Devriez-vous confier votre cybersécurité à une tierce partie?

IL FAUT AINSI TROUVER DES PARTENAIRES SOLIDES DONT LA RÉPUTATION EST IRRÉPROCHABLE

Dans notre dernier article concernant le fonctionnement de notre service MDR, nous avons reçu de nombreux commentaires intéressants. Parmi ceux-ci, une question qui nous a surpris a été posée à deux reprises : « Pourquoi ferais-je confiance à une tierce partie pour la surveillance de mon réseau? » Bien sûr, notre première réaction a été de constater que les personnes qui posaient cette question ne comprenaient pas comment fonctionnent les secteurs des services informatiques et de la cybersécurité. Mais en y réfléchissant davantage, nous nous sommes dit qu'il s'agissait en fait d'une question assez fondamentale.

La réponse est simple lorsqu'on s'interroge sur la possibilité qu'ont les entreprises à faire confiance à une équipe externe pour gérer leurs TI ainsi que leur cybersécurité. Il est question de faire confiance de la même manière qu'avec n'importe quel autre partenaire commercial essentiel. Il faut ainsi trouver des partenaires solides dont la réputation est irréprochable. Il ne s'agit pas de savoir ***comment***, mais bien pourquoi devons-nous leur faire confiance.

La question derrière la question

Pourquoi devrions-nous déléguer le contrôle de la sécurité de notre parc informatique à une entreprise extérieure? La réponse se résume à trois avantages essentiels que les entreprises de cybersécurité réputées, spécialisées et expérimentées, apportent à la table.

1. Niveau de service (peuvent-elles l'offrir?)
2. Type de technologie (ont-elles la bonne?)
3. Expérience et réputation (en ont-elles?)

La leçon d'aujourd'hui est une gracieuseté de la lettre M

Tout d'abord, qui sont ces organisations qui proposent leurs services pour de la cybersécurité externalisée? De manière générale, il existe trois types d'organisations qui sont en concurrence pour devenir votre SOC externalisé.

MSP

Un *MSP* (de l'anglais *Managed Service Provider*) est une compagnie informatique généraliste qui prend en charge tout (ou une partie) de la gestion de vos logiciels, de vos TI et périphériques. Ces services d'externalisation informatique proposent aussi des services de cybersécurité. Ce sont rarement des spécialistes, mais ils ont l'avantage concurrentiel d'avoir une relation préexistante avec le client lorsque des besoins en cybersécurité sont identifiés, mais cela ne fait pas d'eux un bon choix.

MSSP

Les MSSP (Managed Security Services Provider) sont comme les MSP, mais spécialisés dans la cybersécurité. Les

MSSP se concentrent davantage sur la sélection et la mise en œuvre de la plateforme de sécurité ainsi que de la gestion des consoles de sécurité. Ils assurent ensuite la maintenance et l'exploitation de ces logiciels tout en transmettant les alertes à votre équipe informatique pour qu'elle prenne les mesures nécessaires au besoin.

MDR

Aujourd'hui, avec l'augmentation de la fréquence et de la sophistication des cyberattaques, il est essentiel de comprendre non seulement l'origine des attaques, mais également d'identifier les impacts potentiels et de savoir comment combler les failles de sécurité. Les services ***MDR (de l'anglais Managed Detection and Response)*** sont une réponse à cette nouvelle réalité. Les services MDR permettent une approche proactive de la cybersécurité. Ils se concentrent d'abord sur la détection en identifiant les sources de risque et en surveillant ces vulnérabilités. Le véritable pouvoir du MDR réside dans la lettre R - où le fournisseur analyse la menace et propose des mesures correctives exploitables pour contrer et réduire son impact potentiel.

Alors, pourquoi faire confiance à une entreprise externe?

En fait, c'est la seule solution qui a du sens, surtout si vous êtes une petite ou moyenne entreprise. Voici les 5 principaux facteurs qui poussent les PME à externaliser leur cybersécurité :

1. **Coûts** - Parce que vous avez besoin de protection et que la mise en place d'une équipe interne est un processus excessivement coûteux.
2. **Rapidité** - Engager une équipe et mettre en place votre propre SOC prend du temps, ce que vous n'avez probablement pas.
3. **Expérience et expertise** - Votre fournisseur, si vous l'avez bien choisi, dispose d'une équipe qualifiée de professionnels en sécurité qui ne font rien d'autre que de la sécurité informatique. Ils ont plus d'un tour dans leur sac.
4. **Concentration** - L'externalisation de la cybersécurité permet à votre équipe TI de se concentrer sur ses tâches principales plutôt que d'être constamment sollicitée pour des problèmes de cybersécurité.
5. **Couverture 24/7/365** - Si vous deviez mettre ce type de couverture en place à l'interne, cela prendrait du temps et serait très coûteux.

Retournons à la question derrière la question

Au début de cet article, nous avons mentionné trois questions qui devraient influencer votre choix de partenaire en matière de cybersécurité. Nous allons donc examiner chacune d'entre elles de plus près.

Offre-t-il le niveau de service dont vous avez besoin?

Lorsque vous choisissez un fournisseur de services, demandez-lui s'il offre uniquement des services en cybersécurité. De plus en plus d'entreprises opportunistes ajoutent un volet de cybersécurité à leur offre de services informatiques. Malheureusement, selon de nombreux experts en cybersécurité, il s'agit d'un conflit d'intérêts lorsqu'il s'agit de servir un client. La plupart du temps, les organisations qui proposent des services d'externalisation informatique et de sécurité informatique peuvent se retrouver dans une situation où leur personnel de sécurité entre en conflit avec leur propre équipe informatique. Il est important de comprendre que l'expertise en gestion informatique n'est pas une expertise en cybersécurité. Par conséquent, il est essentiel de s'assurer que vous choisissez un partenaire dont l'objectif est la gestion de la sécurité uniquement et dont l'équipe se consacre à 100 % à la cybersécurité.

Quelle est la technologie appropriée pour votre niveau de risque?

Il existe une multitude de technologies sur lesquelles vous pouvez baser une offre de services gérés. Et, même à l'intérieur d'un segment, les outils sont très différents les uns des autres. Voici trois outils standards sur le marché : SIEM, EDR, et IDS/NDR (ou surveillance du réseau).

Les SIEM (de l'anglais ***Security Information and Event Management***) sont des outils créés pour centraliser les journaux et événements de sécurité, tels que les tentatives d'accès échouées ou réussies. Un SIEM vous permet de surveiller des éléments spécifiques de votre réseau.

Les EDR (***Endpoint Detection and Response***) sont des solutions de sécurité conçues pour détecter les cyberattaques sur les machines individuelles. Elles sont comme des logiciels antivirus de nouvelle génération. Les EDR vont au-delà de la simple détection basée sur les signatures : elles utilisent l'analyse de la mémoire, l'analyse comportementale et la détection des IOC. Cependant, les solutions EDR ont des limites importantes. Par exemple, elles ne fournissent pas de visibilité sur les appareils de l'Internet des objets (IoT) ou sur le nuage. Et, même dans les entreprises de taille moyenne, les systèmes EDR provoquent souvent des conflits avec les logiciels antivirus existants.

Basées sur l'analyse des flux de communication du réseau, les technologies IDS (***Intrusion Detection Systems***, également appelées Surveillance Réseau (de l'anglais ***Network Monitoring***)) et les NDR (***Network Detection and Response***) se concentrent sur la détection. Leur avantage le plus significatif : une visibilité à 360° sur des machines telles que les imprimantes, les téléphones IP, les appareils IoT, les téléphones connectés, les caméras de sécurité, etc. Aujourd'hui, il est essentiel de surveiller tous les appareils connectés au réseau, car ils sont souvent utilisés comme relais par les ***hackers***. Les technologies de type IDS/NDR offrent également une détection plus précoce, permettant d'identifier plus rapidement les signaux d'intrusion.

Votre fournisseur vous recommandera probablement une ou plusieurs de ces technologies. Il est donc important de savoir ce qu'elles font et quels sont leurs points forts.

A-t-il l'expertise nécessaire?

Le facteur le plus important à prendre en compte lors du choix d'un partenaire est fort probablement son expertise. L'expérience terrain du personnel est sûrement l'élément le plus important de l'offre de votre partenaire. Cela peut sembler anodin, mais faites vos devoirs et renseignez-vous sur l'équipe proposée par votre partenaire potentiel.

Il existe de nombreux domaines d'expertise en matière de cybersécurité. Assurez-vous que votre fournisseur dispose de tous les analystes qualifiés pour gérer les alertes de sécurité et la réponse aux incidents. Les analystes de sécurité doivent avoir l'expérience et les connaissances nécessaires pour interpréter les signaux d'attaque, comprendre les techniques des pirates et fournir des recommandations pour atténuer les risques de sécurité. Assurez-vous que votre fournisseur de sécurité compte dans son équipe les profils suivants : responsable en chef de la cybersécurité, expert en gestion des cyberattaques, expert en réponse aux incidents, analyste en codes malveillants et spécialiste de logiciels pernicieux, etc.

À retenir

Devriez-vous faire confiance à une tierce partie pour s'occuper de votre cybersécurité? Oui, si vous avez fait vos devoirs et qu'elle a les compétences et l'expérience nécessaires pour répondre à vos besoins. Le bon partenaire spécialisé (comme StreamScan, avec plus de 10 ans d'expérience, une équipe spécialisée et une technologie approuvée par le gouvernement) disposera de connaissances et d'une expertise que vous ne pouvez pas égaler. Il a l'expérience nécessaire afin de répondre aux problèmes de cybersécurité du quotidien.

Lorsque vous choisissez votre partenaire, gardez ces trois éléments à l'esprit. Premièrement, définissez le niveau d'assistance dont vous avez besoin. Ensuite, sélectionnez la ou les technologies qui vous conviennent le mieux. Et enfin, choisissez une entreprise disposant de l'expertise nécessaire pour mettre en œuvre votre stratégie de cybersécurité.

Restez au fait des derniers développements en matière de cybersécurité pour les PME grâce à l'infolettre StreamScanner. Inscrivez-vous ici.

Besoin d'aide? StreamScan est là.

Si vous êtes victime d'un rançongiciel ou que vous désirez mettre en œuvre une solution de Détection et Réponse Gérées (MDR) pour éviter l'irréparable, StreamScan dispose d'experts ayant des années d'expérience pouvant vous aider. Contactez-nous à l'adresse securitepme@streamscan.ai ou appelez-nous au 1 877 208-9040.