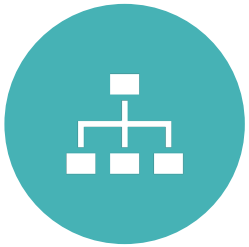
- Mise en place de la surveillance et des processus de réaction
- Surveillance du SI, corrélation, identifier les signaux faibles (collecte et métriques de surveillance)
- Gestion des évènements de sécurité et qualification des évènements (positif ? négatif ?)
- Gestion des incidents de sécurité, évaluation, investigation, remédiation
- Audit, suivi des indicateurs, amélioration continue de sécurité
- Sensibilisation des utilisateurs

STRATÉGIE DE CYBERDÉFENSE : QUELS OUTILS UTILISER ?

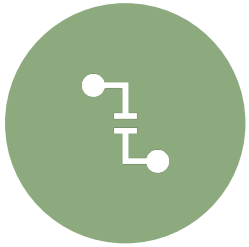
- ✓ Une cartographie non exhaustive des différents outils permet la mise en œuvre de votre stratégie de défense
- ✓ L'**audit en sécurité** et les tests d'intrusion
- ✓ L'intégration de solutions de protection pertinentes et adaptées aux risques et aux menaces visant le périmètre sensible
- ✓ La gestion des vulnérabilités du périmètre sensible et le périmètre exposé, internes ou sous-traités.
- ✓ Les méthodes et techniques de promotion et la sensibilisation des utilisateurs
- ✓ Le SOC (**Centre Opérationnel de sécurité**)
- ✓ Le ResponseTeam

CONCLUSION

« Plan »



« Do »



« Check »

« re-Act »

LES TECHNOLOGIES DE SÉCURITÉ ÉMERGEANTES

- L'analyse du comportement utilisateur
- L'authentification matérielle
- Les applications de sécurité biométrique
- Le nuage
- L'apprentissage "Deep Learning"
- La prévention de la perte de données

QUESTIONS

- **Stratégie offensive, défensive ou mixte… Laquelle devriez-vous choisir ?**