Guide MDR: protégez votre PME des cyberattaques grâce à une centrale d'alarme numérique

Qu'est-ce qu'un MDR et comment améliore-t-il la sécurité?

Un service de détection et de réponse gérées (de l'anglais, *Managed Detection and Response*, *MDR*) ou un centre des opérations de sécurité (de l'anglais, *Security Operations Center, SOC*) fonctionne comme une centrale d'alarme numérique conçue pour assurer une veille en temps réel de l'ensemble de l'infrastructure informatique d'une entreprise et, ainsi, la protéger de toute intrusion malveillante. Cette surveillance continue permet de détecter les menaces en temps réel et de les analyser, ce qui facilite une identification précoce des incidents touchant la sécurité et aide à s'en prémunir.

De nombreux fournisseurs de services MDR/SOC travaillent 24 heures sur 24 et s'appuient sur des technologies de pointe pour détecter les menaces le plus en amont possible et, ainsi, les écarter énergiquement. Des données sensibles provenant des terminaux (périphériques), des réseaux, des services en nuage et des identités sont corrélées de manière centralisée afin de détecter des menaces en fonction du contexte, d'y apporter une réponse automatisée et de les déjouer activement en amont par le biais de mécanismes de prévention intégrés.

Dès qu'une menace est identifiée, une équipe expérimentée de spécialistes en sécurité est alertée. Cette équipe de permanence est chargée de réagir avec rapidité et efficacité aux incidents de sécurité repérés. Des mesures visant à limiter les dommages et à rétablir la situation antérieure sont mises en place à distance par l'équipe de spécialistes afin de prévenir ou de réduire toutes répercussions sur les activités de l'entreprise.

Par la combinaison de la technologie de pointe et de l'expertise humaine, un service MDR/SOC offre un haut niveau de sécurité. Il minimise le risque de dommages susceptibles d'être causés par des cyberattaques et contribue grandement à l'accroissement de la sécurité et de la stabilité des systèmes informatiques d'une entreprise. Cela est particulièrement important à une époque où les cybermenaces sont de plus en plus complexes et fréquentes.

Quelles entreprises devraient mettre en place un MDR pour se protéger?

Il n'est pas évident de désigner avec certitude quels types d'entreprises devraient se protéger avec l'aide d'un MDR, car cela dépend beaucoup de l'appétence de chacune en matière de risques et de ses besoins spécifiques. La mise en place d'un MDR devrait surtout être envisagée par les PME de grande taille qui traitent des données sensibles ou dont l'activité repose largement sur les technologies de l'information. L'Association Suisse d'Assurances recommande aux entreprises qui disposent de 30 postes de travail sur ordinateur ou plus de se pencher sur cette question.

De manière générale, chaque entreprise devrait vérifier la capacité de réaction du prestataire informatique chargé de la surveillance de ses systèmes en cas de cyberattaque. Si un prestataire informatique ou un prestataire MDR externe n'est pas explicitement chargé de ces fonctions, des attaques risquent de n'être ni détectées, ni repoussées.

Que doit apporter la mise en place d'un service MRD *ad hoc*?

Un service de détection et de réponse gérées est approprié s'il répond aux besoins et aux exigences spécifiques de l'entreprise considérée. Il existe différentes variantes de solution MDR, allant des fonctions basiques à des mesures de sécurité substantielles et avancées.

En matière de prévention des dommages, il a été démontré que le risque se réduit progressivement avec un bon rapport coût-bénéfice. Nous décrivons maintenant trois variantes de MDR: la variante de base pour commencer, une variante standard et une variante pour une protection complète. Chacune de ces variantes offre différents niveaux de protection et de fonctionnalités afin de répondre aux exigences respectives.

- **Variante de base: mise en place de mécanismes de protection préventifs**
  Installation sur les ordinateurs portables et les serveurs d'un agent de détection et de réponse aux points de terminaison (en anglais, *Endpoint Detection and Response*, *EDR*) basé sur le comportement, ainsi qu'intégration des données d'identification du service d'annuaire *Active Directory* et d'alarmes de pare-feu. L'agent EDR offre une protection antivirus moderne et capable, dans certains cas, de bloquer automatiquement les attaques. Dans de nombreux cas de figure, il remplace souvent le logiciel antivirus déjà installé.

- **Variante standard: garantie de la capacité d'action en cas d'attaques**
  Mise en place d'une procédure à même de réagir 24 heures sur 24 aux événements menaçant la sécurité et d'évaluer le degré de gravité des alertes EDR ou de sécurité. En la matière, il est essentiel que le prestataire de services MDR dispose d'une équipe de permanence composée de spécialistes informatiques chargés d'intervenir en cas d'urgence. En fonction du profil de risques de l'entreprise, l'équipe dédiée aux urgences informatiques doit surveiller les alertes de sécurité 24 heures sur 24, week-ends compris. La plupart du temps, une surveillance pendant les heures de bureau en semaine est suffisante.

- **Variante complète: extension de la visibilité et couverture des scénarios**
  Mise en place d'un système de détection qui évalue le degré de gravité des alertes provenant d'autres systèmes d'alarme et de surveillance supplémentaires connectés et auquel l'équipe dédiée aux urgences informatiques a accès. Par exemple, il est également possible d'intégrer des alertes provenant d'applications ou de services en nuage afin de cartographier des scénarios de détection spécifiques au client et d'améliorer encore la situation de ce dernier en termes de sécurité.

Quel en est le coût financier?

Les coûts de mise en place d'un service de détection et de réponse gérées peuvent varier du tout au tout et dépendent de différents facteurs. L'un des principaux facteurs réside dans la couverture temporelle et le niveau de service souhaité, c'est-à-dire si la surveillance est assurée 24 heures sur 24 ou seulement à certaines heures. La quantité de données traitées et le nombre de sources jouent également un rôle lors du calcul du prix. L'existence d'une installation EDR et d'une licence *Microsoft Defender* peuvent éventuellement contribuer à réduire le coût de la surveillance. En règle générale, les coûts mensuels par poste de travail informatique et serveur surveillé représentent entre 10 et 15 pour cent du budget informatique.

De quoi faut-il tenir compte lors du choix d'un prestataire?

Lors de la souscription d'un service de détection et de réponse gérées, il y a plusieurs aspects importants à prendre en compte. Tout d'abord, il convient de vérifier si votre propre prestataire habituel de services informatiques propose un service MDR en qualité de revendeur. Si tel est le cas, cela simplifiera la procédure de mise en œuvre et garantira une intégration fluide de ce service complémentaire dans l'infrastructure informatique existante. En l'absence de *Microsoft Defender*, il est nécessaire d'installer un agent approprié et de s'assurer que le pare-feu est configuré de sorte que les alarmes puissent être autorisées et traitées. Un autre point important réside dans la coopération étroite entre le fournisseur de services MDR et le fournisseur de services informatiques habituel afin de garantir une capacité de réaction rapide et l'isolement des menaces détectées. Cette collaboration est décisive pour l'efficacité des mesures de sécurité et la minimisation des dommages causés par les cyberattaques.

Quels sont les prestataires exerçant en Suisse?

Voici quelques exemples de prestataires exerçant en Suisse et spécialisés dans les MDR/SOC:

- Adnovum
- Axians
- Compass Security
- InfoGuard
- Inseya
- Kudelski Security
- Netaccess
- Netcloud
- Swisscom
- Wizlynx

Résumé

Un prestataire de services de détection et de réponse gérées (MDR, de l'anglais *Managed Detection and Response*) offre aux entreprises une protection intégrale contre les cybermenaces grâce à une surveillance en temps réel et une réaction rapide aux incidents de sécurité. Compte tenu de la complexité et de la fréquence croissantes des cyberattaques, le recours aux services MDR revêt une grande importance pour les entreprises, toutes tailles et tous secteurs confondus. Lors du choix d'un prestataire de services MDR, l'Association Suisse d'Assurances (ASA) recommande aux entreprises de bien prendre en compte leurs propres besoins et leurs risques spécifiques. La mise en œuvre d'une bonne solution MDR peut aider de manière significative à accroître la cyberrésilience et, par ricochet, la sécurité et la stabilité de l'ensemble de l'infrastructure informatique.

Qui est l'ASA?

L'Association Suisse d'Assurances ASA est l'organisation sectorielle des assureurs privés suisses. Elle œuvre en faveur d'un développement durable de l'industrie de l'assurance et promeut des solutions contribuant à la stabilité et à la sécurité de l'économie et de la société suisses. L'un des principaux objectifs de l'ASA consiste dans le renforcement de la sécurité des entreprises suisses. Par ses activités, l'association participe à l'accroissement de la cyberrésilience dans notre pays. Cela renforce non seulement le secteur de l'assurance, mais aussi l'ensemble de l'économie nationale.

Pourquoi l'ASA élabore-t-elle un guide MDR?

Forte de son expérience des sinistres dans le secteur de l'assurance, l'ASA a décidé d'élaborer un guide MDR, car les services de détection et de réponse gérées constituent un outil très efficace et contribuent nettement à l'amélioration de la cybersécurité. De nombreux fournisseurs et revendeurs en Suisse proposent désormais un bon rapport qualité-prix pour de tels services. Avec ce guide, l'ASA entend aider ses compagnies membres, mais aussi toutes les entreprises, à identifier les solutions répondant le mieux à leurs besoins spécifiques. Ce faisant, elle participe grandement à la sécurité de l'économie suisse.