Guide de bonne pratique contre le rançongiciels

GUIDE ANSIE

Sommaire

1. Introduction 2
2. Secteurs à haut risque 3
2.1. IT 3
2.2. Les administration Publique 3
2.3. Les secteurs de santé 3
2.4. Services financiers 4
3. Rançon : Payer ou ne pas Payer ? 5
4. Vecteurs d'attaque initiaux 6
4.1. la compromission du RDP 6
4.2. Spear phishing 7
4.3. Vulnérabilités des logiciels 7
4.4. Téléchargement furtif "Drive-by Download" 7
5. Comment prévenir les attaques par ransomware 8
5.1. Sauvegardes régulières du système 8
5.2. Formation et sensibilisation 8
5.3. Sécurisation du mot de passe 9
5.4. Segmentation du réseau 9
6. Conclusion 11

1. Introduction

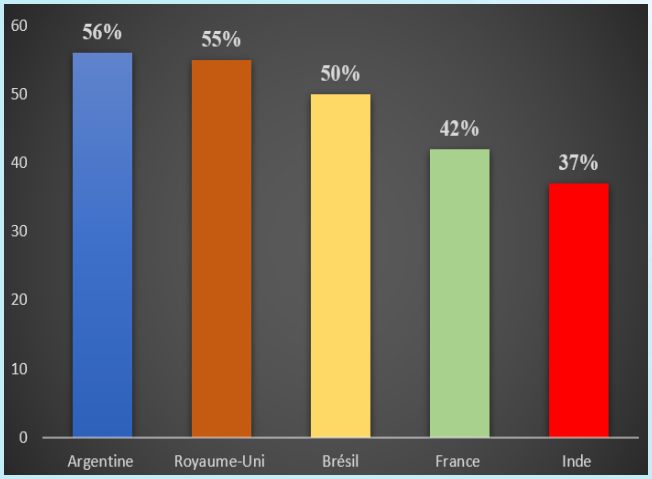
Un ransomware est un type de logiciel malveillant qui crypte les fichiers d'un ordinateur, bloquant ainsi les utilisateurs jusqu'à ce qu'une rançon soit payée à un cybercriminel, généralement en bitcoins.

Les attaques par ransomware sont devenues de plus en plus courantes pour trois raisons :

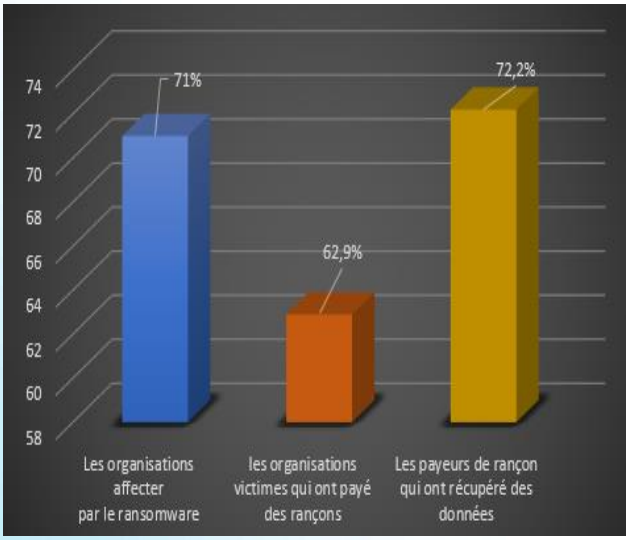
- ✓ Leur lancement nécessite peu d'expertise technique. peuvent même acheter des paquets de "ransomware-as- a-service" sur des dark web
- ✓ Contrairement aux violations de données, où les cybercriminels doivent d'abord voler des données, puis trouver des acheteurs consentants, les ransomwares sont presque immédiats.
- ✓ En 2022, 71 % des entreprises dans le monde ont été touchées par un ransomware. Selon une enquête menée auprès de professionnels mondiaux de l'informatique, environ 72 % des personnes interrogées ont payé la rançon et récupéré les données compromises. Au total, 62,9 % des victimes d'attaques par ransomware ont payé la rançon.

Globalement, 71 % des professionnels interrogés ont déclaré que leur organisation avait été touchée par un ransomware.

Après des mois de déclin, les attaques mondiales de ransomware ont augmenté de manière significative au cours du Q2/2022, soit une hausse de 24 % par rapport au trimestre précédent.



Augmentation de Ransomware de manière significative au cours du Q2/2022



des victimes ont cédé aux demandes de rançon en 2022

> *Une nouvelle attaque a lieu toutes les 14 secondes environ.*

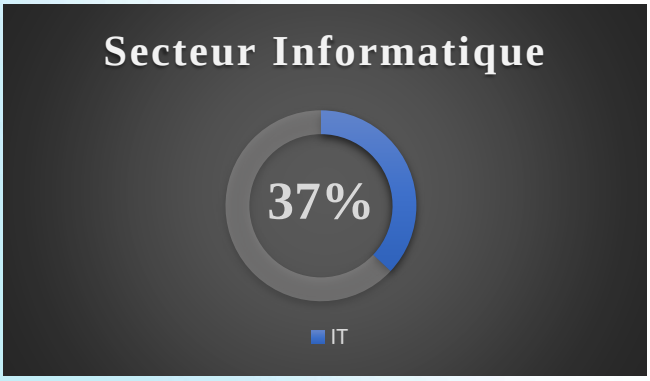
2. Secteurs à haut risque

Lorsque les rançongiciels ont fait leur apparition, les victimes étaient généralement de très grandes entreprises, le raisonnement étant que ces victimes avaient les poches assez profondes pour payer les demandes de rançon. Cependant, les grandes entreprises pouvaient également se permettre de renforcer leurs défenses de sécurité pour prévenir les attaques futures.

En gardant tout cela à l'esprit, voici les 4 principales cibles des ransomwares :

2.1. IT

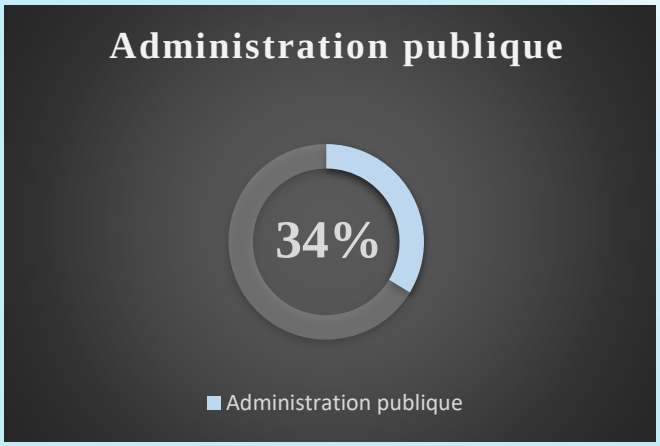
Au début de l'année 2021, le gang de ransomware REvil a compromis le réseau du fabricant taïwanais de PC Acer et a formulé l'une des plus importantes demandes de rançon jamais enregistrées : 50 millions de dollars. On ignore si la société a payé la rançon. Parmi les autres cibles récentes de ransomware dans le secteur informatique, citons le fabricant d'ordinateurs portables Apple Quanta Computer, le fournisseur de technologies d'inspection de véhicules Applus Technologies, le fournisseur de stockage de sauvegarde ExaGrid et le fournisseur de logiciels Kaseya.



2.2. Les administration Publique

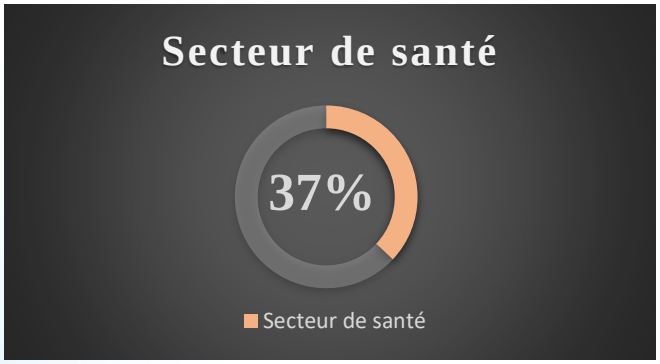
Les données gouvernementales finissent par être volées à des fins de gain financier ou d'espionnage. Les acteurs malveillants peuvent attaquer les bases de données gouvernementales pour obtenir des informations stratégiques.

Certaines brèches peuvent révéler des emails de responsables gouvernementaux qui contiennent des informations stratégiques ou secrètes.



2.3. Les secteurs de santé

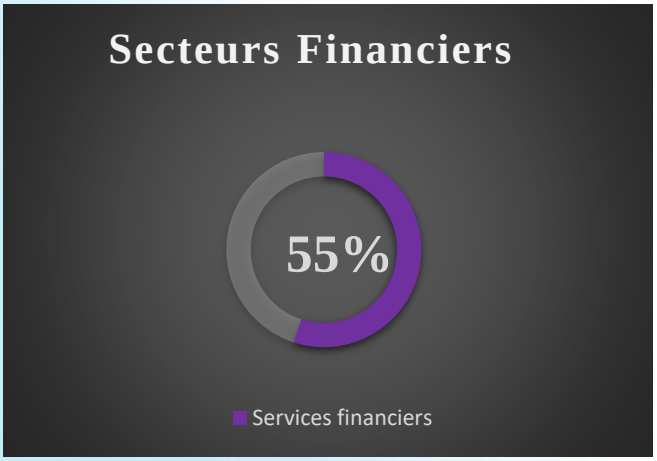
Les attaques de ransomware ont touché plus de 1 200 établissements de santé américains en 2021. Le centre fédéral de coordination de la cybersécurité du secteur de la santé, qui fait partie du département de la santé et des services sociaux, a dénombré 82 incidents distincts de ransomware dans le secteur mondial de la santé au cours des seuls cinq premiers mois de l'année.



2.4. Services financiers

Malheureusement, les attaques dans ce secteur semblent monter en flèche. 55% des organisations de services financiers ont été touchées par un ransomware en 2021, contre 34 % en 2020.

Il s'agit d'une augmentation de 62 % en un an, ce qui montre que les adversaires sont devenus considérablement plus capables d'exécuter des attaques à grande échelle.



> *Tout le monde est une cible potentielle de ransomware*

3. Rançon : Payer ou ne pas Payer ?

L'opportunité de payer une rançon fait l'objet d'un grand débat, même parmi les professionnels de la cybersécurité, certains professionnels de la sécurité affirment que les coûts de la rançon peuvent être bien inférieurs aux coûts de récupération des données, en particulier pour les PME qui ne peuvent pas se permettre une interruption prolongée.

Dans les établissements de santé et les organismes publics, les temps d'arrêt peuvent mettre en danger la santé et la vie des personnes.

D'autres professionnels de la sécurité, ainsi que la plupart des organismes chargés de l'application de la loi, affirment que le paiement de rançons ne fait qu'encourager de futures attaques et que le paiement ne garantit pas la restauration. Si la plupart des organisations qui paient récupèrent effectivement leurs données, environ 20 % d'entre elles ne le font pas. De plus, dans les cas de double extorsion, les cybercriminels sont toujours en possession des données volées. Même s'ils ont promis de détruire les données après avoir reçu la rançon, ils peuvent toujours les vendre, les rendre publiques ou les utiliser comme base pour de futures attaques, telles que la compromission de la messagerie professionnelle (BEC :Business Email compromise).

> *Compte tenu des risques encourus, la meilleure solution consiste à empêcher les attaques par ransomware de se produire*

4. Vecteurs d'attaque initiaux

Toute attaque commence par un accès initial. Il peut s'agir d'un accès au réseau interne via un VPN, d'un cheval de Troie délivré par spear phishing, d'un shell web déployé via l'exploitation d'une application publique.

Dans le même temps, les trois vecteurs d'attaque initiaux les plus courants sont la compromission du RDP, le spear phishing et l'exploitation des vulnérabilités logicielles.

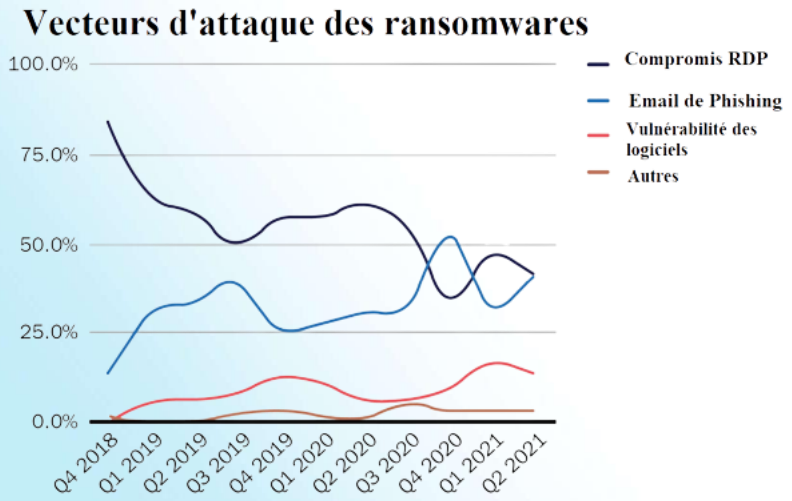


figure1 : les trois vecteurs d'attaque initiaux les plus courants

4.1. la compromission du RDP

Pendant de nombreuses années, RDP est resté le moyen le plus courant pour les acteurs de la menace d'accéder au réseau cible.

La pandémie a encore aggravé la situation, car de nombreuses entreprises ont dû penser à offrir à leurs employés la possibilité de travailler à distance. Un nombre encore plus grand de serveurs ont donc été exposés à l'internet et, bien sûr, sont devenus la cible d'acteurs de menaces de toutes sortes, notamment d'opérateurs de ransomware.

Figure2 : Le nombre de dispositifs avec le port 3389 exposés à l'internet

4.2. Spear phishing

Le spear phishing, c'est-à-dire l'utilisation de l'ingénierie sociale pour inciter les utilisateurs ciblés à ouvrir des pièces jointes malveillantes ou à cliquer sur des liens. Cette technique est utilisée par les acteurs de la menace pour recueillir des informations d'identification.

Il est vrai que de nombreux acteurs de la menace qui, à l'époque, utilisaient ces logiciels malveillants principalement pour la fraude bancaire, les utilisent désormais aussi pour obtenir un accès initial aux réseaux d'entreprises.

4.3. Vulnérabilités des logiciels

Les vulnérabilités logicielles ont permis à de nombreux courtiers en accès initial de gagner des centaines de milliers de dollars, mais les affiliés des programmes de ransomware-as-a-service ont gagné encore plus - **des millions**.

Bien entendu, toutes les vulnérabilités ne permettent pas à un acteur de la menace d'obtenir un accès initial au réseau. Le plus souvent, il s'agit de vulnérabilités qui permettent l'exécution de code à distance ou l'exposition de fichiers contenant des informations d'identification.

Enfin, dans certains cas, les acteurs de la menace parviennent à utiliser même des vulnérabilités de type "zero-day", c'est-à-dire des vulnérabilités dans des systèmes ou des dispositifs qui ont été divulguées mais pas encore corrigées.

4.4. Téléchargement furtif “Drive-by Download”

Une attaque par téléchargement Furtif consiste à télécharger involontairement un code, un fichier ou un logiciel malveillant sur un ordinateur ou un appareil mobile. Les cybercriminels peuvent utiliser ces téléchargements pour recueillir vos informations personnelles, vous espionner, injecter des chevaux de Troie bancaires ou infecter tout votre réseau avec des logiciels malveillants.

se produit lorsqu'un utilisateur visite sans le savoir un site web infecté où un logiciel malveillant est téléchargé et installé à son insu.

5. Comment prévenir les attaques par ransomware

Les logiciels antivirus et la plupart des systèmes de gestion des identités et des accès ne font pas grand-chose pour protéger les entreprises contre les ransomwares.

5.1. Sauvegardes régulières du système

Les sauvegardes régulières du système sont essentielles, non seulement pour récupérer les données après un incident de ransomware ou une autre cyber attaque, mais aussi après des pannes du système et des dommages au matériel après des catastrophes naturelles. Cependant, les sauvegardes ne sont pas une solution-miracle, car les variantes de ransomware de nouvelle génération recherchent et cryptent les fichiers de sauvegarde avant d'attaquer le reste du réseau.

Il existe différents types de sauvegardes que vous pouvez mettre en place pour protéger les informations de votre organisation :

- ✓ Sauvegarde complète : Vous souhaiterez peut-être effectuer une sauvegarde complète de façon périodique (hebdomadaire ou mensuelle) et avant toute mise à niveau importante du système.
- ✓ Sauvegarde différentielle : Une sauvegarde différentielle crée uniquement une copie des données qui ont changé depuis votre dernière sauvegarde complète.
- ✓ Sauvegarde incrémentielle : Avec les sauvegardes incrémentielles, vous ne stockez que les données qui ont changé depuis votre dernière sauvegarde complète ou différentielle.

5.2. Formation et sensibilisation

Étant donné que de nombreuses charges utiles de ransomware sont livrées dans des courriels de phishing, la formation des employés pour éviter les escroqueries par phishing est une autre étape essentielle de la prévention de l'infection. Cependant, tout comme les sauvegardes du système, ce n'est pas une solution-miracle. Les attaques par force brute ont dépassé le phishing pour devenir la méthode la plus courante de transmission des ransomwares. de livraison de ransomware.

> *La défense contre les ransomwares nécessite une approche proactive sur plusieurs fronts*

5.3. Sécurisation du mot de passe

Les mots de passe faibles et compromis sont la plus grande menace la cybersécurité des organisations. En plus d'alimenter les attaques par force brute qui sont la méthode la plus courante de livraison des ransomwares, les mauvaises habitudes des employés en matière de mots de passe sont à l'origine de la grande majorité des violations de données.

Dans une attaque par force brute, les cybercriminels obtiennent une liste de mots de passe volés lors d'une violation de données, puis tentent de les utiliser pour compromettre des serveurs et des terminaux, généralement à l'aide de robots. Étant donné qu'un grand nombre d'utilisateurs utilisent des mots de passe faibles, courants et faciles à deviner, et qu'ils réutilisent les mêmes mots de passe d'un compte à l'autre. sont très efficaces. Les attaques par force brute peuvent être évitées en demandant aux employés d'utiliser des mots de passe forts et uniques pour tous les comptes, d'utiliser l'authentification multifactorielle (2FA) sur tous les comptes qui le permettent et d'utiliser un gestionnaire de mots de passe.

5.4. Segmentation du réseau

Sans segmentation du réseau, les mouvements latéraux au sein d'un réseau sont extraordinairement simples. *Le mouvement latéral désigne les techniques utilisées par un cyberattaquant, après avoir obtenu un accès initial, pour s'enfoncer plus profondément dans un réseau à la recherche de données sensibles et d'autres actifs de grande valeur*. La segmentation du réseau divise le réseau, empêchant ce mouvement latéral, et donc l'accès aux données sensible. Au lieu d'un seul périmètre de sécurité autour de l'ensemble du réseau, **vous avez essentiellement mis en place plusieurs périmètres de sécurité au sein du réseau**.

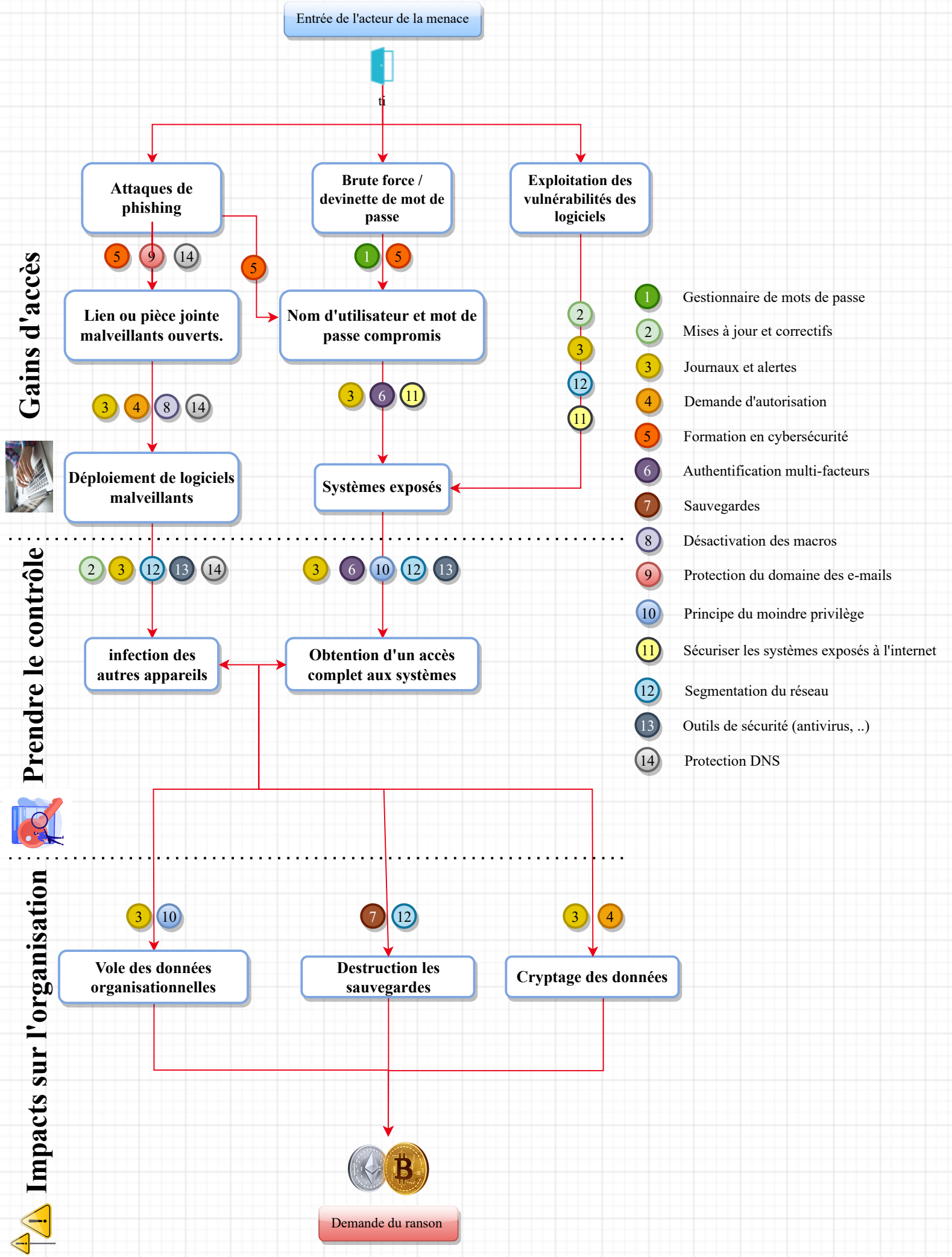


Figure3 : Contrôles de sécurité pour réduire le risque de ransomware

6. Conclusion

Les rançongiciels constituent une menace constante pour votre organisation. Ils peuvent avoir des effets dévastateurs sur votre activité, en interrompant souvent votre capacité à produire des produits et des services. Les incidents liés aux ransomwares peuvent également entraîner des pertes financières, des violations de données et des atteintes à la réputation de votre organisation. La préparation de votre organisation et l'application de mesures proactives pour protéger votre réseau, vos appareils connectés et vos informations sont essentielles pour votre capacité à répondre aux ransomwares et à vous en remettre.