Simplifiez Économisez Rentabilisez

Regard sur la cybersécurité

Le monde a changé

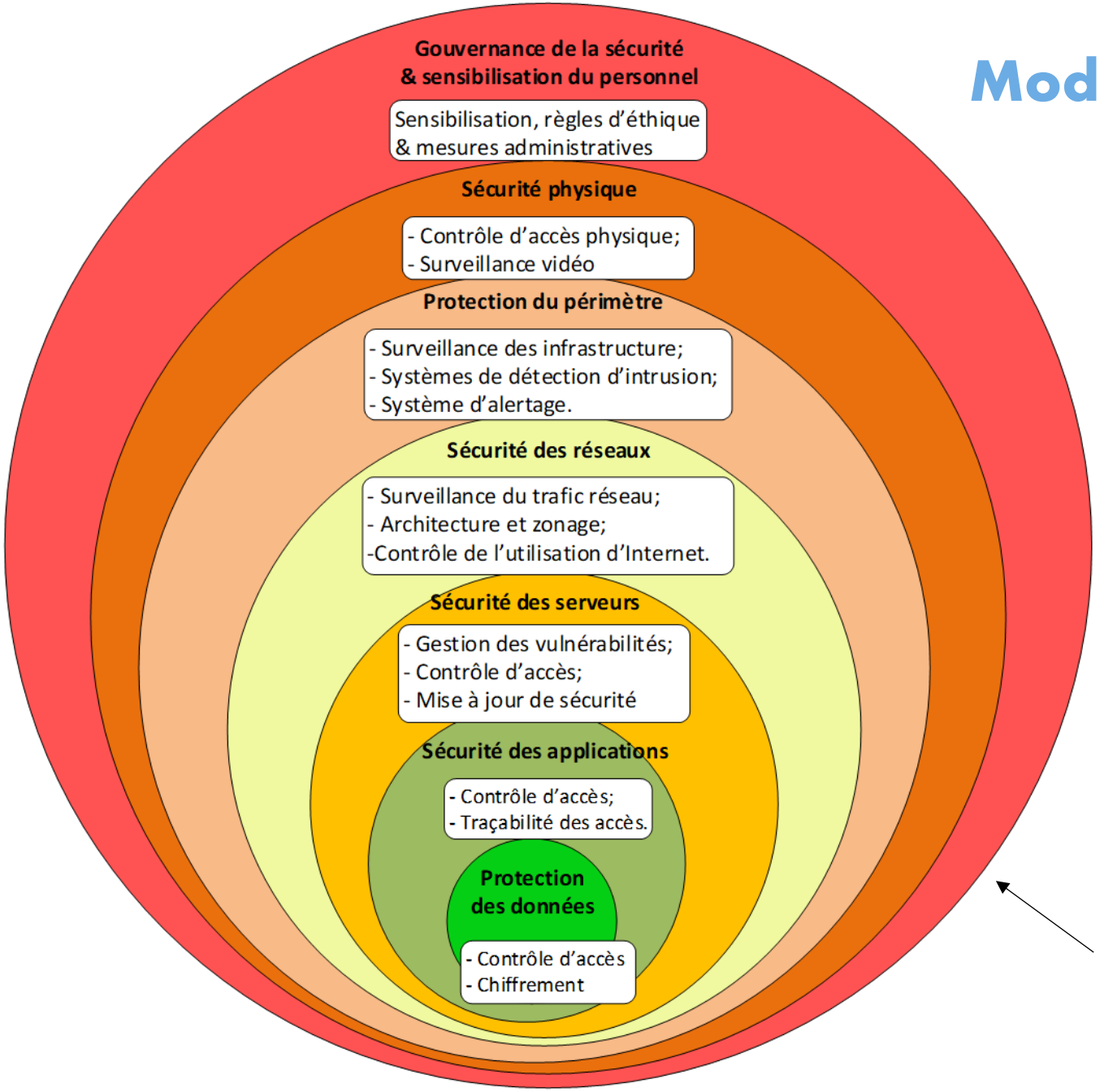
- Modèle traditionnel de la sécurité
- Environnement actuel et à venir
- Nouvelle approche
- Nouvelle méthodologie

Nous devons nous adapter, 5 moyens pratiques

- Sauvegardez vos données
- Mettez à jour vos appareils
- Assurez la sécurité de vos mots de passe
- Sécurisez vos comptes de médias sociaux
- Soyez à l'affût des messages d'hameçonnage

SERVICES INFORMATIQUES

Modèle traditionnel de sécurité



Avantages du modèle

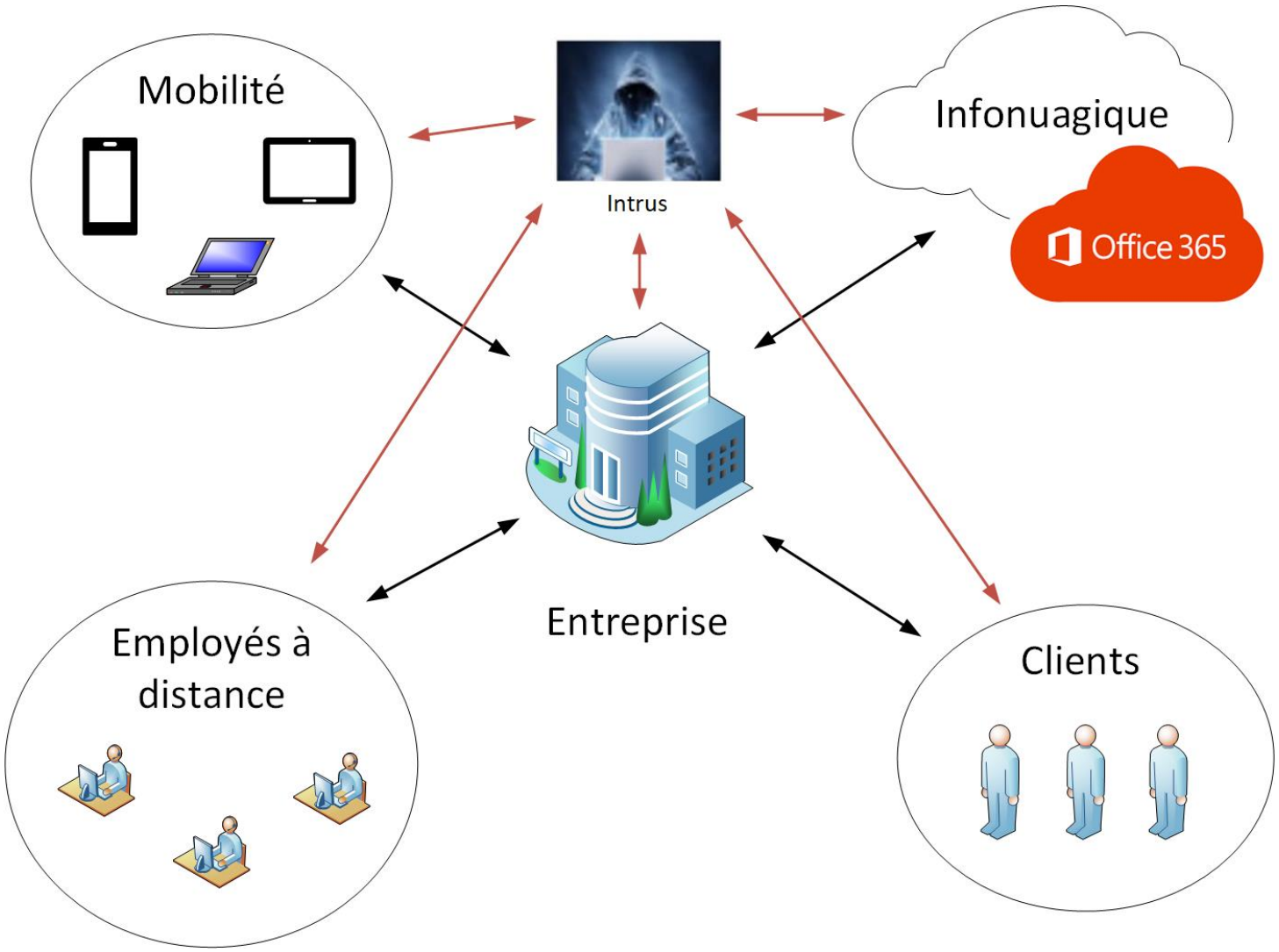
- Augmente la probabilité de détection d'un intrus.
- Réduit les chances de succès d'un intrus.
- Améliore l'efficacité et l'efficience des interventions.

Limite du modèle

- Modèle conçu spécifiquement pour la menace externe

ML SERVICES INFORMATIQUES

Environnement actuel et à venir



- Fusion des menaces internes et externes
- Les TI ne suffisent plus pour contrer les menaces
- Le facteur humain doit être au cœur de la stratégie de cybersécurité

SERVICES INFORMATIQUES

Hygiène numérique

Mode physique

- Barrez les portes de la maison
- N’ouvrez pas la porte à des inconnus
- Ne croyez pas tout ce qu’on vous dit

- Faites un inventaire de vos biens précieux

- Photo de vos biens pour les assurances
- Surveillance à distance, caméra de sécurité
- Se garder en santé, mise en forme, qualité alimentaire

Mode numérique

- Activez le mot de passe sur les équipements
- Ne consultez pas de liens inconnus
- Ayez une réserve sur le contenu disponible sur Internet, risque de partager un lien infecté
- Faites un inventaire des vos données précieuses, secrets industriels, données personnelles
- Copie de sécurité de vos données
- Accès à distance sécuritaire par un VPN

- Mise à jour de sécurité de vos équipements

SERVICES INFORMATIQUES

Ingénierie sociale, soyez un maillon fort !

- Les ingénieurs sociaux visent vos émotions
  - Développer un sentiment d'urgence
  - Cupidité, l'appât du gain
  - Curiosité, est-ce-que c'est vous sur cette photo
  - Sensibilité, désir de rendre service
- Garder en tête que les ingénieurs sociaux misent sur notre désir naturel d'aider autrui. Si une demande éveille vos soupçons, fiez-vous à votre intuition.
- Faites preuve de vigilance en ce qui a trait à tout courriel non sollicité, notamment ceux qui demandent un changement de mot de passe ou de confirmer vos renseignements personnels.
- Confirmer toujours l'identité de la personne et la légitimité de sa demande avant de divulguer des renseignements personnels ou information confidentielle.

SERVICES INFORMATIQUES

Soyez à l'affût des messages d'hameçonnage et de harponnage

- Sachez reconnaître les messages qui sont des tentatives d'hameçonnage ou de harponnage:
  - Hameçonnage, on vise tout le monde ou va à la pêche aux poissons
  - Harponnage, vos êtes la baleine et on vous vise directement, ingénierie sociale
- Méfiez-vous des liens suspects, ne cliquez jamais dessus.
- Vous pouvez ouvrir une porte d'entrée à un rançongiciel.

SERVICES INFORMATIQUES

Le déroulement d'une attaque par hameçonnage

1. Une fois que vous avez cliqué sur le lien, l'attaquant va installer un ver infecté sur votre système
2. Il va répliquer ce ver vers d'autres équipements pour se rendre plus résilient
3. Il va établir une communication IP vers son centre de contrôle
4. Il ne vous connait pas, donc il va vous étudier
5. Recherche d'information personnelless, se vend sur le darkweb
6. Recherche de secrets professionnels, plans et devis, procédures opérationnelles, les chinois achètent
7. Recherche de données financières pour évaluer le montant de la rançon
8. Crypter les données trouvées qui ont de la valeur pour votre entreprise
9. Attendre votre réaction
10. L'attaquant va prendre son temps. Il n'est pas pressé. Cela peut durer plus de 200 jours.

ML SERVICES INFORMATIQUES

Les 3 piliers de votre cybersécurité

Voici 3 piliers pour vous protéger

- 1 MDR Managed Detection & responses
- 2 MFA Authentification multi-facteurs
- 3- Sauvegarde et continuité BCDR
  Business Continuity and Dasacster Recevery

ML SERVICES INFORMATIQUES

Les 3 piliers de votre cybersécurité

- 1 MDR Managed Detection & responses
- C’est une évolution de l’antivirus conventionnel
- Le MDR effectue 5 actions
    1. Identifie une possibilité d’attaque
    2. Protège l’équipement visé par l’attaque (antivirus)
    3. Détecte le type d’attaque
    4. Répond à ce type d’attaque pour la neutraliser
    5. Retourne à un état stable de production
- Le MDR utilise l’intelligence artificielle et l’infonuagique pour offrir cette protection

ML SERVICES INFORMATIQUES

Les 3 piliers de votre cybersécurité

- 2 MFA Authentification multi-facteurs

- Méthode d'authentification qui oblige l'utilisateur à un minimum de deux facteurs de vérification pour accéder à une ressource de l'entreprise
- Mot de passe = qui je suis (insuffisant si seul)
- Mot de passe + MFA = prouver qui je suis
- Exemple, envoie un code aléatoire par SMS sur votre téléphone et vous devez le fournir à la ressource
- Protection efficace des menaces par Hameçonnage et Harponnage

SERVICES INFORMATIQUES

Les 3 piliers de votre cybersécurité

- 3- Sauvegarde et continuité BCDR
  Business Continuity and Disaster Recovery

- Type de solutions utilisées pour aider une organisation à se remettre d'un sinistre et à poursuivre ou reprendre ses opérations courantes et ce, le plus rapidement possible
- Résolution à des problèmes de disponibilité et d'intégrité
- Réduction des impacts lors d'incidents
- Prioriser les solutions CLOUD (isolé, meilleure redondance, plus flexible, …)
- Exemple Office 365 utilisé pendant la pandémie

ML SERVICES INFORMATIQUES

Vos questions

SERVICES INFORMATIQUES

Simplement efficace