Ressource de Petri IT Knowledgebase
de BWW Media Group

Document technique de Petri,
10 novembre 2022

Mesures de cybersécurité incontournable pour les PME

Commandité par

Devolutions

Survol

Bien que la cybersécurité soit l'une des principales préoccupations des entreprises d’informatique, l’implémentation d’une stratégie efficace pour contrer les cyberattaques n'a jamais été aussi ardue.

Qui plus est, les cybermenaces sont maintenant plus courantes et plus sophistiquées que jamais.

La transformation numérique et le « rançongiciel en tant que service » (Ransomware-as-a-Service) engendrent de nouveaux défis de sécurité

Il y a plusieurs raisons qui expliquent l'augmentation des cyberattaques. Tout d'abord, il faut savoir qu'au cours des dernières années la majorité des petites et grandes entreprises, des organisations et même des gouvernements ont été au cœur d'une véritable transformation numérique. Durant ce grand bouleversement, ils ont dû mettre à jour leurs systèmes informatiques et utiliser de nouvelles technologies. Résultat : l'introduction de technologies et de nouveaux appareils qui ne correspondent pas toujours au modèle de sécurité traditionnel.

Ensuite, la montée en flèche des « rançongiciels en tant que service » a favorisé l'essor des rançongiciels. La technologie a évolué pour les entreprises, mais aussi pour les cybercriminels. Ces derniers sont raffinés et disposent d'une panoplie d'outils de piratage facilement accessibles.

Les fournisseurs des rançongiciels en tant que service permettent aux cybercriminels qui n'ont pas les compétences techniques nécessaires pour créer et utiliser un rançongiciel de lancer des attaques quand même.

Pour couronner le tout, la pandémie a engendré une augmentation rapide et considérable du travail à distance. De fait, la surface d'attaque des entreprises a augmenté et a encouragé l'utilisation de périphériques personnels mal sécurisés. Il est évident que les entreprises devront composer avec ces problèmes à l'avenir.

Il est important de souligner que les cybercriminels ne se limitent pas aux grandes entreprises. Les PME sont de plus en plus ciblées ainsi que les entreprises sans défense telles que les écoles, les hôpitaux, les entreprises de fabrications et même les fournisseurs d'infrastructures comme les gazoducs et les centrales électriques. Selon le rapport de IBM et du groupe Ponemon, le coût d'une violation de données pour les organisations de toutes tailles a grimpé à une moyenne de 4,24 millions de dollars US par incident, le montant le plus élevé jamais enregistré. Pour les PME, le montant des pertes peut varier entre 120 000 et 1,24 million de dollars par incident.

Vous l'aurez remarqué : la sécurité informatique et la cybersécurité sont des problèmes à la fois coûteux et de plus en plus présents. Il est cependant important de comprendre que la sécurité n'est pas seulement une question de technologie. De nos jours, la manière d'aborder cette problématique peut décider de la survie d'une entreprise. Jetons ensemble un coup d'œil à certains des sujets qui occupent l'esprit des dirigeants de PME.

Évaluer la qualité de la sécurité informatique et le risque que posent les cybermenaces

La fréquence des cybermenaces augmente au même rythme que leur gravité. Dans le cadre du sondage de Devolutions sur le portrait de la sécurité informatique dans les PME 2022-2023, nous avons demandé aux dirigeants et aux décideurs des PME du monde entier de nous faire part de leur point de vue sur la sécurité informatique. La question suivante leur a été posée : ***« quel est votre niveau d'inquiétude en ce qui a trait aux dangers des cyberattaques contre votre entreprise par rapport à l'an dernier? ».*** Deux tiers (67 %) ont répondu ***« Nous sommes plus inquiets que l'an dernier »***, 28 % ont répondu avoir le ***« même niveau d'inquiétude »***, tandis que 5 % se disaient ***« moins inquiets »***.

Le fait que 67 % des entreprises soient plus inquiètes montre que la plupart d'entre elles se préparent à une augmentation des cyberattaques. Cependant, près d'un tiers des entreprises ont montré le même degré d'inquiétude que l'an dernier, ce qui indique qu'elles ne prennent peut-être pas les précautions adéquates pour faire face à une intensification des attaques. La diminution du niveau d'inquiétude (5 %) est peut-être due au fait que de nombreuses entreprises ont rappelé les travailleurs à distance au bureau depuis le recul de la pandémie, ce qui leur a permis de renforcer les contrôles de sécurité.

Il n'est pas surprenant que, lorsqu'on les interroge sur les types de menaces de cybersécurité qui les inquiètent le plus, la plupart des entreprises (81 %) s'inquiètent principalement des rançongiciels, suivis de :

- L'hameçonnage (69 %);
- Les logiciels malveillants (38 %);
- Et les menaces internes (21 %).

La montée en puissance des rançongiciels démontre hors de tout doute que les PME doivent se préparer à faire face à cette menace.

Sécuriser les logiciels tiers et la chaîne d'approvisionnement

Les attaques contre les logiciels tiers ou la chaîne d'approvisionnement brillent par leur absence dans la liste des préoccupations majeures des PME. Pourtant, la récente attaque de la chaîne d'approvisionnement de SolarWinds/Solarigate indique que les logiciels tiers doivent faire l'objet d'un contrôle rigoureux pour s'assurer qu'ils sont conformes aux meilleures pratiques de sécurité.

13 % des PME n'ont aucun moyen pour éviter les cyberattaques

La première étape est d'évaluer le risque à votre cybersécurité afin de comprendre et de répondre de manière appropriée aux dangers que posent les cyberattaques. Alors que la plupart des entreprises se préparent à une intensification des attaques par rançongiciel, des attaques par hameçonnage et des logiciels malveillants, le sondage a également révélé que 13 % des PME ne prennent aucune mesure pour se prémunir contre ces types d'attaques.

En d'autres termes, la cybersécurité ne doit pas être négligée, et ce, malgré les ressources limitées des PME.

Implémenter la gestion des accès privilégiés

La gestion des accès privilégiés (PAM ou Privileged access management en anglais) désigne la gestion des comptes administratifs et des comptes dotés de droits de sécurité élevés qui permettent d'effectuer des opérations de maintenance, de modifier le système et d'exécuter d'autres types d'opérations privilégiées. Ces comptes privilégiés sont souvent la cible de cyberattaques, car ils ont accès à des informations très sensibles, confidentielles et exclusives.

La protection et la gestion de ces comptes privilégiés sont donc une priorité absolue. Les solutions PAM sont la réponse appropriée à ce problème. Elles réduisent les risques de sécurité en protégeant les comptes à privilèges élevés, tout en diminuant les coûts opérationnels et en augmentant la visibilité de ces types de comptes.

Pour notre ***Portrait de la sécurité informatique dans les PME de 2022-2023***, nous vous avons posé la question suivante : ***« comment gérez-vous les accès aux comptes privilégiés dans votre entreprise? ».*** Seuls 12 % des entreprises ont déclaré avoir déployé une solution PAM complète. 9 % ont déclaré disposer d'une implémentation PAM partiellement déployée, dont ils n'utilisent que certaines des fonctionnalités.

La question suivante portait sur les raisons pour lesquelles certaines PME ne déploient pas de solutions PAM. Le sondage a révélé que 28 % des entreprises ont indiqué qu'elles ne disposaient pas du budget nécessaire. Par ailleurs, 12 % pensent que les solutions PAM sont trop complexes à implémenter et à gérer. Bien que compréhensible, ce point de vue ne correspond pas à la réalité d'aujourd'hui.

Les solutions de gestion des accès privilégiés sont désormais abordables et simples à déployer

Au départ, les solutions PAM étaient destinées aux grandes entreprises, et les PME ne pouvaient pas se les offrir. En plus, les PME ne pouvaient pas se permettre d'avoir une équipe de spécialistes internes de la cybersécurité pour configurer et utiliser ces anciennes solutions. Toutefois, ce paradigme a changé au fil des ans. Il y a désormais plusieurs solutions PAM faciles à utiliser et abordables pour les PME.

L'implémentation d'une solution PAM est l'une des méthodes les plus efficaces pour renforcer la cybersécurité des PME. Le sondage a également révélé que les trois fonctionnalités les plus importantes que les PME doivent retrouver dans une solution PAM sont :

1. L'expiration automatique des accès privilégiés;
2. L'authentification multifacteur intégrée (AMF);
3. La Rotation et la réinitialisation des mots de passe.

Les solutions PAM modernes offrent ce type d'automatisation, ce qui les rend efficaces et bien adaptées aux besoins des PME.

Sensibiliser les utilisateurs finaux à la sécurité

Malheureusement, la plupart des mesures de cybersécurité peuvent être déjouées par vos utilisateurs finaux. Ils constituent le maillon faible de la sécurité informatique, et il existe une multitude de moyens pour eux de compromettre même les meilleures stratégies de sécurité.

Parmi les compromissions majeures attribuables aux utilisateurs finaux, citons les mots de passe faibles (comme « mot de passe »), la réutilisation des mots de passe sur plusieurs sites, le partage des mots de passe, l'écriture des mots de passe, le fait de cliquer sur des liens suspects qui téléchargent des logiciels malveillants, ainsi que l'accès aux ressources de l'entreprise par des connexions Wi-Fi publiques non sécurisées.

La diversité des moyens par lesquels les utilisateurs finaux peuvent causer des failles de sécurité est presque infinie. Selon le rapport d'enquête de Verizon sur les fuites de données (DBIR) de 2022, 82 % des brèches survenues l'année dernière impliquaient le personnel de l'entreprise.

La sensibilisation à la cybersécurité demeure la meilleure façon de se prémunir contre les faux pas des utilisateurs finaux. Dans ***le rapport de Devolutions sur le Portrait de la sécurité informatique dans les PME de 2022-2023***, nous vous avons posé la question : ***comment votre entreprise sensibilise-t-elle les utilisateurs finaux à la sécurité des TI?*** Environ un tiers d'entre elles (30 %) se fient uniquement à des ressources telles que des vidéos, des articles et des webinaires. Un autre tiers (31 %) utilise la formation en ligne. Enfin, un nombre beaucoup plus faible (16 %) utilise la formation en direct, les ateliers ou les simulations (5 %). Et 12 % ne font rien du tout. Ne pas former l'utilisateur final revient pratiquement à l'exposer à une forme de faille de sécurité.

La bonne nouvelle est que la plupart des PME (88 %) offrent une certaine forme de formation à leurs utilisateurs. Un investissement important procure une protection immédiate en raison des coûts élevés d'une intrusion puisque la plupart des failles proviennent des utilisateurs finaux. Les coûts de la formation des utilisateurs sont insignifiants par rapport aux coûts d'une cyberattaque réussie qui pourrait mettre une PME en faillite.

Sécuriser la gestion de l'accès à distance

Au cours des deux dernières années, la pandémie a fait exploser l'utilisation des outils d'accès à distance pour les entreprises de toutes tailles. La surface d'attaque de l'organisation s'est ainsi considérablement étendue, et ce, malgré la facilité d'accès aux ressources et aux applications de l'entreprise depuis le domicile des travailleurs à distance.

L'accès à distance permet aux employés de se connecter aux systèmes locaux de leur bureau pour effectuer leur travail ou aux administrateurs d'entreprendre diverses tâches de gestion à distance. Les administrateurs et les responsables informatiques ont, comme on peut s'y attendre, souvent besoin d'identifiants privilégiés. Des mots de passe faibles, aisément identifiables, ou des mots de passe réutilisés qui peuvent être récupérés sur d'autres sites peuvent faciliter le travail des pirates. Une fois qu'un cybercriminel a obtenu l'accès à votre réseau, il peut potentiellement accéder à d'autres systèmes latéralement à travers vos réseaux.

Pour déterminer l'utilisation actuelle de l'accès à distance, nous avons demandé aux PME : ***quelle est la situation dans votre entreprise en ce qui concerne le travail à distance?*** Sans surprise, la majorité des entreprises (75 %) autorise le travail hybride, pratique selon laquelle les employés partagent leur temps entre le bureau et la maison. Seules 19 % d'entre elles demandent à leurs employés de travailler au bureau en tout temps et quelques-unes (6 %) les obligent à travailler à distance uniquement. Ces résultats montrent que le travail à distance et les technologies d'accès à distance restent très répandus et le resteront probablement pendant un certain temps encore, si ce n'est indéfiniment.

Une question supplémentaire portait sur les outils et les technologies utilisés par les entreprises pour sécuriser et gérer l'accès à distance.
Voici les trois solutions les plus populaires :

- Le réseau privé virtuel (VPN);
- L'authentification multifacteur;
- Devolutions Remote Desktop Manager (RDM).

Les travailleurs à distance ont davantage recours aux VPN depuis la pandémie. De nombreuses entreprises ont utilisé l'AMF comme couche de sécurité supplémentaire, car les travailleurs distants doivent confirmer leur identité en fournissant leur identifiant de connexion ainsi qu'un autre élément d'information externe, comme un code envoyé sur un téléphone portable.

RDM organise non seulement vos connexions à distance, mais renforce également la sécurité à distance grâce à ses capacités de gestion des mots de passe. La gestion des mots de passe de RDM prend en charge des politiques qui limitent l'utilisation des mots de passe, en plus d'exiger une longueur et une complexité minimales. Des outils supplémentaires, tels qu'un générateur et un analyseur de mots de passe, permettent aux utilisateurs de créer et d'utiliser plus facilement des mots de passe forts.

RDM stocke les mots de passe de manière centralisée dans un emplacement sécurisé, ce qui évite aux utilisateurs de devoir inventer leurs propres systèmes de stockage de mots de passe aléatoires et peu sûrs. RDM peut également fournir une vue d'ensemble et un journal de toutes les activités de connexion à distance pour votre entreprise.

Planification de la gestion de la cybersécurité informatique

Une gestion complète de la cybersécurité informatique consiste en des stratégies, des politiques, des processus, des technologies et des outils qui garantissent la protection, l'intégrité et la disponibilité des systèmes informatiques. L'augmentation constante du niveau des menaces, combinée à l'afflux de nouvelles technologies à sécuriser, laisse à penser que la sécurité accaparerait un pourcentage important du budget informatique des PME. Étonnamment, ce n'est pas le cas.

Pour ce qui est de la question « quelle part du budget de votre entreprise est allouée à la sécurité? », un tiers des entreprises sondées (32 %) a répondu qu'elle était inférieure à 5 %. Bien que le montant qu'une entreprise doit consacrer à la cybersécurité varie considérablement d'une entreprise à l'autre, 5 % ne semblent pas correspondre au niveau de menace actuelle.

58 % ont répondu que le pourcentage était inférieur à 20 % et seulement 10 % disent allouer plus de 20 % de leur budget à la sécurité. 49 % ont signalé une augmentation des dépenses de sécurité, mais 45 % ont répondu qu'elles étaient inchangées. À première vue, cela peut sembler insuffisant. Cependant, les entreprises doivent également tenir compte de l'environnement commercial global.

La pandémie a entraîné des dommages financiers d'une ampleur sans précédent pour de nombreuses entreprises. Une étude menée par la Réserve fédérale entre avril 2020 et avril 2021 a révélé qu'environ 200 000 PME aux États-Unis ont dû fermer définitivement leurs portes en raison de la pandémie. Pour de nombreuses PME, la réduction des dépenses de sécurité informatique était une question de nécessité plutôt qu'une stratégie volontaire.

Les principaux projets de sécurité que les entreprises envisagent pour l'avenir sont les suivants : les solutions PAM, A2F (authentification à deux facteurs, aussi appelée AMF), la formation des utilisateurs finaux, la mise à jour des stratégies VPN, la mise en œuvre de la rotation automatique des mots de passe et l'extension de la gestion des mots de passe. Tous ces projets de sécurité informatique fréquemment mentionnés sont liés à la gestion des identités et des accès, qui sont deux facteurs essentiels pour une cybersécurité à toute épreuve.

De la préparation à la protection

L'adage « la bonne planification protège des mauvaises performances » trouve sa pleine signification dans le domaine de la cybersécurité. Les entreprises se trouvent aujourd'hui à la croisée des chemins, car l'empreinte numérique des organisations continue de changer et d'évoluer, rendant obsolètes de nombreuses mesures de cybersécurité bien établies. Parallèlement, les menaces augmentent et de nouvelles apparaissent.

Les PME vont continuer d'accorder une importance accrue à la cybersécurité, en plus de se préparer à faire face à ces nouvelles menaces. Néanmoins, les PME doivent également s'assurer qu'elles tirent le meilleur parti de leurs investissements en matière de sécurité.

La préparation à la cybersécurité d'aujourd'hui requiert un ensemble de facteurs pour affronter les menaces actuelles telles que les rançongiciels, les logiciels malveillants et l'hameçonnage. Mettre en place des mesures de cybersécurité dignes de ce nom exige des PME qu'elles réévaluent les technologies de sécurité qu'elles ont mises en place pour faire face aux nouvelles menaces sophistiquées d'aujourd'hui.

Les mots de passe robustes et les politiques de mots de passe, comme celles prises en charge par RDM, offrent aux entreprises un niveau de protection essentiel en éliminant les mots de passe faibles et réutilisés. L'implémentation d'une solution de gestion des accès privilégiés comme Devolutions Server permet de s'assurer que les comptes privilégiés sont surveillés et que les utilisateurs disposent des niveaux de sécurité appropriés pour effectuer leur travail efficacement.

Il est important d'insister sur la sensibilisation à la sécurité des utilisateurs finaux pour favoriser des méthodes de travail plus sûres. En outre, les entreprises doivent aujourd'hui s'assurer que leurs chaînes d'approvisionnement sont protégées et que les autres entreprises avec lesquelles elles font des affaires ont mis en place des mesures de sécurité informatique solides et de bonnes pratiques.

Consultez le ***Portrait de la sécurité informatique dans les PME de 2022-2023*** pour en apprendre davantage sur la situation.

Informations supplémentaires

Pour plus d'informations concernant les enjeux et les solutions qui touchent les PME, veuillez consulter le portrait de la cybersécurité dans les PME en 2020-2021.

Devolutions