Les essentiels de la cybersécurité pour les moyennes entreprises

Barracuda

Résumé analytique

Les entreprises de taille moyenne, que nous définissons ici comme des entreprises dont le chiffre d'affaires est compris entre 12 et 240 millons d'euros et qui emploient entre 200 et 2 000 personnes, sont des cibles attrayantes pour les cybercriminels, car elles font souvent partie de la chaîne d'approvisionnement d'une entreprise plus importante et peuvent être considérées comme un tremplin vers des victimes plus lucratives. Certaines PME se sont développés plus rapidement que leurs équipes de sécurité. Certaines ont peut-être gardé la même stratégie de sécurité que celle d'une entreprise beaucoup plus petite. En outre, certaines PME sont le résultat de rachats et de fusions rapides qui peuvent avoir laissé des vulnérabilités non documentées dans les réseaux et les systèmes partagés.

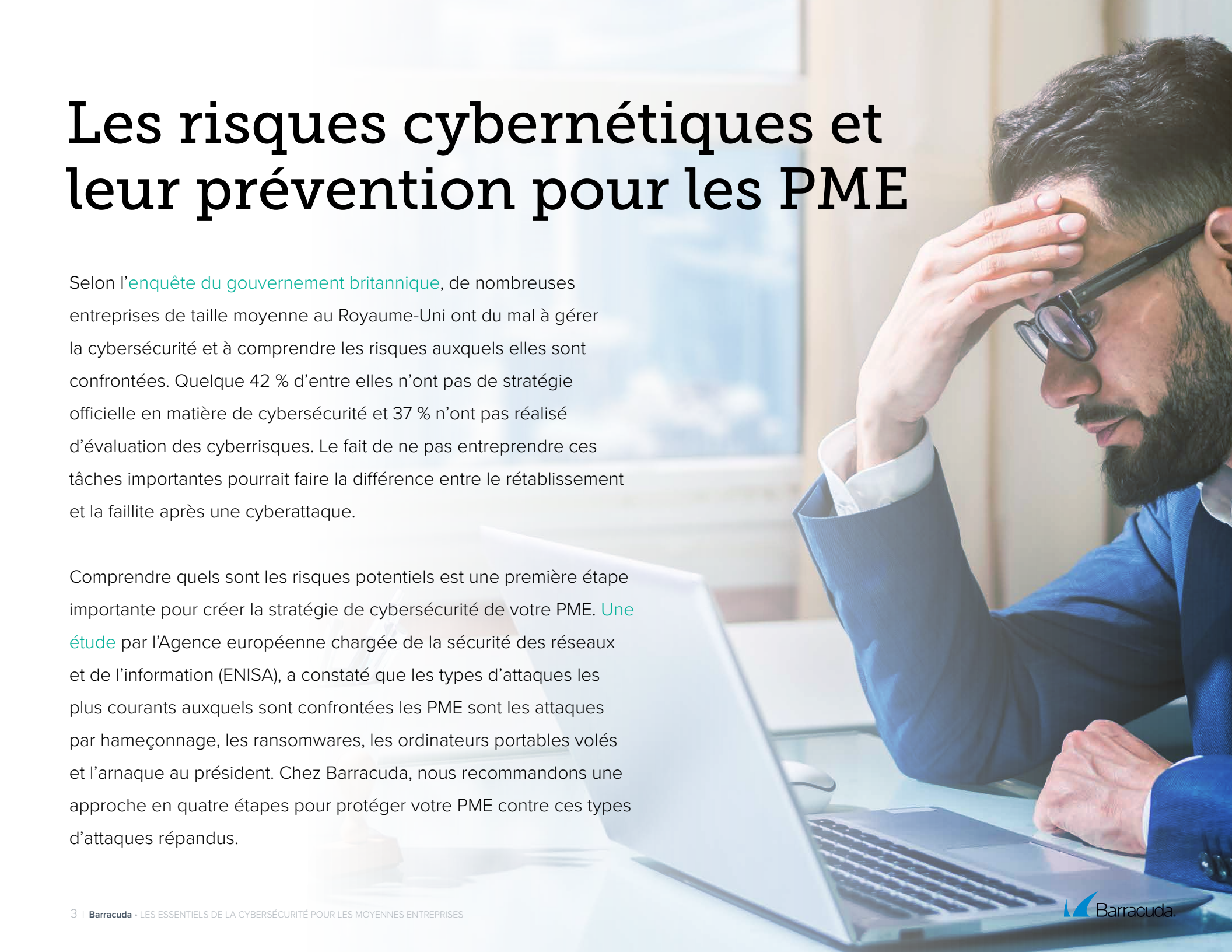
La recherche qui sous-tend le rapport Cybernomics 101 de Barracuda a révélé que près de la moitié (48 %) des entreprises de 100 à 750 employés décrivent leur position en matière de cybersécurité comme étant assez inefficace. Ce sentiment est partagé par 37 % des entreprises employant entre 750 et 2 500 salariés. Dans le même temps, l'impact médian et le coût de récupération des dommages causés aux actifs informatiques varient de 50 000 à 100 000 dollars pour les plus petites TPE à 1 million de dollars ou plus pour les plus grandes PME. Il s'agit de coûts importants à assumer pour une PME.

Pour limiter et contenir l'impact et les coûts d'un incident de sécurité informatique, les PME doivent disposer d'un plan et de mesures claires pour se protéger des conséquences potentiellement dévastatrices d'une attaque. Nous espérons que les pages suivantes inciteront les entreprises de taille moyenne à prendre des mesures pour se prémunir contre les cybermenaces actuelles et protéger leurs e-mails, leurs applications, leur réseau et leurs données.

Les risques cybernétiques et leur prévention pour les PME

Selon l'enquête du gouvernement britannique, de nombreuses entreprises de taille moyenne au Royaume-Uni ont du mal à gérer la cybersécurité et à comprendre les risques auxquels elles sont confrontées. Quelque 42 % d'entre elles n'ont pas de stratégie officielle en matière de cybersécurité et 37 % n'ont pas réalisé d'évaluation des cyberrisques. Le fait de ne pas entreprendre ces tâches importantes pourrait faire la différence entre le rétablissement et la faillite après une cyberattaque.

Comprendre quels sont les risques potentiels est une première étape importante pour créer la stratégie de cybersécurité de votre PME. Une étude par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), a constaté que les types d'attaques les plus courants auxquels sont confrontées les PME sont les attaques par hameçonnage, les ransomwares, les ordinateurs portables volés et l'arnaque au président. Chez Barracuda, nous recommandons une approche en quatre étapes pour protéger votre PME contre ces types d'attaques répandus.



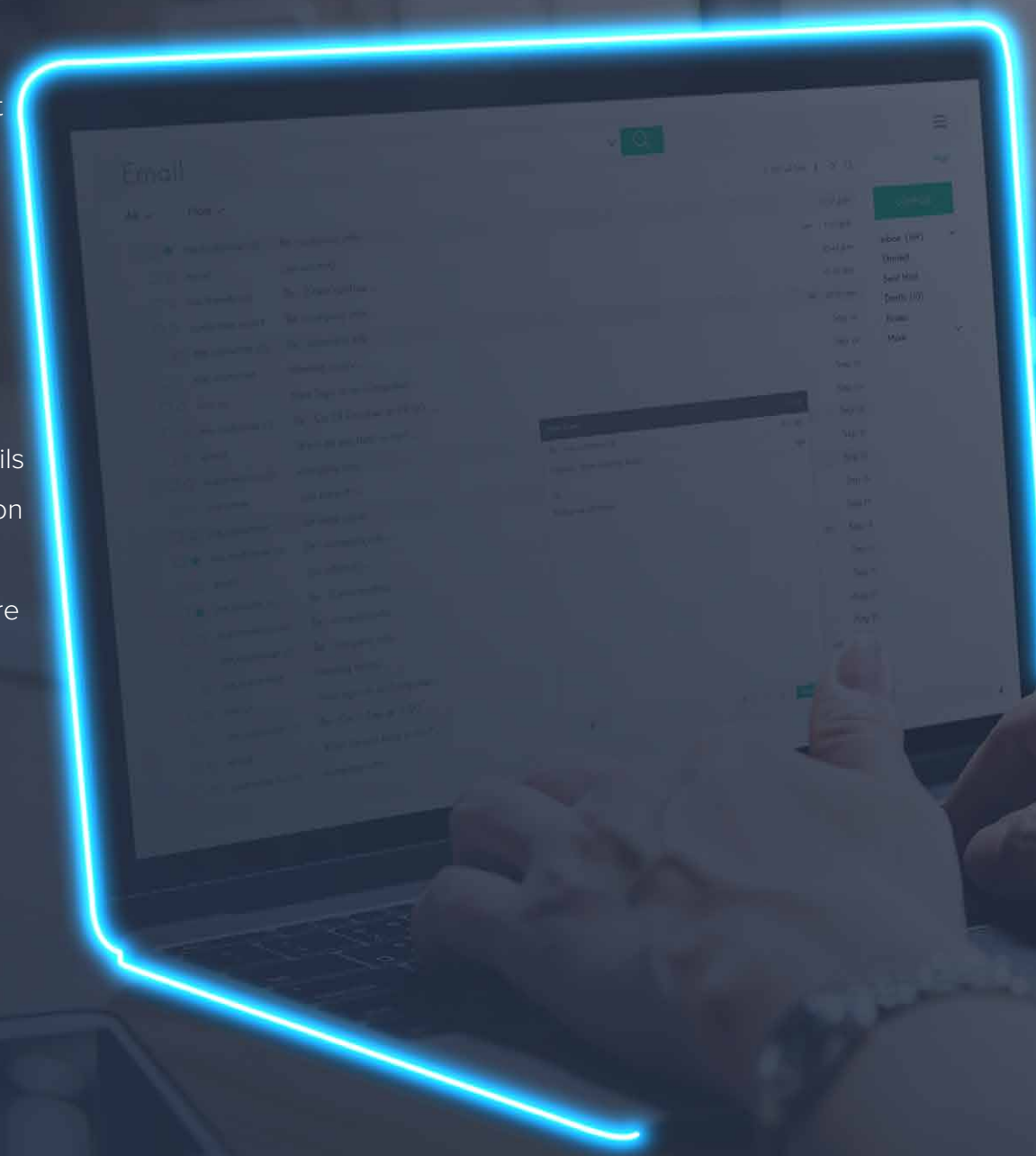
Première étape : protégez vos e-mails

L'e-mail reste une méthode très attrayante pour mener des cyberattaques, le hameçonnage, le spear-phishing, l'arnaque au président et le quishing (hameçonnage par code QR) offrant aux criminels plusieurs méthodes pour pénétrer dans une entreprise par e-mail. Les entreprises de taille moyenne sont des cibles attrayantes pour les attaques par e-mail, car les pirates peuvent supposer que les pratiques de cybersécurité sont moins rigoureuses que dans les grandes entreprises. Dans ce type d'attaque, les pirates envoient des e-mails frauduleux contenant une méthode d'obtention d'identifiants de connexion ou d'autres informations sensibles, ce qui pourrait leur permettre d'accéder au réseau et aux systèmes de votre entreprise pour extorquer de l'argent. Notre eBook, 13 types de menaces pare-mail à découvrir dès maintenant, peut vous aider à identifier les différentes façons dont les pirates peuvent exploiter les e-mails pour compromettre votre entreprise.

L'approche de Barracuda en matière de protection des e-mails comporte trois étapes : prévenir les menaces, détecter et répondre, et sécuriser vos données. La prévention des menaces par e-mail est un facteur important et comporte de multiples facettes. La méthode de prévention la plus importante consiste peut-être à former vos utilisateurs. Un e-mail de hameçonnage ne peut causer aucun dommage à une entreprise si personne ne clique sur un lien. L'essentiel est de former régulièrement et minutieusement votre personnel afin qu'il soit en mesure d'identifier les e-mails de hameçonnage et de mettre en place un processus pour signaler tout e-mail suspect qui se retrouve dans les boîtes de réception de vos utilisateurs.

Barracuda

Les outils qui vérifient le contenu des e-mails peuvent aider à identifier les e-mails malveillants, mais ils ne doivent pas être considérés comme un substitut à la formation de votre personnel à la détection des menaces. Ces scanners utilisent des méthodes telles que l'intelligence artificielle (IA) pour analyser automatiquement chaque e-mail de votre boîte de réception afin de détecter les intentions malveillantes. Ils peuvent également créer des rapports qui vous indiquent les domaines dans lesquels vous devez renforcer votre stratégie de sécurité en fonction du type de menaces qui envahissent les boîtes de réception. Le chiffrement des e-mails est également un élément important quand on parle protection des e-mails. Cela protège les informations sensibles de toute personne qui n'a pas la clé de déchiffrement, ajoutant un autre niveau de protection.



Barracuda

Deuxième étape : protégez les applications

Vos applications métier constituent un autre point d'entrée attrayant pour les pirates. Les entreprises de taille moyenne peuvent disposer de différentes applications destinées au public, notamment des portails de connexion et clients et des plateformes de e-commerce pour l'achat de produits. De telles applications sont critiques pour l'entreprise et contiennent des données sensibles sur les clients et les entreprises. Si celles-ci sont ciblées, les cybercriminels peuvent causer des dommages importants à votre entreprise de plusieurs façons. Les applications sont vulnérables aux attaques par déni de service distribué (DDoS), dans lesquelles un pirate envoie un volume excessif de trafic de bots pour saturer une application et la mettre hors ligne.

Forcer les temps d'arrêt et voler des données en injectant des malwares sont deux moyens potentiels pour les cybercriminels d'exploiter vos applications. Selon le rapport de Verizon : Data Breach Investigations de 2024 les principaux motifs d'attaque des applications sont l'argent (97 %) et l'espionnage (3 %). Les applications elles-mêmes peuvent être vulnérables aux attaques parce qu'elles n'acceptent pas que les utilisateurs se connectent à elles via des réseaux non sécurisés tels que le WiFi public, qui n'est pas chiffré. Pour ces raisons, la sécurité des applications doit être intégrée dès le départ, et non pas ajoutée après coup.

Barracuda

La mise en œuvre d'un Web Application Firewall (WAF) pour surveiller et filtrer le trafic entre Internet et les applications web est un élément important de la protection de vos applications. Le WAF agit comme un mur entre les sources de trafic et votre application, en filtrant les requêtes et en bloquant celles qu'il identifie comme malveillantes. Des mises à jour régulières et la gestion des correctifs sont essentielles pour s'assurer que l'application est à jour et que toutes les vulnérabilités ont été détectées et corrigées. Les failles non corrigées sont une cible facile pour les cybercriminels, il est donc important de s'assurer d'avoir un calendrier de gestion des correctifs régulier et complet.

La surveillance de vos applications pour détecter les activités suspectes est un autre élément clé de leur protection. Cela peut vous aider à identifier tout trafic ou comportement inhabituel susceptible de révéler une attaque potentielle, et vous permettre de réagir en conséquence. La mise en place d'un plan d'intervention en cas d'incident vous permet de faire face à un tel événement avec une stratégie, plutôt que de réagir au hasard.

Barracuda

Étape 3 : Protégez votre réseau

De nombreuses entreprises de taille moyenne emploient des personnes qui travaillent à divers endroits, et non dans des bureaux. Avec l'essor du télétravail et même des politiques de « travail depuis n'importe où », le périmètre du réseau s'est étendu de telle sorte qu'il est plus difficile de le protéger. Les employés sont connectés aux systèmes de l'entreprise et les uns aux autres par le biais d'applications cloud et de logiciels de communication, qui sont eux-mêmes des points d'entrée potentiels pour les pirates. Et avec les politiques BYOD (bring your own device), tant que vous n'aurez pas mis en œuvre une stratégie de sécurité des appareils rigoureuse et reproductible, les niveaux de protection seront variables, voire inexistants. Il est essentiel de s'assurer que tous les appareils sont sécurisés selon les mêmes normes rigoureuses.

Les PME doivent appliquer les meilleures pratiques pour sécuriser le périmètre et créer une protection renforcée autour de leurs réseaux afin de protéger et de connecter les personnes, les sites et les objets. Secure Access Service Edge (SASE) est une approche de la sécurité des réseaux qui consolide les fonctions de sécurité et centralise la gestion de la cybersécurité, améliorant ainsi la position globale de l'entreprise. Elle associe des fonctions de protection du réseau à des capacités de réseau étendu (WAN) pour répondre aux besoins d'accès sécurisé des entreprises modernes.

Zero Trust Network Access (ZTNA) est une autre approche qui contribue à protéger votre réseau en appliquant la philosophie « ne jamais faire confiance, toujours vérifier ». Elle accorde l'accès aux différents actifs et parties du réseau au cas par cas, en ne donnant l'accès qu'aux personnes qui en ont besoin et en vérifiant à chaque fois que ce sont bien ces utilisateurs qui tentent d'obtenir l'accès. ZTNA offre un moyen de connecter en toute sécurité les utilisateurs à votre réseau, quel que soit l'endroit où ils se trouvent, ce qui est parfait pour les entreprises dont le personnel est réparti.

Étape 4 : Protégez vos données

Les données sont un bien convoité, et les cybercriminels ne reculent devant rien pour s'en emparer. Les entreprises dont la protection des données est insuffisante s'exposent à des risques de fraude et d'extorsion. Alors que les pirates utilisant le hameçonnage et le ransomware tentent de voler des données pour exploiter des entreprises de toutes tailles, les entreprises de taille moyenne doivent appliquer des politiques strictes de protection des données, même si elles ne pensent pas que toutes leurs données sont sensibles.

Des backups réguliers sont essentiels, car ils protègent vos données en cas de dommages ou de perte de matériel et ajoutent un niveau de protection contre les attaques telles que les ransomwares. Grâce à des backups réguliers et complets, vous pouvez restaurer vos données à volonté, quelles que soient les actions du pirate et de son ransomware. ZTNA contribue également à la protection de vos données en veillant à ce qu'elles ne soient accessibles qu'aux personnes disposant des autorisations nécessaires.

L'état d'esprit, l'éducation et la formation à l'échelle de l'organisation sont également des aspects essentiels de la protection des données de votre entreprise. Même les PME doivent travailler dans l'optique de savoir quand, et non pas si, elles seront ciblées par une cyberattaque, et doivent former leur personnel en conséquence. Cela inclut l'éducation sur les politiques de mot de passe, car les mots de passe faibles sont un moyen courant pour les pirates d'accéder aux données.

Barracuda

Conclusion : agissez maintenant avant qu'il ne soit trop tard

Les PME ont besoin de solutions de cybersécurité et de protection rigoureuses, même si elles sont plus petites que les acteurs mondiaux que l'on pourrait croire être les cibles habituelles des pirates informatiques. Le fait est que chaque entreprise est une cible.

Les quatre points abordés dans cet eBook constituent un excellent point de départ pour une entreprise de taille moyenne qui cherche à renforcer son approche de la cybersécurité. Chaque zone nécessite une attention particulière et des solutions fiables doivent être mises en place pour garantir une protection maximale. Mais cela ne signifie pas que vous devez vous arrêter là. Considérez plutôt ces points comme une base essentielle de cybersécurité sur laquelle vous continuerez à vous appuyer à l'avenir.

Barracuda

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque entreprise doit se doter de solutions cloud-first, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients. Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda