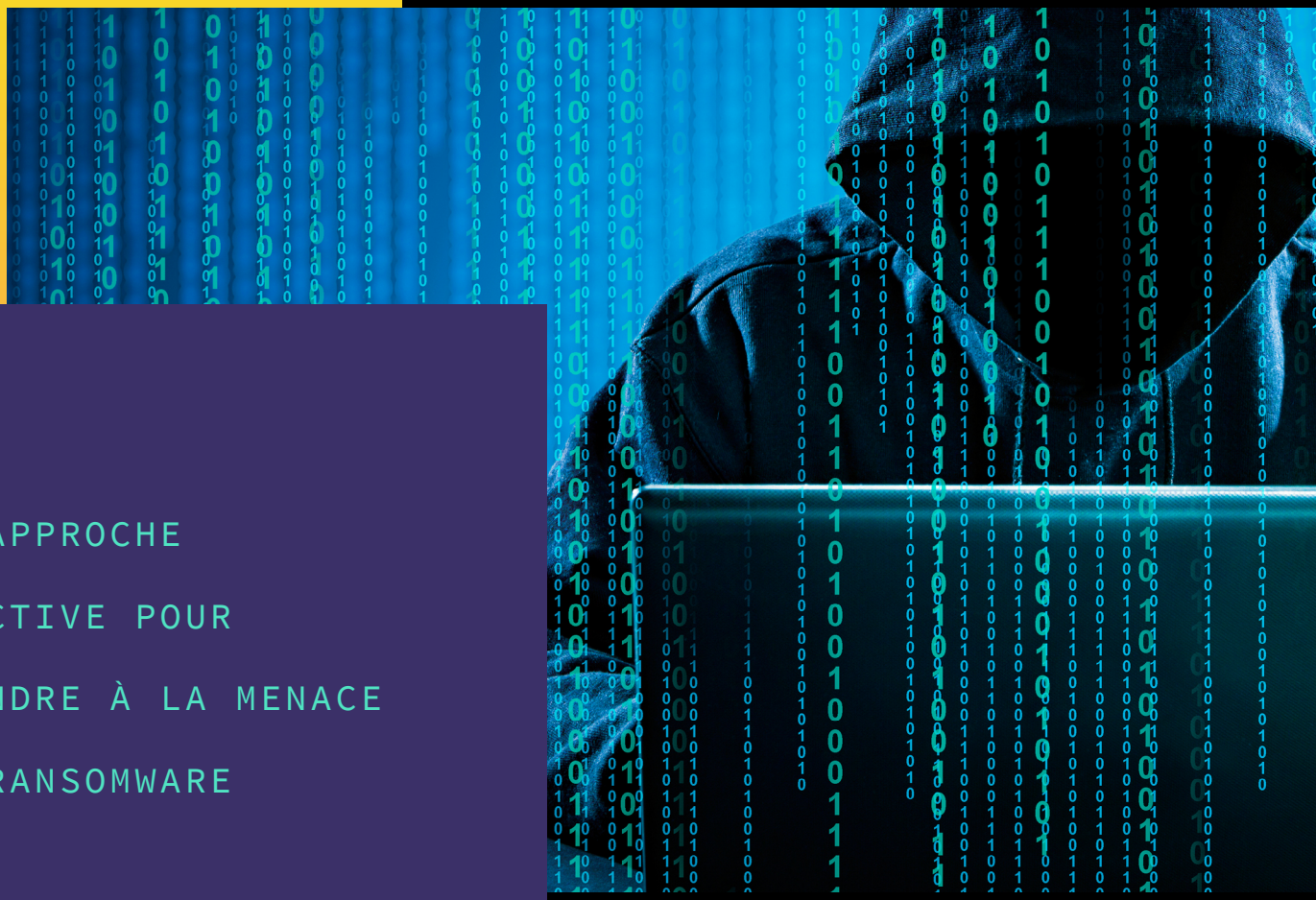
arcserve®

Protéger ce qui n'a pas de prix

ÉVALUATION DE VOTRE PRÉPARATION EN MATIÈRE DE RANSOMWARE



UNE APPROCHE PROACTIVE POUR RÉPONDRE À LA MENACE DES RANSOMWARE

ÉVALUATION

MESUREZ VOS CAPACITÉS ET ÉLABOREZ VOTRE FEUILLE DE ROUTE POUR UN AVENIR SANS RANSOMWARE

Le ransomware est devenu l'un des plus grands risques pour les entreprises et constitue la menace la plus importante pour les organisations informatiques. Ce phénomène a atteint des proportions dignes d'une épidémie mondiale, dont les coûts estimés pourraient atteindre 20 milliards de dollars d'ici 2021[1].
La gestion de la sécurité des informations est essentielle à une bonne gouvernance des systèmes informatiques, en particulier en ce qui concerne la protection des données personnelles et d'entreprise critiques contre les ransomware.
Ce guide d'évaluation peut vous aider à identifier rapidement les lacunes de vos systèmes informatiques et à composer votre feuille de route vers un avenir sans ransomware.

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

SCORE DE MATURITÉ EN MATIÈRE DE RANSOMWARE

Instructions

Mener à bien l'évaluation à l'aide de la fiche ci-dessous du **Modèle de maturité des capacités**[2] (CMM). Cette fiche fournit un parcours évolutif à cinq niveaux de processus de plus en plus organisés et systématiquement plus matures. Pour chacun des éléments du cadre sans rançongiciels, vous pouvez évaluer le score de maturité de votre organisation et réfléchir à vos priorités.

Score de maturité	Niveau de maturité	Description
0	Absence	Aucune preuve que l'action est en place au sein de l'organisation.
1	Informé	Connaissance limitée de l'action, avec des processus et procédures informels en place.
2	Reproductible	Un programme d'action de base est en place avec des documents d'appui.
3	Normalisé	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs définis.
4	Maîtrisé	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs, et les écarts sont gérés au sein de l'organisation en fonction de l'importance pour l'entreprise.
5	Opérationnel	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs, et les écarts sont gérés au sein de l'organisation en fonction de l'importance pour l'entreprise. Des examens réguliers valident que les objectifs fixés sont atteints.

2 Le modèle de maturité des capacités (Capability Maturity Model, CMM) a été conçu par le Software Engineering Institute (SEI) du Département de la Défense des États-Unis en 1986, à l'Université de Carnegie Mellon située à Pittsburgh en Pennsylvanie.

Cochez la case correspondant au profil de votre entreprise.

1 Gérer activement les accès

Une gestion efficace des accès et des contrôles sur l'ensemble de notre portefeuille de produits est-elle actuellement en place ?

ACTION	ABSENCE	INFORMÉ	REPRODUCTIBLE	NORMALISÉ	MAÎTRISÉ	OPÉRATIONNEL
Limiter l'accès aux points d'entrée courants des ransomware, tels que les comptes de messagerie personnels et les sites de réseaux sociaux, et utiliser un filtrage Web au niveau de la passerelle et du point de terminaison afin de bloquer les tentatives d'hameçonnage pour les utilisateurs qui sont invités à cliquer sur un lien.						
Utiliser des règles d'authentification et de mot de passe à facteurs multiples et inclure des critères de mot de passe lorsque les utilisateurs communiquent avec des sites Web non classés par le proxy ou le pare-feu.						
Utiliser des serveurs de proxy et des logiciels de blocage des publicités et limiter les autorisations pour installer et exécuter des applications logicielles.						
Contrôler et surveiller les parties tierces qui disposent d'un accès distant au réseau de l'organisation et vos connexions avec les tiers afin de s'assurer qu'ils appliquent les pratiques recommandées en matière de cybersécurité.						
Utiliser une liste blanche d'applications afin d'autoriser uniquement l'exécution de programmes autorisés sur un réseau.						

2 Gérer la configuration des systèmes pour l'ensemble des vecteurs d'infection

Avons-nous élaboré une gestion centralisée et une approche de bout en bout destinées à lutter contre toutes les attaques potentielles ?

ACTION	ABSENCE	INFORMÉ	REPRODUCTIBLE	NORMALISÉ	MAÎTRISÉ	OPÉRATIONNEL
Évaluer et classer les données sensibles de l'entreprise et mettre en place une séparation physique et logique des serveurs, réseaux et banques de données.						
Veiller à ce que des solutions antivirus et anti- logiciels malveillants soient configurées pour se mettre à jour automatiquement et analyser les messages entrants et sortants afin de détecter un possible hameçonnage, d'empêcher l'usurpation d'adresses électroniques et de filtrer les fichiers exécutables.						
Utiliser un système centralisé de gestion des correctifs permettant de corriger tous les points de terminaison au fur et à mesure que des vulnérabilités sont découvertes, y compris sur les appareils mobiles, systèmes d'exploitation, logiciels et applications, emplacements cloud et l'Internet des objets.						
Déployer des technologies anti-attaque, anti-rançongiciel et Deep Learning sans signature, capables de détecter des logiciels malveillants connus et non connus.						
Déployer des technologies intégrées de protection de point de terminaison et de continuité de l'activité afin d'accélérer la prévention des menaces et d'activer la restauration immédiate des données.						
Sécuriser les applications et serveurs Web au moyen de pare-feux d'applications Web.						
Désactiver les scripts des fichiers Microsoft Office envoyés par e-mail et envisager d'utiliser le logiciel Office Viewer pour ouvrir des fichiers Office.						
Contrôler votre réseau afin de rechercher les systèmes qui utilisent le protocole RDP (Remote Desktop Protocol) en fermant les ports inutilisés, au moyen d'une authentification à deux facteurs.						
Détecter et diagnostiquer les comportements, tels que le chiffrement de fichiers de masse, ainsi que les comportements malveillants et de blocage.						
Utiliser des systèmes de gestion unifiée des menaces (Unified Threat Management ou UTM) qui combinent un pare-feu, un anti-virus de passerelle et des capacités de prévention et de détection des intrusions afin de bloquer l'accès aux adresses IP malveillantes connues.						

3 Combiner des solutions de sécurité et de protection des données

Notre configuration informatique offre-t-elle une solution complète de protection de point de terminaison, de disponibilité des données et de cybersécurité ?

ACTION	ABSENCE	INFORMÉ	REPRODUCTIBLE	NORMALISÉ	MAÎTRISÉ	OPÉRATIONNEL
Protéger les espaces de sauvegarde contre les logiciels malveillants, les rançongiciels et les attaques zero-day.						
Arrêter et supprimer des sauvegardes les menaces telles que les logiciels malveillants et les ransomwares.						
Conserver les sauvegardes des données sur des dispositifs distincts et utiliser des espaces de stockage hors ligne lorsque ceux-ci peuvent être la cible directe de dispositifs infectés.						
Sauvegarder les machines virtuelles, les espaces de stockage dans le cloud et les systèmes opérationnels en fonction des objectifs de point de récupération, en estimant le niveau de perte de données acceptable en cas de défaillance.						
Utiliser un système permettant de sauvegarder plusieurs itérations des sauvegardes, dans le cas où une copie des sauvegardes inclut des fichiers cryptés ou infectés.						
Intégrer des dispositifs de récupération après sinistre et de disponibilité des applications et tirer profit de l'intelligence artificielle pour assurer une protection de point de terminaison.						
Utiliser l'analyse des vulnérabilités, le chiffrement SSL et d'autres contrôles techniques afin de confirmer que les sauvegardes sont en cours.						
Utiliser la règle 3-2-1 et créez trois copies de vos données, en les stockant sur deux supports différents, dont un hors site.						
Tester régulièrement les sauvegardes afin de s'assurer de l'intégrité des données et de garantir						
Tester régulièrement les processus de récupération des données et de récupération après sinistre afin de s'assurer qu'ils sont prêts.						

4 Impliquer les utilisateurs dans des formations et communications

Donnons-nous à nos utilisateurs les méthodes dont ils ont besoin pour se protéger contre les menaces des ransomwares ?

ACTION	ABSENCE	INFORMÉ	REPRODUCTIBLE	NORMALISÉ	MAÎTRISÉ	OPÉRATIONNEL
Proposer régulièrement des formations et communications de sensibilisation, de sorte que chaque personne au sein de votre organisation comprenne la menace que représente les rançongiciels et connaisse les techniques sécuritaires.						
Établir des politiques et procédures de prévention contre les ransomware destinées aux utilisateurs finaux.						
Inviter les utilisateurs à ne pas ouvrir les e-mails suspects ou les pièces jointes, ni à cliquer sur les liens douteux, et à faire preuve de prudence lors de l'ouverture de sites Web non connus, ainsi qu'à fermer son navigateur après utilisation.						
Veiller à ce que les employés sachent comment et à qui signaler toute activité suspecte.						

5 Tenir à jour et tester un plan de continuité de l'activité et de récupération après sinistre

Sommes-nous en mesure de récupérer des applications et des données opérationnelles à la suite d'un sinistre ?

ACTION	ABSENCE	INFORMÉ	REPRODUCTIBLE	NORMALISÉ	MAÎTRISÉ	OPÉRATIONNEL
Mettre en place des plans de contingence et de résolution essentiels pour la récupération et la continuité de l'activité, quelle que soit la source du dysfonctionnement.						
Mener une évaluation des risques qui permette de classer les types de sinistres susceptibles de survenir, et établir des priorités en matière de récupération et de continuité de l'activité.						
Déployer des solutions de récupération après sinistre, de sauvegarde et de haute disponibilité, sur site et hors site.						
Élaborer un plan d'intervention en cas d'incident indiquant les mesures à prendre en présence d'un ransomware, notamment déconnecter le système infecté du réseau afin d'empêcher la propagation de l'infection et déterminer le niveau de sensibilité des données.						
Tester le plan, y compris les dispositifs et systèmes technologiques, afin de s'assurer qu'une protection complète est en place.						
Signaler toute infection aux autorités concernées.						

RÉSUMÉ DE L'ÉVALUATION

En tenant compte des cinq pratiques relatives à la protection contre les ransomware, dans quelle mesure sommes-nous prêts pour un avenir sans ransomware ?

Score de maturité	Niveau de maturité	Description	Quel est notre niveau de maturité global ?
0	Absence	Aucune preuve que l'action est en place au sein de l'organisation.	
1	Informé	Connaissance limitée de l'action, avec des processus et procédures informels en place.	
2	Reproductible	Un programme d'action de base est en place avec des documents d'appui.	
3	Normalisé	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs définis.	
4	Maîtrisé	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs, et les écarts sont gérés au sein de l'organisation en fonction de l'importance pour l'entreprise.	
5	Opérationnel	Le programme d'action est déployé à l'échelle de l'organisation avec un langage, des définitions, des responsabilités et des rôles communs, et les écarts sont gérés au sein de l'organisation en fonction de l'importance pour l'entreprise. Des examens réguliers permettent de valider que les objectifs fixés sont atteints.	

Quelles sont les étapes suivantes ?

PARLEZ Á UN EXPERT DANS LE DOMAINE DES RANSOMWARE

Explorez les meilleures pratiques en matière de ransomware et laissez nos experts vous aider à identifier les lacunes potentielles pour pouvoir entrevoir un avenir sans ransomware. **Organisez une consultation.**

Pour en savoir plus sur Arcserve, **visitez le site** arcserve.com/fr