Pistes d'action - Cybersécurité

Marie Truchassou

marie@forwardsinternationalhr.com

MasterClass ALIPTIC 15/03/2022

Organisé par :

ALIPTIC

France IT

En collaboration avec :

DIGITAL AQUITAINE

Avec le soutien de :

RÉGION Nouvelle-Aquitaine

Bonnes Pratiques

Mise en place de systèmes de binomes / Partenariat

Au regard des tactiques d'ingénierie sociale, il faut encourager les salariés à échanger entre eux, éventuellement avec un partenaire dédié afin de jeter un oeil à l'email, écouter le message vocal ou encore prendre partie à l'interaction.

Bonnes Pratiques

Mise en place de procédures et inclusion dans la culture d'entreprise

- Il est plus simple d'introduire une Politique, des procedures et des bonnes pratiques qui initialement semblaient superflus que de les rendre applicables ultérieurement et en particulier en situation de contrôle des dommages déjà réalisés.

Ex concret : le transfert de l'ensemble des data d'une société vers un espace cloud sans que ces données n'aient été proprement classifiées et sécurisées.

- Il faut d'assurer de la pérennité de ces bonnes pratiques dans le temps, dans ce cadre l'inclusion dans la culture d'entreprise est primordiale, mais également dans la stratégie RH (inclusion dans le process d'onboarding, mise en place de formations régulières etc)

Bonnes Pratiques

Clarté et communication pour gérer la complexité

La clarté est la sécurité.

Le point clé ici n'est pas forcément d'avoir un expert qui puisse complètement gérer l'aspect technique, mais plutot la capacité de traduire les bonnes pratiques de cybersécurité en decisions manégériales générant des bonnes pratiques mises en oeuvre par les salaries et poussées par les managers.

- Ne pas oublier que de moins en moins, les attaques ciblent les systèmes ou les specialistes sécurité des organisations.

  Mais de plus en plus ciblent les salariés.

- Une communication Claire, récurrente et transparente afin de permettre la remontée des problemes et l'implication de chacun des acteurs est necessaire.

Bonnes Pratiques

Appliquer la CIA au sein de votre organisation

La CIA reflète 3 principes clés en matière de cybersécurité

1. Confidentialité
2. Integrité
3. Accessibilité.

Bonnes Pratiques

Appliquer la CIA au sein de votre organisation - Confidentialité

Comment nous assurer que nous gardons nos informations sécurisées des regards indiscrets tiers à notre organisation ?

Comment nous assurer que nos salaries ont accès à l'information dont ils ont besoin et uniquement l'information dont ils ont besoin ?

Bonnes Pratiques

Appliquer la CIA au sein de votre organisation - Intégrité

Comment nous assurer que l'information est protégée de toute manipulation / modification accidentelle ou malveillante ?

Comment nous assurer que nos salaries ont accès à l'information mais ne peuvent la modifier que si absolument nécessaire ?

Bonnes Pratiques

Appliquer la CIA au sein de votre organisation - Accessibilité

Aucun système d’information n’est utile s’il n’est pas accessible.

Bonnes Pratiques

Problématiques Pratiques de la CIA

Sur les dernières années, grâce au cloud computing notamment, l'accessibilité a été "simple" à mettre en place.

Mais les entreprises ont plus de mal à concilier **confidentialité et intégrité**.

Concrètement, la CIA se mesure et s'applique par des mesures concrètes :

1. gestion des accès,
2. classification des données qui doivent être liées à la gestion des RH
3. définitions de poste au sein de l'organisation qui définissent le scope d'accès aux données.

Bonnes Pratiques

Shadow IT

Définition de Shadow IT :

Ensemble d'usages informatiques qui échappent au contrôle du responsable de la sécurité de l'entreprise, une sorte d'informatique parallèle qui comprend différentes formes d'activités liées aux technologies de l'information.

- Identifier les pratiques de Shadow IT et trouver des solutions adaptées
- Qualifier, identifier et communiquer les outils informatiques “validés” par l’organization
- Intégrer les solutions trouvées dans le format de formation et d’onboarding afin d’intégrer le changement sur le long terme + faire un booster pour l’intégrer dans la culture / Pratiques de l’organisation

Bonnes Pratiques

Anticiper la continuation / reprise de l'activité

S'inspirer de la gestion de crise et mettre en place des stratégies / procédures de manière pro-active au sein de l'organisation afin de pouvoir anticiper la continuation et / ou la reprise de l'activité suite à une attaque de cybersécurité.

Etudier les caractéristiques de l'organisation, de son activité et celle de ses clients avant de définir les plans de gestion de risque / crise.

Ne surtout pas dupliquer ce qui est fait chez le voisin. Définir une procédure correspondant à son ADN et idéalement impliquer les salariés dans la préparation de ces procédures afin de bénéficier d'un engagement maximum.

Bonnes Pratiques

Distinguer Menace et Vulnérabilité

Une menace est généralement un **acteur cherchant à bénéficier de la faille pour cause un dommage**.

La vulnérabilité peut être génériquement qualifiée de **fragilité** qui peut causer un tort au système et à l'organisation.

Généralement une attaque a lieu quand une menace exploite une vulnérabilité.

Afin de gérer cette attaque, il est généralement recommandé de gérer une part de l'équation cad soit la menace, soit la vulnérabilité.

Bonnes Pratiques

Distinguer Menace et Vulnérabilité

De manière Générale, il est recommandé et plus efficace de **supprimer la vulnérabilité** (par ex par le biais d'une mise à jour d'un software) plutôt que de tenter d'empêcher toutes les menaces.

En deçà de cette dichotomie, il ne faut pas oublier non plus la notion d'exposition

Une exposition ici peut être qualifiée de manière générique comme une **erreur d'implémentation ou d'utilisation.**

En anologie pratique, prenons l'exemple d'un système de fermeture de porte hyper sécurisé. Si le système n'est pas sécurisé, cela constitue une vulnérabilité. Un système hyper sécurisé mais dont la personne oublie d'activer la fonctionnalité constituerait une exposition.

Ici on retombe sur l'importance de la notion de formation «utilisateur », ici votre salarié.