SOPHOS

Les bonnes pratiques de protection Endpoint pour bloquer les ransomwares

Des conseils pratiques pour configurer votre solution Endpoint de manière optimale.

Un livre blanc Sophos. Octobre 2024

Introduction

Les ransomwares figurent parmi les cybermenaces les plus importantes, avec des conséquences de grande ampleur et souvent catastrophiques. 59 % des personnes interrogées dans le cadre de l'enquête « L'état des ransomwares 2024 » de Sophos ont déclaré que leur organisation avait été victime d'un ransomware au cours de l'année écoulée. Dans 70 % de ces incidents, les données ont été chiffrées par les attaquants.

Le coût moyen de remédiation d'une attaque de ransomware s'élève à 2,73 millions de dollars, soit une augmentation de 50 % par rapport à l'année précédente. Qui plus est, plus d'un tiers (34 %) des organisations ont mis plus d'un mois à se rétablir après une attaque, ce qui témoigne de la complexité et de la gravité croissantes de ces incidents.

L'allongement des délais de rétablissement met en évidence la nécessité de déployer des efforts de réponse plus complets. Cette complexité croissante n'est pas sans poser des problèmes aux équipes de sécurité internes, puisque 95 % des entreprises déclarent rencontrer des difficultés pour mener à bien leurs opérations de sécurité de base[1].

Ces observations montrent combien il est crucial pour les organisations de renforcer leurs défenses contre les ransomwares, ainsi que leurs stratégies de rétablissement. En effet, l'augmentation des coûts, l'allongement des temps de rétablissement et la pression croissante exercée sur les équipes de sécurité font des ransomwares une menace redoutable pour la continuité des activités. Une solution de protection Endpoint correctement configurée est l'un des moyens de défense les plus efficaces contre les ransomwares. Ce livre blanc examine les mécanismes des attaques de ransomware, les stratégies pour les prévenir et les bonnes pratiques pour optimiser votre protection Endpoint, afin d'assurer une sécurité maximale.

Méthodes de déploiement des attaques de ransomware

Il existe autant d'acteurs malveillants que de types d'attaques de ransomware différents. Certaines attaques sont très ciblées, tandis que d'autres sont plus opportunistes. Bien souvent, les adversaires (aussi appelés cybercriminels ou attaquants) analysent les réseaux pour trouver des failles ou des vulnérabilités qui leur permettront d'accéder à votre environnement. Voici pour preuve les propos tenus par un gang de ransomwares ayant attaqué un établissement scolaire au Canada :

> *« Vous aviez une ancienne vulnérabilité critique Log4j non corrigée sur Horizon, c'est ainsi que nous avons pu pénétrer initialement. Il s'agissait d'un scan effectué en masse ; on ne vous visait pas spécialement. »*

Ces propos mettent également en évidence l'exploitation courante par les attaquants de vulnérabilités non corrigées, qui a été la principale cause première des attaques de ransomware en 2024.[2]

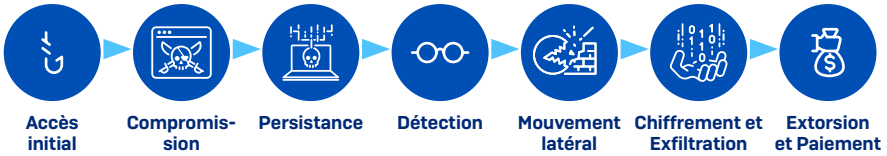
La hausse des attaques de ransomware au cours des dernières années peut être attribuée en grande partie à l'essor du modèle RaaS ou Ransomware-as-a-Service. Depuis l'avènement du modèle RaaS, un groupe de cybercriminels peut créer un ransomware et le louer à d'autres adversaires. Cela rend les ransomwares accessibles à un plus grand nombre d'acteurs malveillants que jamais.

Dès lors que ces derniers accèdent à l'environnement de leurs victimes, ils passent alors plusieurs jours, plusieurs semaines, voire plusieurs mois à explorer le réseau, à élever leurs privilèges, à exfiltrer des données ou à installer des malwares. En 2023, le temps de séjour moyen d'une attaque de ransomware était de six jours[3]. Ce délai laisse aux défenseurs la possibilité d'identifier et d'arrêter les intrus avant qu'ils ne mènent à bien leur attaque.

1 Remédier à la pénurie de compétences en cybersécurité dans les PME — Sophos

2 L'état des ransomwares 2024 - Sophos
3 Le rapport Sophos Active Adversary du premier semestre 2024 — Sophos

Mode opératoire classique d'une attaque de ransomware :



Il faut savoir que les adversaires attaquent stratégiquement leurs cibles à des moments où ils ont moins de chances d'être détectés. Les attaques de ransomware se déroulent le plus souvent le vendredi ou le samedi, les auteurs misant sur une moindre surveillance des systèmes d'information pendant le week-end.

L'analyse des experts en réponse aux incidents de Sophos X-Ops montre par ailleurs que 43 % des attaques de ransomware en 2023 ont été lancées les samedi et dimanche, et que 91 % des attaques ont commencé en dehors des heures de bureau habituelles (de 8 h à 18 h, du lundi au vendredi) dans le fuseau horaire de la victime[4].

Ransomwares distants

Selon le rapport de défense numérique 2023 de Microsoft, environ 60 % des attaques de ransomwares pilotées manuellement reposent sur le chiffrement à distance. Aussi appelé 'ransomware distant', un chiffrement à distance survient lorsqu'un poste compromis est utilisé pour chiffrer des données sur d'autres appareils du même réseau.

L'un des facteurs clés de l'utilisation de plus en plus répandue de cette méthode est son évolutivité. De fait, un poste non géré ou sous-protégé risque d'exposer l'ensemble de l'organisation à un chiffrement à distance malveillant, même si d'autres appareils sont protégés par des solutions de sécurité avancées.

Les entreprises ont tout intérêt à être attentives à la menace posée par les attaques de ransomware distant, d'autant plus que toutes les solutions de sécurité Endpoint ne permettent pas de se protéger efficacement contre ces menaces.

4 Comment stopper les adversaires actifs : les leçons tirées de la ligne de front de la cybersécurité — Sophos

Protocole RDP ou Protocole de Déploiement de Ransomware ?

Le protocole RDP (Remote Desktop Protocol) a joué un rôle dans 90 % des cyberattaques prises en charge par l'équipe de réponse aux incidents de Sophos en 2023, contre 83 % l'année précédente[5].

Si le RDP et les outils de partage de bureau comme Virtual Network Computing (VNC) sont très utiles pour gérer les systèmes à distance, en l'absence de mesures de protection adéquates, ces solutions peuvent être exploitées par les auteurs de ransomwares pour élever leurs privilèges, voler des identifiants, se déplacer latéralement, installer des portes dérobées, créer de faux comptes et échapper à la détection.

Il est donc essentiel d'empêcher les attaquants d'utiliser le RDP pour les accès externes, les accès internes et les mouvements latéraux. Malgré les progrès réalisés par les entreprises pour s'assurer que le RDP n'est pas exposé vers l'extérieur, les adversaires continuent d'utiliser ce protocole pour se déplacer sur le réseau de l'entreprise.

Bonnes pratiques de sécurité IT pour se protéger contre les ransomwares

Pour se protéger contre des menaces telles que des ransomwares, il ne suffit pas d'installer les solutions de cybersécurité les plus récentes. Il est indispensable d'adopter de bonnes pratiques de sécurité informatique, en particulier de bien former les employés de manière régulière. Assurez-vous de suivre cette liste des bonnes pratiques, en gardant en tête qu'elle n'est pas exhaustive.

1. Patchez au plus tôt et fréquemment

L'exploitation d'une vulnérabilité non corrigée constituait la cause principale des attaques de ransomware en 2024[6]. Les malwares et les adversaires exploitent les vulnérabilités de sécurité des applications les plus répandues. Plus vous appliquez tôt les correctifs à vos postes, serveurs, mobiles et applications, moins de failles pourront être exploitées par vos adversaires.[7]

5 Le rapport Sophos Active Adversary du premier semestre 2024 – Sophos
6 L'état des ransomwares 2024 - Sophos
7 Vulnérabilités non corrigées : le vecteur d'attaque de ransomware le plus agressif - Sophos

Le saviez-vous ?

Même si toutes les attaques de ransomware ont des conséquences négatives, celles qui commencent par l'exploitation de vulnérabilités non corrigées sont particulièrement agressives. Les organisations touchées par des attaques ayant commencé de cette manière ont signalé des coûts de rétablissement 4 fois plus élevés et des délais de rétablissement plus longs par rapport à celles ayant commencé avec des identifiants compromis.

2. Utilisez des mots de passe complexes

On ne le dira jamais assez : un mot de passe faible et prévisible peut permettre aux hackers d'accéder à votre réseau en quelques secondes. Nous recommandons de choisir des mots de passe uniques, composés d'au moins douze caractères, mêlant lettres majuscules et lettres minuscules, et d'ajouter une ponctuation aléatoire Ju5te.C0mM3çA!

3. Activez l'authentification multifacteur (MFA)

La MFA fournit une couche de sécurité supplémentaire au premier facteur d'authentification — qui consiste généralement en un mot de passe. Il est essentiel d'activer la MFA dans toutes les applications et tous les services qui la prennent en charge. Les adversaires achètent souvent des identifiants valides sur le Dark Web ou tentent activement d'obtenir ces informations lorsqu'ils ont réussi à pénétrer dans votre environnement. La MFA dresse un obstacle supplémentaire pour les adversaires en les empêchant de s'authentifier sans difficulté en tant qu'utilisateurs légitimes. Enfin, il est recommandé d'utiliser des clés d'accès résistantes au phishing, lorsque les applications le permettent.

4. Réglementez l'accès aux réseaux internes et externes

Ne laissez pas de ports réseau exposés. Verrouillez l'accès RDP et tous les autres protocoles de gestion à distance de votre organisation. Assurez-vous que les utilisateurs distants disposent d'une solution Zero-Trust Network Access (ZTNA) pour accéder aux applications, aux services et aux autres ressources de l'organisation.

5. Contrôlez les droits administrateur

Réexaminez constamment qui dans votre organisation a des droits d'administrateur local et domaine. Identifiez les personnes et retirez les droits de celles qui n'en ont pas besoin. Ne restez pas connecté en tant qu'administrateur plus longtemps que nécessaire.

6. Sauvegardez régulièrement vos données dans plusieurs emplacements et entrainez-vous régulièrement à les restaurer.

Dans notre enquête L'état des ransomwares 2024, 68 % des responsables informatiques des entreprises dont les données ont été chiffrées ont pu restaurer ces dernières à l'aide de sauvegardes. C'est pourquoi il est important de sauvegarder régulièrement vos données en plusieurs endroits, et d'utiliser une solution MFA pour protéger les sauvegardes dans le Cloud. Par ailleurs, il est conseillé de s'entraîner à effectuer des restaurations à partir de sauvegardes afin d'assurer une récupération sans heurts. Enfin, surveillez les activités suspectes pour protéger les sauvegardes contre les menaces potentielles.

7. Supprimez les applications inutiles

Les adversaires exploitent les applications courantes à des fins malveillantes. Avec cette méthode, appelée « Living-off-the-Land », il est plus difficile de différencier un usage légitime d'une activité malveillante. Par conséquent, lorsqu'une application n'est pas nécessaire au travail d'un utilisateur, demandez-vous s'il est nécessaire de la laisser sur l'appareil. En cas de doute, supprimez-la.

8. Repérez les appareils non protégés sur votre réseau

Les adversaires ciblent les appareils dépourvus de protection Endpoint pour passer sous les radars et agir librement au sein de votre environnement. Ces appareils non protégés peuvent être utilisés pour des attaques de ransomware distant.

Bonnes pratiques pour votre protection Endpoint

Une méthode efficace pour se prémunir contre les attaques de ransomware consiste à utiliser une solution EDR (Endpoint Detection and Response) ou XDR (Extended Detection and Response) qui inclut des technologies de prévention avancées et des capacités de chasse aux menaces.

La mauvaise configuration des outils de sécurité est le principal cyber risque pour les entreprises[8]. Mal configurer les paramètres des politiques de sécurité, des exclusions ou d'autres facteurs peut compromettre la posture de sécurité. Il est important de configurer correctement votre protection Endpoint pour bénéficier d'une protection optimale.

Nous vous recommandons donc de suivre ces bonnes pratiques pour bien protéger vos postes contre les ransomwares :

1. Activez toutes les politiques de sécurité et fonctionnalités recommandées

Cela peut paraître évident, mais c'est une condition *sine qua non* pour obtenir la meilleure protection possible de la part de votre solution de sécurité Endpoint.

Les politiques et paramètres de sécurité sont conçus pour bloquer des menaces spécifiques. Le fait de vérifier régulièrement que toutes les options de protection sont activées permet de s'assurer que vos postes sont protégés contre les ransomwares actuels et émergents. Veillez à activer les fonctionnalités qui permettent de détecter les techniques d'attaque sans fichier et les technologies comportementales. De plus, nous vous recommandons de prendre les mesures suivantes :

A) Activer la protection antialtération

Cela empêche toute modification ou suppression non autorisée de logiciels de protection Endpoint. L'une des premières choses que les adversaires font après avoir pénétré un système est de désactiver ou de supprimer les systèmes de protection Endpoint.

B) Activer la journalisation analytique (idéalement dans le Cloud)

Si vous êtes attaqué, il est essentiel de savoir ce qui s'est passé, afin d'éviter que cela ne se reproduise. Cependant, les adversaires nettoient souvent les journaux du système pour effacer leurs traces, supprimant ainsi les preuves post-mortem qui pourraient permettre de reconstituer le déroulement de l'attaque. Par ailleurs, il arrive parfois que l'on ne puisse plus accéder à l'appareil contenant les informations. Enregistrer ses activités dans le Cloud vous permet de conserver des informations critiques.

C) Vérifier que le contenu de la protection Endpoint et les mises à jour du produit sont activés

Afin de suivre le rythme des menaces en constante évolution et de se protéger contre les menaces émergentes, il est extrêmement important de mettre régulièrement à jour les produits de sécurité avec de nouvelles données. Désactiver les mises à jour des produits et du contenu entraînera une dégradation de votre protection au fil du temps.

2. Vérifiez régulièrement vos exclusions

Les exclusions empêchent la recherche de malwares dans les répertoires et les types de fichiers de confiance. Elles sont parfois utilisées pour réduire les délais du système et minimiser le risque de faux positifs dans les alertes de sécurité.

Au fil du temps, une liste croissante d'exclusions crée des failles de sécurité dont les adversaires peuvent tirer parti. Les malwares qui parviennent à s'introduire dans des répertoires exclus (par exemple déplacés accidentellement par un utilisateur) ont de grandes chances d'atteindre leurs objectifs.

Vérifiez régulièrement votre liste d'exclusions dans les paramètres des politiques de sécurité et supprimez-en le plus possible. Pour celles que vous ne pouvez pas supprimer, faites en sorte qu'elles soient aussi spécifiques que possible. Par exemple, plutôt que d'exclure un répertoire ou un lecteur d'une base de données, excluez uniquement des fichiers spécifiques avec leur chemin complet. Vous empêcherez ainsi le malware de contourner votre sécurité et de s'exécuter à partir du même dossier.

3. Activez l'authentification multifacteur (MFA) pour votre console de sécurité

Cela permet de garantir un accès sécurisé à la plateforme qui gère votre protection Endpoint et vos autres contrôles de sécurité. De plus, cela empêche les adversaires de modifier délibérément vos paramètres ou de désactiver/supprimer votre protection, dans le but de pouvoir ensuite cibler vos postes et vos serveurs.

8 Remédier à la pénurie de compétences en cybersécurité dans les PME - Sophos

4. Maintenez de bonnes pratiques et une bonne hygiène informatiques

Instaurer une maintenance informatique régulière garantit que vos systèmes et les logiciels qui y sont installés fonctionnent avec une efficacité maximale. Cette pratique limite vos risques de cybersécurité et peut vous faire gagner du temps lorsque vous devez remédier à des incidents futurs.

Il est particulièrement important de mettre en œuvre un programme de maintenance de la sécurité informatique pour se prémunir contre les attaques de ransomware et d'autres cybermenaces. Par exemple : s'assurer que le RDP ne fonctionne que là où vous en avez besoin, vérifier régulièrement les problèmes de configuration, surveiller les performances des appareils et supprimer les programmes indésirables ou inutiles. Le contrôle de l'hygiène informatique peut vous informer sur la nécessité de mettre à jour certaines applications logicielles. C'est aussi un bon moyen de s'assurer que vos données sont sauvegardées régulièrement.

5. Chassez proactivement les adversaires actifs sur votre environnement

Dans le paysage actuel des menaces, les adversaires sont plus rusés que jamais. Ils déploient souvent des outils légitimes et utilisent des identifiants volés pour éviter la détection. C'est pourquoi il est indispensable de chasser de manière proactive les menaces avancées et les adversaires actifs afin d'identifier et de bloquer ces attaques Living Off The Land. Une fois découverts, vous devez également être capables de prendre les mesures nécessaires pour les bloquer rapidement.

Des solutions telles que les technologies EDR (Endpoint Detection and Response) et XDR (Extended Detection and Response) fournissent des capacités de chasse, d'investigation et de neutralisation des menaces à votre équipe de sécurité interne. Mais comme les adversaires prennent souvent le soin de lancer leurs attaques en dehors des heures de bureau, il arrive parfois que l'équipe dédiée ne soit pas sur place pour intervenir. Bon nombre d'entreprises peinent à maintenir une couverture 24 h/24 pour se protéger contre les attaques de ransomware avancées. C'est pourquoi les services managés de détection et de réponse ou MDR (Managed Detection and Response) sont essentiels pour de nombreuses organisations.

Superposer les technologies de sécurité pour mieux lutter contre les ransomwares

Comme le dit l'adage « Mieux vaut prévenir que guérir », il est plus facile de stopper un problème à un stade précoce que de réparer ensuite les dégâts. La stratégie de protection de votre entreprise contre les ransomwares gagne à s'appuyer sur une approche multicouche de la sécurité informatique, dans le cadre de laquelle plusieurs technologies sont associées. En commençant par la protection Endpoint, les entreprises peuvent ajouter des couches supplémentaires en fonction de leurs besoins, de manière à optimiser la protection et la visibilité au fil du temps.

Par exemple :

- **Un pare-feu** pour identifier et bloquer le trafic réseau suspect et prévenir toute intrusion de menaces dans votre environnement. Un pare-feu a une visibilité sur le trafic réseau entrant et sortant de votre organisation. Il n'a en revanche aucune visibilité sur le trafic réseau à l'intérieur de l'environnement.
- **Un produit NDR (Network Detection and Response)** permet de détecter les appareils non protégés et d'identifier les adversaires qui se déplacent latéralement sur votre réseau. La solution NDR offre une visibilité sur le trafic du réseau interne que les pare-feux ne peuvent pas voir.
- **Une plateforme XDR** peut fournir des capacités de chasse, d'investigation et de neutralisation des menaces. Elle peut également s'intégrer à vos autres solutions de sécurité informatique, pour offrir une visibilité sur l'ensemble des contrôles de sécurité à partir d'une seule et unique plateforme.
- **Un service MDR** offre une surveillance 24/7 et une chasse aux menaces orchestrée par des experts spécialisés dans la détection et la réponse aux cyberattaques, que les solutions technologiques à elles seules ne peuvent pas prévenir. Votre service MDR doit offrir une réponse complète aux incidents pour intercepter, contenir et éliminer complètement les adversaires sans coûts supplémentaires. Un service MDR doit s'intégrer à vos outils de cybersécurité existants pour une visibilité complète sur l'ensemble de votre environnement. Il offre également le plus haut niveau de protection contre les attaques de ransomware pilotées par des humains.
- **Une solution de gestion de la surface d'attaque externe (EASM) ou de gestion des vulnérabilités (VM)** peut être utilisée pour identifier et prioriser les vulnérabilités. Cela vous permet d'identifier et d'appliquer les correctifs manquants avant que les adversaires ne puissent les exploiter.

Sophos protège contre les ransomwares

Sophos Endpoint adopte une approche globale axée sur la prévention pour protéger tous les postes de travail et ne s'appuie pas uniquement sur une seule technique de sécurité. Cette solution utilise des technologies sophistiquées qui bloquent les attaques les plus diverses, notamment :

- **La protection anti-ransomware imperméable** protège contre les attaques de ransomware locales et distantes, y compris les nouvelles variantes. Elle bloque le chiffrement malveillant en temps réel et restaure automatiquement tout fichier affecté vers son état d'origine sain, minimisant ainsi tout impact sur l'entreprise.
- **La technologie anti-exploit** protège contre les attaques sans fichier et les exploits zero-day en bloquant les techniques utilisées par les adversaires tout au long de la chaîne d'attaque.
- **La protection adaptative contre les attaques** est une défense dynamique qui s'adapte en réponse aux adversaires actifs et aux attaques pilotées manuellement. Les défenses renforcées dynamiquement empêchent les adversaires de poursuivre leurs actions en réduisant la surface d'attaque et en perturbant leur tentative malveillante.

Sophos Endpoint est facile à configurer et à administrer. Installez Sophos Endpoint et lancez-vous ! Les technologies de protection que nous recommandons sont activées par défaut. Vous bénéficiez ainsi immédiatement des paramètres de protection les plus puissants, sans qu'aucun réglage ne soit nécessaire. Un contrôle granulaire est également disponible si nécessaire.

La gestion de Sophos Endpoint se fait depuis **Sophos Central,** la plateforme de cybersécurité la plus fiable au monde. Cette puissante plateforme de gestion de la cybersécurité basée dans le Cloud unifie toutes les solutions de sécurité Sophos Next-Gen et son accès est conditionné par MFA.

Les clients Sophos gèrent leurs systèmes de protection Endpoint depuis Sophos Central et bénéficient de la fonctionnalité « Intégrité du compte ». Les administrateurs peuvent ainsi identifier les dérives de leur posture de sécurité au niveau des politiques de sécurité et des exclusions, ainsi que d'autres erreurs de configuration à haut risque. Cela leur donne la possibilité de remédier aux problèmes d'un simple clic.

Sophos XDR — outils proactifs pour la chasse aux menaces et l'hygiène informatique

Sophos XDR est une plateforme unifiée de détection et de réponse, basée sur l'approche robuste de protection de Sophos Endpoint. Elle vous permet de détecter, d'investiguer et de répondre aux menaces multi-étapes, à travers tous les vecteurs d'attaque clés, dans les plus brefs délais.

Les technologies Sophos sont entièrement intégrées à la plateforme Sophos XDR et fonctionnent ensemble pour fournir de manière transparente les meilleurs résultats possibles en matière de sécurité. Par ailleurs, vous pourrez optimiser le retour sur investissement de vos produits de cybersécurité existants grâce à des intégrations clés en main avec un vaste écosystème de solutions tierces endpoint, pare-feu, réseau, messagerie, gestion d'identité, productivité, sécurité cloud, sauvegarde et récupération.

Sophos XDR fournit des outils et des fonctionnalités conçus pour accroître la productivité des analystes de sécurité et des administrateurs informatiques.

- Les détections priorisées par l'IA sur toutes les surfaces d'attaque clés permettent de repérer les activités suspectes qui requièrent une attention immédiate.
- Les détections et les dossiers sont automatiquement mappés avec les tactiques de MITRE ATT&CK, ce qui vous permet d'identifier facilement les lacunes dans vos défenses.
- Les actions automatisées, telles que l'arrêt des processus, la restauration des fichiers touchés par un ransomware et l'isolement sur le réseau, permettent de contenir rapidement les menaces et de gagner un temps précieux. Les capacités de l'IA générative axées sur les résultats donnent aux analystes de sécurité les moyens de neutraliser les adversaires plus rapidement, renforçant ainsi la confiance des analystes et de l'entreprise.

Sophos MDR — Services managés de détection et réponse 24/7

Sophos MDR est un service de sécurité managé 24/7, mis en œuvre par des experts hautement qualifiés qui luttent en votre nom contre les nouvelles menaces avancées et les adversaires actifs. Le service Sophos MDR offre une protection ultime contre les ransomwares.

En obtenant le niveau de service Sophos MDR Complete, vous bénéficiez de la réponse aux incidents complète et illimitée, sans plafond ni frais supplémentaires. Nos équipes peuvent exécuter un ensemble complet d'actions de réponse en votre nom et à distance pour intercepter, contenir et éliminer complètement l'adversaire.

Comme Sophos XDR, Sophos MDR intègre et collecte les données télémétriques de tous les produits Sophos et s'intègre à la même gamme étendue de produits de sécurité tiers pour accroître la visibilité et la protection sur votre environnement.

Contrat de services Sophos de réponse aux incidents — un service de réponse aux incidents prêt à intervenir

Disposer d'une équipe de réponse aux incidents avant que les adversaires ne frappent est le seul moyen de gagner du temps, de réduire les coûts et d'atténuer les conséquences d'un incident (par exemple, lorsque des adversaires déploient un ransomware).

Le **Contrat de services Sophos de réponse aux incidents** est un abonnement annuel qui vous fait bénéficier d'une assistance à la demande assurée par une équipe d'experts en réponse aux incidents pouvant se déployer rapidement dans votre environnement pour intercepter, contenir et éliminer complètement les adversaires actifs. Il comprend également des supports de préparation aux incidents critiques pour vous aider à améliorer la posture de sécurité de votre entreprise et à réduire la probabilité d'une violation.

Remarque : le Contrat de services de réponse aux incidents de Sophos n'est pas nécessaire si vous acheter le niveau de service MDR Complete de Sophos, qui inclut par défaut une réponse aux incidents complète.

Sophos Managed Risk – service de gestion des vulnérabilités et de la surface d'attaque externe

Les vulnérabilités non corrigées sont la principale cause des attaques de ransomware. Il est donc indispensable de pouvoir identifier, investiguer et prioriser les vulnérabilités à haut risque dans votre environnement avant qu'elles ne constituent un problème. Sophos Managed Risk, optimisé par la technologie Tenable, leader sur le marché, vous aide à atteindre cet objectif.

Avec **Sophos Managed Risk,** nos analystes expérimentés identifient les vulnérabilités de cybersécurité de première importance et les vecteurs d'attaque potentiels dans votre environnement en vue de prendre des mesures pour prévenir les attaques avant qu'elles ne perturbent votre activité.

Conclusion

Les ransomwares ne cessent d'évoluer et restent un moyen de pression efficace pour forcer les organisations qui en sont victimes à payer une rançon. Votre objectif est d'empêcher l'intrusion des adversaires dans votre organisation et de les repérer et les expulser rapidement s'ils arrivent à y pénétrer. Prenez soin d'appliquer les bonnes pratiques en matière de sécurité informatique et de sécurité Endpoint, d'assurer la formation continue des utilisateurs et de rester vigilant face aux menaces et aux adversaires au sein de votre environnement. En suivant une approche de la cybersécurité multicouche et axée sur la prévention, et en mettant en place une détection et une réponse 24/7, votre organisation se donne les moyens de se protéger au maximum contre les ransomwares et les menaces les plus récentes.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site www.sophos.fr

© Copyright 2024. Sophos Ltd. Tous droits réservés.
Immatriculée en Angleterre et au Pays de Galles N° 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni.
Sophos est la marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

2024-10-01 (WP-NP)

SOPHOS